Asia-Pacific
Economic Cooperation

2009

Critical Infrastructure and Support Systems Standardization Project

A Standards Australia and APEC initiative to identify and prioritize standards to enhance regional security and emergency management

APEC Sub Committee on Standards and Conformance

June 2009

Sponsored by
Standards Australia

Prepared by

Mark Bezzina

StanCert Pty Ltd
PO Box 49 Burwood Plaza NSW 2134 Australia
Tel: (61) 2 8721 6434 Fax: (61) 2 9012 0073
Email: **bezzina@stancert.com** Website: **www.stancert.com**

Produced for
The Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 68919-600 Fax: (65) 68919-690
Email: **info@apec.org** Website: **www.apec.org**

APEC Publication Number: APEC#209-CT-01.5 **(revised to 209-CT-01.13 - duplicate)**

Disclaimer
The views expressed and the conclusions reached in this report are those of the author and do not necessarily reflect the views of APEC, Standards Australia or the consensus view of APEC member economies.

Foreword

You do not need to search far to understand the importance that the leaders of the 21 APEC Member Economies place on security. For the last five years there has been a strong emphasis by leaders in their annual declaration on the importance of security. Again in 2008, leaders declared that 'Enhancing human security and protecting the region's business and trade against natural, accidental or deliberate disruptions remains an enduring priority for APEC, and an essential enabling element in APEC's core trade and investment agenda.'

Security is and will remain a top priority for APEC Member Economies. It is important that tools be provided to businesses and government within the region to enable them to understand security issues and to manage and respond appropriately to security threats. This is why good security standards are so valuable. They provide essential information and advice to guide decisions on a whole range of issues. Of course, standards can't tell businesses what they need to do - but they provide critical benchmarks which say what is reasonable and prudent.

Standards Australia along with APEC have contributed significantly to resource this project in order to understand the region's needs in terms of information to better manage security threats. The outcomes and recommendations of the project are based on feedback received from a range of stakeholders across the 21 APEC Member Economies. The project has also identified where gaps exist in the existing standards, and it has set out recommendations for future actions.

Mr. John Tucker
Chief Executive Officer
Standards Australia

Mr. TEO Nam Kuan
Chair
APEC Sub-Committee on Standards and Conformance (SCSC)

Acknowledgments

Mark Bezzina, the author of this report, wishes to thank the following individuals and organizations for their support of the project.

- All individuals and organizations participating in the survey
- The key contact points and their deputies
- The CEOs, executives, management and staff of all National Standards Bodies in APEC Member Economies
- APEC Secretariat
- The members of the APEC Business Advisory Council (ABAC)
- The members of the APEC Sub-committee on Standards and Conformance (SCSC)
- The members of the Pacific Area Standards Congress (PASC)
- The members of ASIS International
- The members of Standards Australia's National Centre for Security Standards (NCSS)
- The project sponsor: Brian Phillips, Manager, Standards & International Liaison, Industry & Small Business Policy Division, Department of Innovation, Industry, Science and Research, Australia
- The project supervisor: Karen Hitchiner, Manager, International Development, Standards Australia
- The co-sponsoring economies: New Zealand, Peru, Viet Nam
- The Directorate for Standards and Quality (STAMEQ), Viet Nam for their assistance in hosting the project workshop and facilitating travel visas. Particular thanks to Vu Van Hong, Deputy Director, International Cooperation Department, and Mai Sinh Nguyen, Senior Officer. The assistance provided by staff at the Directorate was also greatly appreciated.
- Colleagues from Standards Australia including John Tucker, Chief Executive Officer, Colin Blair, Deputy Chief Executive Officer, LoAnne Lam, Sherene Daniel, Rebecca Ball and Eliza Young
- Co-authored by Clare Morrison, Lead Consultant, StanCert Pty Ltd

Contents

Table of figures

1. Executive Summary

The Critical Infrastructure and Support Systems Standardization Project was initiated at the ABAC - PASC dialogue meeting in Cartagena on 26 April 2007. It builds on the outcomes of the Security Standards and Support Systems (4S) project, a similar Australian initiative that was instigated by Standards Australia and conducted in collaboration with the Australian Commonwealth Attorney-General's Department and the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN).

Standards are critical to the achievement of improved security in the Asia-Pacific region. Clearly, the owners and operators of critical infrastructure in the region agree with this premise as 82% of respondents indicated their major source of guidance was international standards. Through this project, the owners and operators of critical infrastructure were given the opportunity to identify and clarify their security standards requirements. They also shared important insights about major security issues in their sectors and potential solutions. Many of the security issues highlighted were common across sectors and this provides a sound basis for strategic planning in the region.

The project was based on an online survey that was structured on the Integrated Security Standards Framework developed by Standards Australia as part of the 4S project and revised by representatives from APEC Member Economies.

The project received widespread support and involvement. All 21 APEC Member Economies agreed to participate in the project and there was active engagement from 18 Economies. Each of the Economies, with the exception of Australia, nominated a key contact point to coordinate and promote the survey in their economy. Australia did not nominate a key contact point due to prior participation in the 4S project.

The benefits to APEC economies from participation in the survey are:

- a more consistent approach to security along with emergency and disaster management in the APEC region;
- the promotion of security standards and systems capacity which support business as well as critical infrastructure in times of emergency, helping to minimize impact on economies;
- harmonization of related standards across the APEC region, which will help improve the interoperability and compatibility of systems related to securing critical infrastructure;
- improved technical capacity through assistance in ascertaining key areas of standardization focus so that programs may be targeted for the development of security standards; and

- the capacity to make more informed choices about effective security solutions through better access to information on tested and consistent methods to protect critical infrastructure.

The key project objectives were to:

- identify and detail some of the issues, barriers and solutions related to protecting critical infrastructure and identify user perceptions of the importance of standards related to securing critical infrastructure;
- identify and prioritize the standards required by the owners and operators of critical infrastructure and identify the gaps between existing standards and the needs of the owners and operators of critical infrastructure; and
- make recommendations on how the gaps in standards may be addressed and develop a blueprint for the development of a security standards framework that is essential in identifying and categorizing security standards.

There were 539 valid survey responses including 26 partially completed surveys with sufficient information provided for inclusion in the survey results. This was an excellent response rate, especially given that the survey was in English. The gender breakdown was 21% female 79% male. All major sectors were represented in the results. There was a large response from government, however this is due to the fact that in many economies critical infrastructure is owned and operated by government. There was a high level of representation from managers and technical specialists. The views of CEOs and executives were also well represented in the results.

The analysis focuses on overall results and, where relevant, comparison is made with results from CEOs and executives and results by sector. Although the initial intention was to provide results by economy, this was not a possibility due to the varying levels of participation by the member economies. In the preparation phase, feedback was received about the importance of ensuring confidentiality and anonymity for survey responses. There was a risk that potential respondents would not complete the survey due to these concerns. It was not possible for the survey to be completely anonymous as there would be no way to verify that the data was genuine. It was also necessary to have some means of contacting the respondents if the data entered was incomplete or incorrect. The issue was addressed by providing information in the survey instructions about how the data would be used and minimizing requirements for mandatory contact information in the survey.

Although there is strong support for standards at the CEO level, this support diminishes at the executive and particularly the managerial levels. This shows that the message CEOs intend to convey is not necessarily permeating through the organization to the operational level. This is a serious concern and it has been recommended that ABAC consider liaising with APEC (SCSC) on holding a high-level workshop to allow CEOs and executives across the region an opportunity to prioritize common security issues and consider regional strategies. An outcome of this workshop could be the development by APEC (SCSC) of a regional security plan, based on the workshop outputs and the results from this survey. CEOs should also consider implications from this finding within their organizations. The importance of establishing a security culture within organizations was highlighted, particularly in relation to information security.

A further recommendation has been made that SCSC consider education and awareness raising programs to ensure that personnel at technical and operational levels understand the importance of standards to the protection of critical infrastructure. These programs could be targeted to particular sectors and linked to capacity building in the member economies. The report also recommends consideration of communication strategies to ensure adherence to standards deemed critical to security.

Overall respondents rated governance, strategy and policy along with risk management as the key broad areas requiring standards development. This is at odds with the traditional view that standards should only focus on technical issues.

The top four security issues overall were information / data, funding, resources and training. Respondents raised concerns about workforce planning, the quality of security personnel and the need to lift the profile of the security industry. This report recommends that SCSC consider engaging with industry bodies to develop security officer qualification guidelines to raise standards and attract professionals to the industry. These guidelines could then be promoted for adoption throughout the region.

As in many other industries, the aging population is presenting challenges to the security industry in relation to the retention of expertise, knowledge and experience. Succession planning is an important area for consideration by organizations and within industry. Access to quality training, particularly in technological areas that are changing rapidly, was also highlighted as a key issue.

Respondents wanted a common platform for sharing information, experience and best practice, especially on an international level. Respondents were struggling to work through this concept as they needed to balance their need for knowledge with the obligation to protect sensitive national and organizational information. The TISN in Australia has developed such protocols and this is a proven and effective model for application on a regional basis. It has been recommended that SCSC consider the creation of protocols to enable data to be securely shared between organizations, such as those established for the TISN.

It has also been recommended that, if deemed useful, ABAC consider supporting the feasibility of deploying emergency response teams and / or security advisors in the region. In this way, expertise or experience in managing particular types of emergencies could be shared with other countries. Emergency management was identified as a priority area for standards development and there have been several examples in recent times of countries in the Asia-Pacific region dealing with major disasters. At the time of writing, Australia has been battling severe floods and the worst bushfires on record, with widespread and tragic consequences. Other countries in the region have experience in dealing with tsunamis, hurricanes, earthquakes, acts of terrorism and political unrest. Invaluable knowledge and experience has been gained through the management of such disasters and this could be passed on to other member economies.

The vast majority of respondents indicated that training was the preferred method that would make the implementation of security standards more successful. The proportion of support for all other methods was significantly lower. Emphasis was also placed on the need for standards to be simple to understand, practical and tailored to local conditions and industry sectors.

For ease of reference, the recommendations from the project are summarized in the following section. The recommendations are also embedded in the main body of the report to show the rationale and logical sequence for these conclusions.

Based on the analysis of survey responses, 15 priority areas were identified for the development and revision of international standards related to the security of critical infrastructure in the region:

Governance, strategy & policy

1. Effective leadership
2. Crisis management
3. Security management

Risk management

1. Emergency management
2. Risk management
3. Command, control and communications

Information security

1. Network security
2. Systems access control
3. Information security (storage and categorization of sensitive information)

Personnel security

1. Security training systems for staff
2. Building and facility access control
3. Pre-employment screening

Physical security

1. Security of facility utilities (water, gas, electricity, telecommunications and waste)
2. Perimeter security (e.g. lighting, fencing, bollards, chains, doors, windows, gates)
3. Construction security (e.g. construction materials, building structure, fire protection)

For the sake of brevity, the gap analysis focuses on international standards. It is acknowledged that there are also national standards, legislation and other sources of guidance available and under development. The analysis showed that there are opportunities for further standards development, particularly in the categories of Crisis management, Security management, Emergency management, Information security, Pre-employment screening, Building and facility access control, Security of facility utilities, Construction security and Perimeter security.

With regard to Emergency management there has been important work carried out by the SOM Special Task Forces on Emergency Preparedness (TFEP) and Counter-Terrorism (CTTF). There are also a number of projects and new initiatives that the CTTF has endorsed for implementation in 2009. In relation to Information security, there is a focus on IT and document control in available standards with less emphasis on the management of sensitive information with the potential to impact on security. This also relates to the recommendation in the report about the creation of protocols for sharing sensitive information. Similarly, there are many relevant construction standards, however graded security is an area that warrants further consideration in standards development. The gap analysis also highlighted the following areas for inclusion in the education and awareness programs recommended in the report:

- Key standards related to security
- Risk management
- ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management (Redesignation of ISO/IEC 17799:2005)
- Emergency management with particular emphasis on ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management and the emerging standards:

  ISO/WD 22300 Societal security - Fundamentals and vocabulary;

ISO/NP 22320 Societal security - Principles for command and control, coordination and cooperation in resolving incidents

ISO/NP 22322 Societal security - Inter/Intra organizational warning procedures

The gap analysis also found that there were no standards on Effective leadership and this is an area of focus for inclusion in the CEO / Executive workshop recommended in the report.

Finally the gap analysis found that it is quite difficult to segregate key security standards when using existing databases. This was particularly difficult when searching in categories with high volumes of standards, such as risk management and IT. Standards bodies may need to consider new approaches to organizing standards so that key security standards can be quickly and easily identified by topic. This may be a question of restructuring existing databases. There is a risk that important information may be missed by organizations if this is not addressed.

It is recommended in the report that SCSC consider engaging with the ISO/IEC/ITU-T Strategic Advisory Group on Security (SAG-S) to address the gaps in standards identified as critical to security in the region. It would also be important to communicate with the SOM Special Task Forces on Emergency Preparedness (TFEP) and Counter-Terrorism (CTTF) in relation to this dialogue.

Based on the analysis and comments from respondents, transport and health are areas that warrant further investigation in relation to security standards development on national and international levels.

The survey was based on the Integrated Security Standards Framework. Analysis of comments showed that the model was robust and comprehensive. It has been recommended in the report that this Framework be considered by SCSC as a blueprint for identifying and categorizing standards that are critical to the security of critical infrastructure in the region. The Framework would underpin and inform the future development and revision of standards related to the protection of critical infrastructure in the region.

The way forward to maximize benefits from this project will involve consideration by ABAC and SCSC of the key recommendations from this report, which include proposed strategies to implement a more integrated approach to the security of critical infrastructure in the region.

2. Summary of Recommendations

In order to ensure that the project achieves its objectives in the region, consideration to be given by ABAC to:

i) Liaising with APEC (SCSC) on holding a high-level workshop to allow CEOs and executives across the region an opportunity to prioritize common security issues and consider regional strategies.

An outcome of this workshop could be the development by APEC (SCSC) of a regional security plan, based on the workshop outputs and the results from this survey.

ii) If deemed useful, supporting the feasibility of deploying emergency response teams and / or security advisors in the region. If these options are already in existence, consideration to be given to communication about access to these within the region.

Consideration by SCSC of the following strategies would also be very beneficial:

iii) Implementation of the Integrated Security Standards Framework as a blueprint for identifying and categorizing standards that are critical to the security of critical infrastructure in the region.

iv) Engaging with the ISO/IEC/ITU-T Strategic Advisory Group on Security (SAG-S) to address the gaps in standards identified as critical to security in the region. It would also be important to communicate with the SOM Special Task Forces on Emergency Preparedness (TFEP) and Counter-Terrorism (CTTF) in relation to this dialogue.

v) Communication strategies to encourage adherence to existing standards related to the protection of critical infrastructure in the region.

vi) Engaging with industry bodies to develop a set of security officer qualification guidelines to raise standards and attract professionals to the industry. These guidelines would need to be promoted for adoption throughout the region.

vii) Introducing education and awareness raising programs in the region to ensure that personnel at technical and operational levels understand the importance of standards to the protection of critical infrastructure. The programs could initially be targeted to particular sectors, such as transport and health, and linked to capacity building.

viii) Exploring alternative sources of funding, such as private/public partnerships, for areas of standards development deemed critical to the security of particular sectors within the Asia-Pacific region.

ix) The creation of protocols to enable data to be securely shared between organizations, such as those established for the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) in Australia.

If such protocols are already in existence, SCSC to consider communicating these to the owners and operators of critical infrastructure in the region.

3. Introduction

The impetus for this project came from the need to refocus on security in the Asia-Pacific Region following events such as natural disasters and criminal activity in recent times. It builds on the outcomes of the Australian Security Standards and Support Systems (4S) project, a similar initiative that was undertaken in Australia.

The pressure on security professionals and businesses to manage and respond appropriately to security threats has never been greater. Good security standards provide essential information, advice and benchmarks to guide reasonable and prudent decisions. Fundamentally, standards articulate best practice.

The project aimed to identify where gaps exist in the existing standards and recommend priorities for the development of future standards. There was a solution-oriented approach to barriers identified relating to protecting critical infrastructure. Most importantly, the project provides a blueprint for the development of a standards framework for identifying and categorizing security standards.

There are clear benefits to APEC Member Economies from participation in this project including:

- a more consistent approach to security along with emergency and disaster management in the APEC region;
- the promotion of security standards and systems capacity which support business as well as critical infrastructure in times of emergency, helping to minimize impact on economies;
- harmonization of related standards across the APEC region, which will help improve the interoperability and compatibility of systems related to securing critical infrastructure;
- improved technical capacity through assistance in ascertaining key areas of standardization focus so that programs may be targeted for the development of security standards; and

- the capacity to make more informed choices about effective security solutions through better access to information on tested and consistent methods to protect critical infrastructure.

4. Key objectives

The key project objectives were to:

- identify and detail some of the issues, barriers and solutions related to protecting critical infrastructure and identify user perceptions of the importance of standards related to securing critical infrastructure;
- identify and prioritize the standards required by the owners and operators of critical infrastructure and identify the gaps between existing standards and the needs of the owners and operators of critical infrastructure; and
- make recommendations on how the gaps in standards may be addressed and develop a blueprint for the development of a security standards framework that is essential in identifying and categorizing security standards.

An all hazards approach has been taken to threats. This approach includes security threats that are intentional or man-made (such as criminal acts or terrorism), as well as accidents, natural disasters and pandemics. The reason for this all hazards approach is to ensure that where possible multiple risks are dealt with by effective and integrated treatments, such as standardized products and services. The resultant standards can be developed in a modular fashion or in such a way as to not cause additional vulnerabilities by describing key aspects of security that can form the basis for new attacks.

Critical infrastructure can be damaged or destroyed by a number of factors including the following:

- natural disasters
- negligence
- accidents
- terrorism
- hacking and vandalism
- criminal activity
- malicious damage.

The standards identified under this project should assist the owners and operators of critical infrastructure to:

- provide adequate security for their assets

- actively apply risk management techniques to their planning processes
- conduct regular reviews of risk management plans
- report any incidents or suspicious activities to the police
- develop and regularly review business continuity plans, and
- participate in any exercises to test plans conducted by government authorities.

An important aspect of this project is that it needs to be supported and driven by the owners and operators of critical infrastructure.

The project focused on elements of critical infrastructure as shown in Figure 1.

Sectors	Sub Sectors
Energy	Gas, petroleum fuels, electricity generation, transmission and distribution.
Utilities	Water, waste water and waste management.
Transport and transport infrastructure	Air, road, sea, rail and inter-modal (cargo distribution centres)
Communications	Telecommunications (phone, fax, Internet, cable, satellites), electronic mass communications and postal services.
Health	Hospitals, public health and research and development laboratories.
Food supply	Bulk production, storage and distribution.
Finance	Banking, insurance and trading exchanges.
Government services	Defence and intelligence facilities, houses of parliament, key government departments, foreign missions, key residences, emergency services (police, fire, ambulance and others) and nuclear facilities.
National icons and places of mass gathering	Buildings, cultural, sport and tourism.
Essential manufacturing	Defence industry, heavy industry and chemicals.

FIGURE 1 ELEMENTS OF CRITICAL INFRASTRUCTURE

5. Project output

The major project output is this final report that contains the following elements:

- An outline of some of the issues, barriers and solutions related to protecting critical infrastructure and a summary of user perceptions of the importance of standards related to securing critical infrastructure.
- A suggested list of the standards required by the owners and operators of critical infrastructure and the identification of gaps between existing standards and the needs of the owners and operators of critical infrastructure.

- Clear recommendations on how the gaps in standards may be addressed and a blueprint for the development of a standards framework that is essential in identifying and categorizing security standards.
- Details of the issues and barriers facing the owners of critical infrastructure from an industry, APEC Member Economy and APEC regional perspective.

An inventory has been developed of standards that are required to protect critical infrastructure in times of an emergency, to minimize the impact on business and to assist business continuity. A gap analysis has been conducted against existing standards addressing the priority needs of owners and operators of critical infrastructure.

A framework for categorizing the constituent elements of a security management framework for critical infrastructure is proposed in the report. There is also a set of recommendations in the form of a roadmap for developing standards to assist with the protection of critical infrastructure.

6. Drivers for the project

The Critical Infrastructure and Support Systems Standardization Project is necessary because there is a need for simple and agreed standards to protect infrastructure. This guidance is necessary due to the many drivers that are shown in Figure 2.

- Environmental change and its impact as well as the advent of a number of natural disasters
- Demand to manage security risks and compliance to protect assets and the community
- Transfer of infrastructure from public to private companies
- The need for documents with authority that have been developed through a formal process of openness, transparency and consensus
- The need for internationally harmonized documents developed by an impartial body not bound by any jurisdiction
- The need for simple and agreed guidance
- The heightened threat of terrorist attack
- Community concerns about security and privacy
- Regulation (light touch)
- Demand for food and supply chain security
- Demand for indicative assurance confidence and consensus
- The need for collaboration in the development of systems

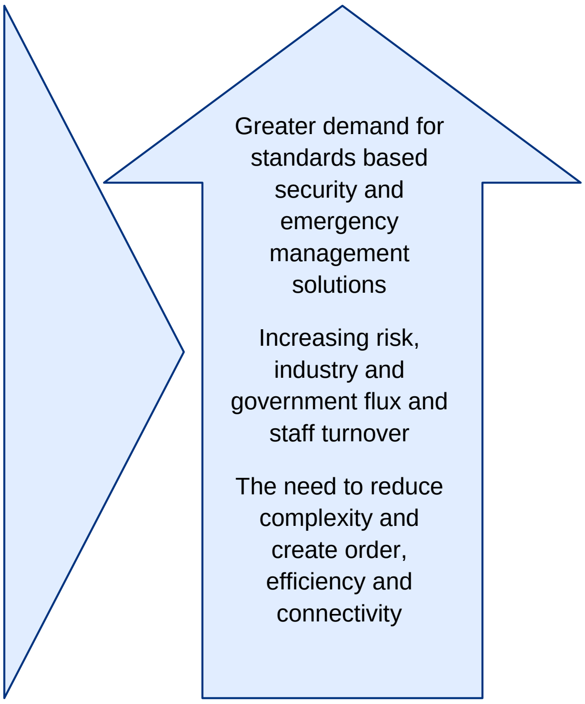

Greater demand for standards based security and emergency management solutions
Increasing risk, industry and government flux and staff turnover
The need to reduce complexity and create order, efficiency and connectivity

FIGURE 2 DRIVERS FOR SECURITY STANDARDS

7. Integrated security standards framework

Traditionally standards develop in a bottom up fashion. This occurs because industry experts working in a particular field identify a need for a new standard. For example an information technology (IT) expert may want to exchange secure data, so they recommend the development of a new cryptography standard. This is a valid approach to standards development, however such an approach makes it difficult to prioritize and resource standards development projects. Additionally there may be new areas where standards are required but work does not proceed because there is not an existing standards development group in place. It is also difficult to coordinate groups responsible for preparing related standards, which is necessary in order to achieve a consistent approach to security.

To address this problem a top down approach should complement the bottom up approach to standards development. A top down approach would involve looking at the entire area of security and identifying where standards are required and should have priority. It is impossible to effectively and comprehensively apply a top down approach without some framework to identify all the areas covered by standards development. For this purpose it is suggested that a security standards framework be established.

The use of a framework is recommended to ensure that each specialized standard is restricted to specific aspects and makes reference to wider ranging standards for all other relevant aspects. The structure is built on the following types of standards:

- Basic security standards, comprising fundamental concepts, principles and requirements with regard to general security applicable to a wide range of products, processes and services.
- Group security standards, comprising security applicable to several or a family of similar products, processes or services dealt with by more than one committee, making reference, as far as possible, to basic security standards.
- Security product standards, comprising security aspect(s) for a specific, or a family of product(s), process(es) or service(s) within the scope of a single committee, making reference, as far as possible, to basic security standards and group security standards.
- Product standards containing security aspects but which do not deal exclusively with security aspects; these should make reference to basic security standards and group security standards.

Keeping in mind the purpose, it is important that any framework addresses the following criteria:

- Identify the broad areas that require security standards.
- Simple, communicable and easily understood.
- Provide the basis for categorizing, managing the scope and taking stock of existing standards activities as well as identifying gaps and priority areas.
- Supported by key stakeholders.
- Widely used, openly available and unencumbered by intellectual property protection.

On the basis of results from the preceding Australian Security Standards and Support Systems (4S) project, a draft integrated security standards framework developed by Standards Australia's National Centre for Security Standards (NCSS) was revised. This revised framework became the foundation for this new body of work in the Asia-Pacific region.

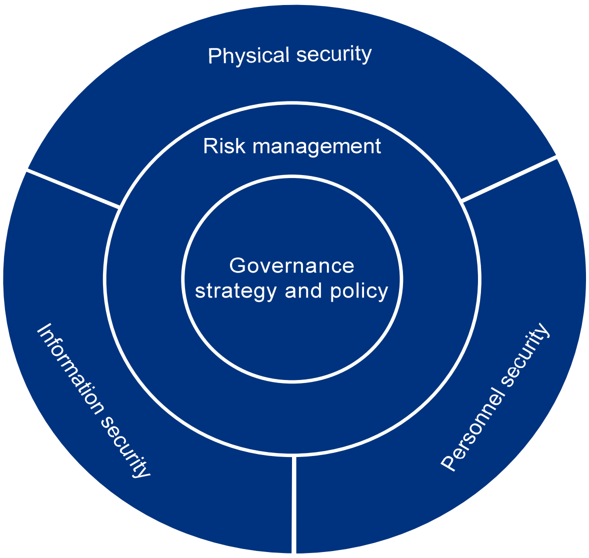


FIGURE 3 INTEGRATED SECURITY STANDARDS FRAMEWORK

The key components of the model are explained below.

Governance, strategy and policy

This element encapsulates product and systems standards related to the overall governance and management of an organization with respect to security.

The focus of this element is on the continued ability of an organization to achieve its strategy, objectives and targets.

To achieve the organizational strategy it is necessary to have in place a rigorous system that assists with the identification, quantification and categorization of tangible (physical) and intangible (information and people) assets in relation to their importance in achieving the organizational strategy. The reason why such a process is necessary is that it ensures the level of security chosen for a given asset is fit for purpose or based on the value of the asset in terms of its impact on the organization.

Other important aspects of this element include legal compliance management, communications and media management, audit, compliance and management review mechanisms for the purposes of continuous improvement. This element also includes standards designed to manage outsourcing and the purchasing of security services or services that impact on security as well as reporting incidents and issues management.

Risk management

The risk management element includes all standards and supporting material associated with risk management including:

- Systems to assist with monitoring the environment and intelligence gathering, such as examining the social, political and economic environment.
- Understanding interdependencies, intents, capabilities and threats.
- Tools to help establish the security context.
- Risk identification, analysis, evaluation, treatment, communication and monitoring.

This element encompasses business continuity management, which is one possible risk mitigation strategy. Business continuity management involves preparing for the eventuality of an event or incident by having in place a pre-developed and practiced emergency response, continuity response and ultimate recovery strategy.

Information security

The information security element includes all standards and supporting material associated with an integrated system for the management of information security. This element deals with the confidentiality, integrity and availability of information and encompasses such things as document, data and records control. It also addresses the security of networks, hardware, software, communications and supporting processes.

Personnel security

Personnel security involves a procedural system implemented to ensure that only those people whose work responsibilities require them to access official information and assets have such access. This is done by limiting the number of people who have access to those who can demonstrate a need to know or a need to have access and whose eligibility has been determined after an evaluation of their history, attitudes, values and behavior.

The personnel security element includes all standards and supporting material associated with an integrated system for the management of personnel security. Personnel security standards encompass occupational health and safety, pre-employment screening, privacy, administrative records, security roles and responsibilities, induction and training, identity management, access control (employees and other), protecting individuals, working from home and the security of employees when working overseas.

Physical security

Physical security is the part of security concerned with the provision and maintenance of a safe and secure environment for the protection of the organization's employees and clients. This includes physical measures designed to prevent unauthorized access to official resources and to detect and respond to intruders.

The physical security element includes all standards and supporting material associated with an integrated system for the management of physical security.

Physical security standards include access to security advice from professionals, security equipment requirements, site selection, design security, building security, perimeter security, lighting, alarms, safes and strong rooms, guards, patrols and control rooms, CCTV and emergency planning and incident procedures.

Analysis of comments on the Integrated Security Standards Framework showed that the model was robust and comprehensive. It is therefore proposed that this Framework be considered by SCSC as a blueprint for identifying and categorizing standards that are critical to the security of critical infrastructure in the region. The Framework would underpin and inform the future development and revision of standards related to the protection of critical infrastructure in the region.

Recommendation:

- SCSC to consider implementation of the Integrated Security Standards Framework as a blueprint for identifying and categorizing standards that are critical to the security of critical infrastructure in the region.

8. Methodology

The project methodology took the following form:

1. Preparation
2. Capacity building
3. Consultation
4. Analysis and validation
5. Reporting and communicating results

Preparation

The Critical Infrastructure and Support Systems Standardization Project built on the work of the Security Standards and Support Systems (4S) project that was undertaken previously in Australia. A survey conducted during the 4S project was revised in accordance with the new categories in the Integrated Security Standards Framework, which was modified as a result of that project.

Given the international setting for the project it was decided to conduct the survey online. A review of available online survey applications was carried out and SurveyMonkey was identified as the most appropriate choice in terms of sophistication, ease of use, scalability, flexibility and data analysis capability.

The initial draft of the survey was set up online and made available for review and feedback from 28 February 2008 until 1 October 2008 when the survey commenced.

The project plan and background paper were also revised during this period to reflect changes since the original proposal was submitted to APEC. It was necessary to revise the timetable attached to the project plan due to administrative requirements.

The chief executive officers of the National Standards Bodies in APEC Member Economies were provided with information on the project and invited to nominate a key contact point and deputy to represent their economy on the project. This email correspondence was sent on 28 February 2008 with the project plan and background paper attached for information.

An online form was set up on the survey application for registration of nominations. Most representatives completed this form, which was used to establish a mailing list for communication.

Outstanding nominations were followed up during ensuing weeks. This was necessary due to changes in contact information and emails failing to reach recipients due to technical issues such as firewalls. The project team also followed up by email, telephone and fax as necessary to ensure that information had been received. The project supervisor also promoted the project and followed up outstanding nominations through her international contacts. The executive management of Standards Australia delivered formal presentations on the project at international events and forwarded information through their associations with APEC, ABAC and the Pacific Area Standards Congress (PASC). The high level of participation from APEC Member Economies was eventually achieved as a result of these concerted efforts.

There was limited feedback on the draft online survey prior to the training workshop however the comments received were positive and constructive. The comments were considered during further revision of the survey tool. The limited initial feedback was not seen as a cause for concern as extensive consultation had occurred during the previous project in Australia prior to the development of the tool. During preparation for the training workshop sufficient time was allocated in the program to allow participants to test the survey tool and provide feedback on the content.

This feedback from the workshop was considerable, very positive and constructive. This assisted the project team to refine the tool further. The comments were collated and this information was emailed to all delegates with the responses to suggestions. Where the suggestions were in line with the focus of the project, most were taken on board in the final review of the survey tool. If suggestions were not included the responses to the feedback explained the reasons for this.

There were differing views expressed about the draft survey tool during this preparation phase. The challenge in developing the survey tool was to achieve a balance in meeting the needs of the diverse interest groups involved in the protection of critical infrastructure and support systems within the different APEC Member Economies. The project team believes a fair balance was achieved when considering all views in the final review of the survey.

SSL encryption was applied to the final version of the survey to protect the security of the data. This helped to address concerns raised during the workshop about the confidentiality of information provided.

The workshop program and training materials were also prepared during this period. Three quotes for possible venues and accommodation were obtained and the Hilton Ha Noi Hotel was identified as the most appropriate and cost-effective choice. The Events Manager and her team at Standards Australia provided excellent support in organizing the logistics of the venue and travel arrangements. Regular communication with the APEC Secretariat was required during this period to clarify requirements and comply with procedures for reimbursement of funding to APEC

Member Economies eligible for travel funding from APEC. This also involved regular email communication with the eligible member economies.

This stage of the project also included the preparation of two presentations on the project that were delivered by Standards Australia to APEC SCSC and PASC, as well as a project update report to the APEC Secretariat.

The project team also reviewed the various publications related to APEC funded projects to ensure that requirements were met.

Capacity building

The capacity building stage focused on providing guidance to participating APEC Member Economies on how to carry out the survey in their own economy. This was primarily provided through a training workshop held in Ha Noi, Viet Nam, on 27 August 2008. The presentation slides from the workshop were also emailed to the key contact point group.

The workshop was considered a success. This was evident in the evaluation forms completed by participants with the average overall rating on the training provided being 4.6 out of 5. All participants rated the quality of the content at the highest level possible on the evaluation forms.

Ongoing instruction and support were provided remotely during the project. Following the workshop an online training tutorial was made available on the Standards Australia consultant's website. This allowed representatives who were not able to attend the workshop to access the training.

The key contact points employed a number of strategies to promote the survey in their economies. These included mail-outs directly and through industry bodies, newsletters, website coverage and presentations at national and international events. The key contact points provided beneficial support to one another through this stage of the project. They also took opportunities to promote the survey more widely when attending international events, rather than simply focusing on their own personal targets.

As PASC co-sponsored the project, non-APEC members of PASC were also invited to participate in the survey. It was not seen as appropriate to include these countries in the workshop which was APEC funded, however the online training tutorial provided a viable training alternative. Survey responses were received from all non-APEC member countries of PASC and included in the results.

Analysis and validation

The survey opened online on 1 October 2008 and was to close on 1 December 2008. A decision was made to extend the survey until 8 December 2008 as the opening of the survey coincided with the celebration of the end of Ramadan. This may have impacted on the availability of some key contact points at the start of the survey. The extension also allowed time for key contact points to complete manual data entries in cases where there was limited access to the internet.

During the survey it became apparent that some respondents were not fully completing the survey. In most of these cases the respondents had only completed the contact details and background information page before closing the survey tool. As this data did not add value to the survey results, these entries were backed up and then deleted from the online survey tool. Follow-up emails were then sent to the respondents to invite them to return and complete the survey. A note was also added to the introductory page of the online survey to clarify that the survey needed to be completed in one sitting. The key contact point group was made aware of this issue so that it could be highlighted in communications.

Partially completed survey responses were included in the results if respondents progressed beyond the contact details and background information page. Variations in the total number of responses for particular questions are due to skipped questions in partially completed survey responses.

The survey tool had the capacity to enable live viewing of the results as these were collected in real-time. Progress towards achieving targets could therefore be carefully monitored.

One or two member economies found that potential respondents did not have access to the Internet or were reluctant to complete an online form. For this reason, a manual data entry link was made available. This link looped back to the start of a new form upon submission, which was more convenient for manual data entry. The respondents were able to complete the .PDF version of the survey by hand and the data was then entered manually on their behalf. The key contact point group was briefed on storing the survey forms securely in order to ensure the confidentiality of data collected using this approach.

Summary results were viewable by the project team on screen in bar graph format. The summary and total results could also be exported as spreadsheets for further analysis. The survey tool also had the capacity for filtering the data and exporting filtered results. These facilities meant that there were considerable savings on time and resources in relation to data analysis.

During this phase the responses were checked and key results set up in chart and table format for the report. The data was analysed at a high or broad level, rather than by member economy (for APEC) or country (for PASC) due to data spread considerations. Additional filtering of results was undertaken for comparison with the overall results. Analysis was undertaken by sector as necessary for interpretation of results. The results from CEOs and executives were also compared with overall results. As Information security is a specialized area across all industry sectors, the results were analysed on an overall basis and compared with results from the Communications sector in addition to the CEOs and executives. Analysis of the data by organization was not undertaken as this was raised as a confidentiality issue during consultation. Although the data was not analysed by economy or country, there were significantly larger numbers of responses from two economies. For this reason, additional data analysis was undertaken to ensure that the results were not skewed by these anomalies. This was done by excluding the anomalous results and running reports on the remaining data. Comparison of the new tables with the overall results showed that the findings were almost identical. This verified the reliability of the overall findings.

It is important to consider the results in accordance with the level of representation from the particular industry sector(s) or occupational group. For example, the highest percentage of responses (35%) was received from the Government services sector. The data spread in this group showed that the main occupational groups were represented. Although respondents are expressing their personal views, certain conclusions can reasonably be drawn from the results from this sector. On the other hand the percentage of responses from other sectors such as Food supply are quite low and results should not be interpreted as reflecting the views of the entire sector.

It should also be noted that rounding has been applied to the percentage results in some of the tables. As a result, the total for results in some tables will not be exactly 100%.

Reporting and communicating results

The flexibility of the survey tool enabled accurate information to be made available at any time to those involved in the project.

During the project regular project update emails were sent to key contact points and their deputies. Leading up to the survey this occurred on a weekly basis. During the survey these update emails were sent fortnightly and the key contact points were asked to provide fortnightly activity reports. The project management group was copied in on correspondence.

At the completion of the survey, the project team analysed the survey data and prepared this report on the results and possible follow-up activities. The report contains a number of recommendations that are based on the survey results and reflect the views of respondents. These recommendations are for consideration and do not necessarily reflect the views of APEC, Standards Australia or the consensus view of APEC Member Economies. A disclaimer has been included at the beginning of this report.

The draft report was circulated to the key contact point group by email for comment prior to finalization. It was also circulated to 496 survey respondents who provided an email address. The draft findings from the report were presented by Standards Australia to the APEC Business Advisory Council in Wellington, New Zealand 10-12 February 2009, the Sub-Committee on Standards and Conformance in Singapore 24-25 February 2009, and the 32nd meeting of PASC 1-2 April 2009 in Hobart, New Zealand. A presentation on the draft findings was also made to the ISO/IEC/ITU-T Strategic Advisory Group on Security 10-11 March 2009. The draft report was circulated for comment to members of ABAC, SCSC, non-APEC members of PASC and the ISO/IEC/ITU-T Strategic Advisory Group on Security. The APEC Secretariat was also provided with a copy of the draft report.

The comment period closed on 31 March 2009. There was minimal feedback received comprising two additional suggestions from one respondent and comments on the recommendations from ABAC. The two additional suggestions have been mentioned in this final report and the recommendations have been modified to better reflect the respective roles of ABAC and SCSC. The minimal commentary received indicated that the draft report was satisfactory therefore this final report was prepared for publishing.

9. Project overview

There were 539 survey responses in total and 513 of these were complete in terms of answering all mandatory questions. The remaining 26 respondents partially completed the survey and this data was included in the overall results. Of the 26 partially completed responses 7 omitted only one mandatory question on the last page of the survey.

Overall the data is balanced in terms of representation by gender, organizational role and sector.

Respondents by gender

Respondents were requested to indicate their gender as reporting by gender is a requirement for APEC funded projects. The gender breakdown for respondents was 21% female and 79% male.

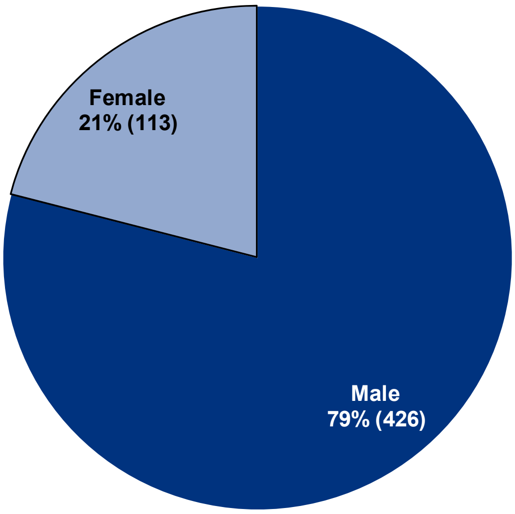


FIGURE 4 RESPONDENTS BY GENDER

Respondents by organizational role

CEOs (4%) and executives (12%) were well represented in the survey. This result is significant as the importance of executive buy-in / commitment for implementation of security standards was highlighted in survey responses. Figure 5 shows that 28% of respondents identified themselves as managers and 22% of respondents were technical specialists. This proportion is actually higher due to some technical specialists choosing the 'Other' category.

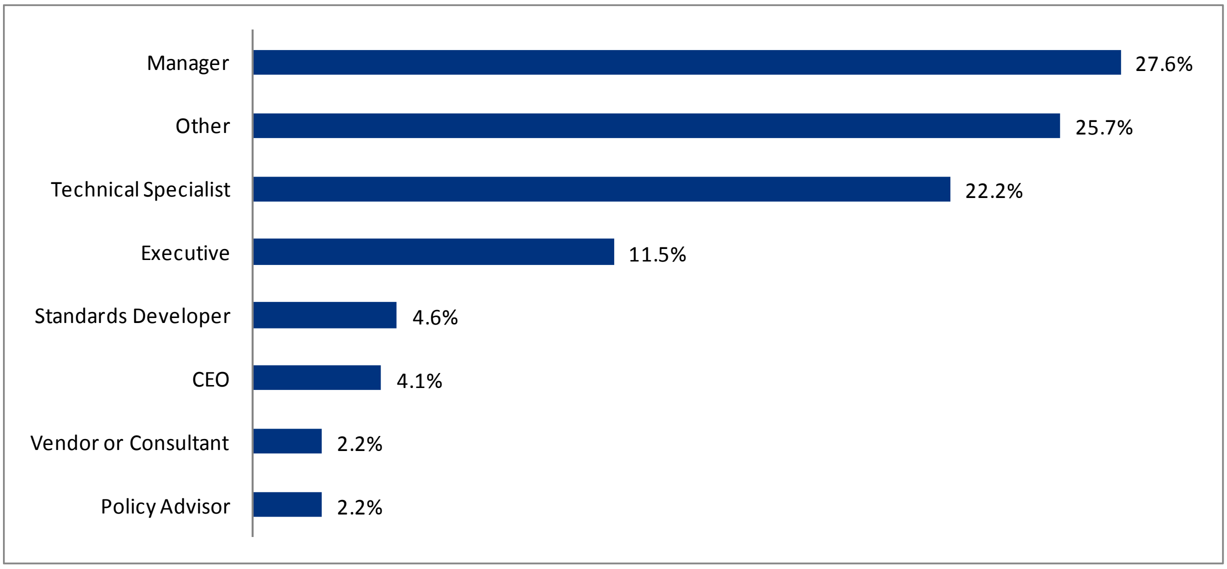


FIGURE 5 RESPONDENTS BY ORGANIZATIONAL ROLE

Respondents by sector

All major sectors were represented in the survey with the highest number of responses from Government services (35%), Energy (9%) and Finance (9%). Of the 17% of respondents who chose the 'Other' category, many individuals would fit under the list of choices provided. The large response from government is due to the fact that in many economies critical infrastructure is owned and operated by government.

As mentioned in the methodology section, the level of representation by sector should be considered when drawing any conclusions from the results by sector. It is possible to reach reasonable conclusions when there is a sufficiently high level of representation from a particular sector.

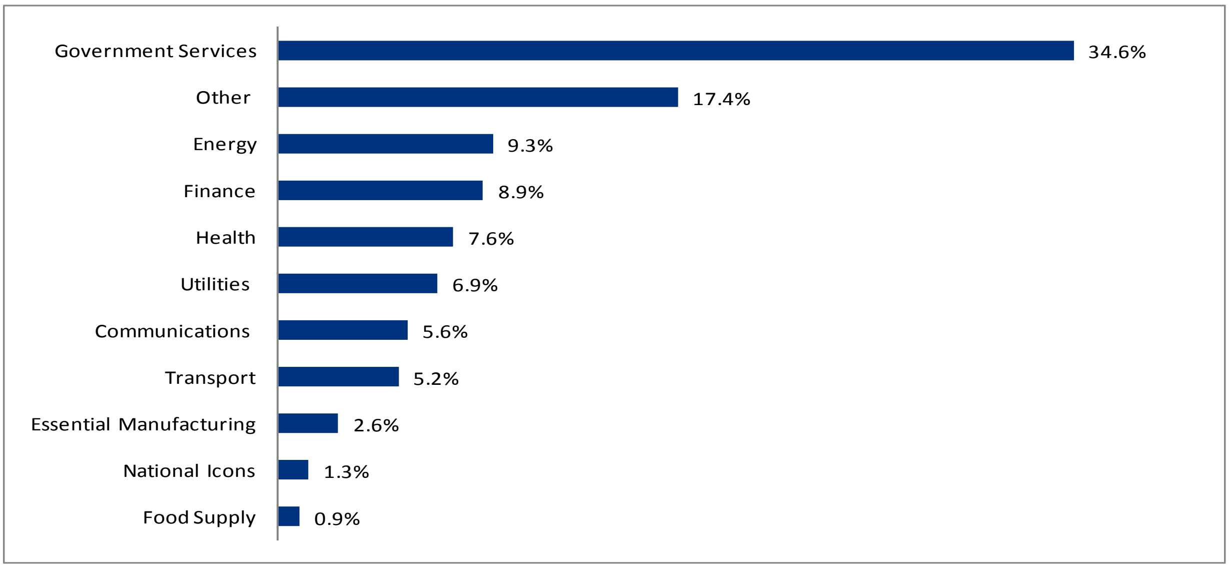


FIGURE 6 RESPONDENTS BY SECTOR

Respondents by role within organization and sector

Comparison of roles by sector shows that the views of CEOs and / or executives were represented in the results for all major sectors. There is also a high level of representation from managers across the sectors. Respondents from the main occupational groups are represented to some extent across most sectors. Some sectors have low or zero percentages for particular organizational roles and this should be considered when interpreting results. Low percentages are to be expected for particular roles such as CEOs and consultants. In other cases, this reflects the representation level by sector. For example, as the Food supply sector is less that 1% of the survey population, it is unlikely that all roles would be represented for this group.

Sector	CEO	Executive	Manager	Technical Specialist	Policy Advisor	Standards Developer	Vendor or Consultant	Other
Communications (e.g. telecommunications, IT, postal services)	7%	3%	43%	13%	3%	10%	3%	17%
Energy (e.g. gas, electricity, petroleum fuels)	6%	6%	32%	28%	2%	2%	2%	22%
Essential Manufacturing	0%	29%	43%	14%	7%	0%	0%	7%
Finance	0%	21%	38%	8%	0%	2%	4%	27%
Food Supply	0%	20%	20%	40%	0%	0%	0%	20%
Government Services	3%	8%	17%	32%	4%	5%	1%	31%
Health	2%	10%	17%	20%	0%	5%	0%	46%
National Icons (e.g. buildings, cultural, sport and tourism)	0%	29%	57%	0%	0%	0%	14%	0%
Other	7%	16%	26%	17%	1%	4%	4%	24%
Transport	0%	15%	62%	8%	0%	8%	0%	8%
Utilities (e.g. water, water waste management)	11%	8%	35%	24%	0%	0%	5%	16%

FIGURE 7 RESPONDENTS BY ROLE WITHIN THEIR ORGANIZATION AND SECTOR

10. Security issues and solutions

Respondents were asked to choose the top security issue for their sector then suggest a solution. The aim was to identify the common security concerns across sectors and gain insight into possible solutions.

This was a non-mandatory question and 514 respondents identified an issue. There were 285 solutions suggested overall, however some respondents commented in the 'additional comments' area of this section.

The top 4 issues chosen by respondents were Information / data (20%), Funding (18%), Resources (14%) and Personnel (workforce) (13%). Due to the volume of information, this overview is limited to proposed solutions to these 4 top issues.

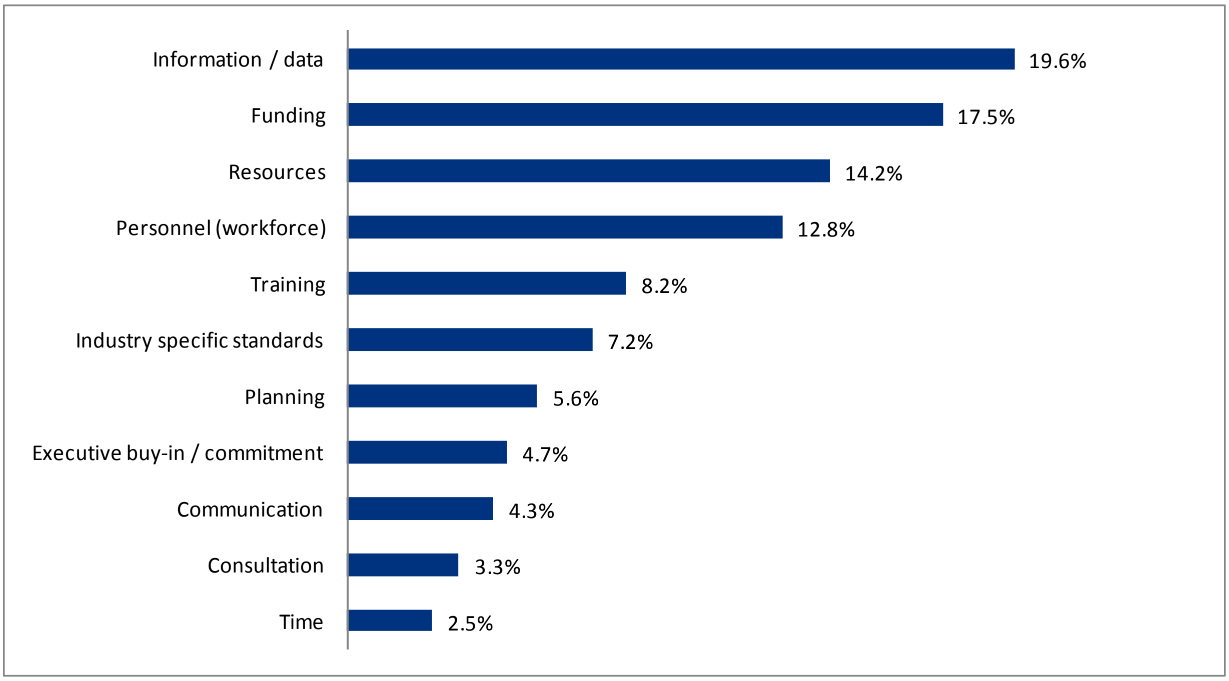


FIGURE 8 COMMON SECURITY ISSUES AND CONCERNS

Information / data

There were 51 solutions suggested for information / data issues. These included improved access to security intelligence to better understand the nature of security threats. Respondents also identified a need for better tools (anti-virus programs, operating systems, encryption methods, etc.), policies, procedures, firewalls, standardized encryption and systematic inventory and management of asset data and information through effective information management systems.

A suggestion was also made to conduct employee and user awareness to prevent information theft and system breaches. There were also references to the need for training and sufficient funding.

One respondent suggested the establishment of *"guidelines which will cover the handling of information/data from the source all the way to the handlers and users, within or outside of the Corporation."*

Information sharing between the owners and operators of critical infrastructure and the Government was seen as a key challenge by a respondent who suggested that this *"can be addressed by developing and agreeing to information sharing agreements that contribute to a common understanding of what happens to the data at all stages of the information sharing process, how information is to be handled and stored, who has access to the information and the procedures for dealing with any problems or disputes, should they arise*."

Another respondent commented that the threat of *"an external attack with ever changing software and external interactions mean that this is an evolving area".*

There were also suggestions made about specific technological solutions, however these are outside the scope of this project. Other solutions proposed were the creation of a lead agency and / or a common platform for sharing intelligence and best practices. As one respondent commented, *"It would be nice to know what works and what doesn't at other critical infrastructures".* Respondents also raised concerns about the protection of sensitive information shared in inter-agency coordination. These responses illustrate the need for a common data format and set of procedures to enable data to be securely shared between organizations. An example of this is the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) in Australia. Although the TISN is a national network, this is a proven model that could be applied on a regional level.

Funding

Proposed solutions to funding issues included internationally benchmarked industry-specific standards, effective planning and budgeting, liquidity management, government securities and grants. Suggestions were also made to explore other sources of funding such as public / private partnerships. Specific allocation in annual budgets was also suggested. One respondent thought that the longer term effects of security issues should be highlighted in funding negotiations. Funding for research was also raised as an issue and the solution suggested was to *"Allow/require colleges/universities 'to the table' for grants."*

References were also made to funding being tightly-regulated and not well-coordinated. Delays in funding payments have also impacted on projects and one individual suggested allowing organizations to:

> *"hold funding in trust … so payment can be faster and projects can be completed on time".*

A view was also expressed that:

> *"Generally security is the least and last to be funded within an organization. Management and decision makers need to be made more aware of the criticality of the security area."*

Resources

There was some overlap in the responses related to funding and resources and this is understandable as there are clearly inter-linkages between the major issues.

The need for effective planning and systematic control of resources was highlighted in responses. This was seen as particularly important to ensuring that resources are used for the purpose intended. It was stressed that people with responsibility for planning must have the necessary knowledge and expertise. One organization is currently assessing the utilization of technology in relation to reducing dependence on resources, especially in relation to human resources (personnel). Reference was also made to establishing networks and technical exchange forums.

Respondents commented:

> *"Resources encompass human, material and capital requirements to effectively and efficiently implement security policies and procedures for the protection of vital infrastructure. The organization will only provide the necessary resources if it is necessary and within their capability. Therefore, it is a must that risk elimination/reduction processes be suited to the organization's capabilities. There is no single solution as condition/situation varies from site to site."*

> *"Security should be seen as a 'cost of doing business', but is often seen as a cost centre and not taken seriously."*

Personnel

The complexity of this area is highlighted in responses. It is clearly not simply a matter of providing adequate personnel levels. Reference was made to the many challenges associated with recruiting security personnel with appropriate qualifications and professional attitude. Respondents were concerned about raising the profile of the industry and finding ways to attract professionals so that *"people consider it as a career rather than a second job or a job to pay the bills until a real job comes along".*

The difficulty in retaining personnel was an issue for one organization that was finding highly trained personnel were migrating to other countries due to more attractive salaries, conditions and opportunities.

A concern was also raised about *"Aging workforce vs growth" and the "need to invest in training and personnel to sustainable levels".* The respondent suggested solutions of targeted recruitment, apprentice schemes and being an employer of choice. This issue of an aging workforce is currently impacting on other professions.

One respondent suggested the development of security officer qualification guidelines and promoting the adoption of these throughout the industry. The challenge in doing this on a regional level would be to achieve consensus and ensure applicability in the different APEC Member Economies, local settings and industry sectors.

Solutions proposed included higher recruitment standards, appropriate succession planning at all levels, training, sound human resource development programs, automation of security controls and outsourcing. There was an emphasis in responses on the need for a capable and technically competent workforce. The use of volunteers with credentials was suggested as an option for consideration in rural or remote locations. The need for personnel with research skills was also highlighted in responses.

Conclusion

The solutions proposed demonstrate the complexity of the issues impacting on the security of critical infrastructure. It would be more strategic to consider common challenges from a regional perspective, rather than organizations grappling with the issues independently. An initial approach could be to bring CEOs and executives together at a tightly facilitated high-level workshop to prioritize common issues and consider regional strategies. This report provides a sound foundation for structuring the workshop as extensive consultation with industry has already taken place. There is also an opportunity to initiate a project to develop a regional security plan based on the outcomes of the workshop and the results from the survey.

Would the solutions to these issues involve adopting standards?

This was a mandatory question and there were 539 responses. The majority of respondents (82%) considered that solutions to the major issue identified in their sector would involve the adoption of standards.

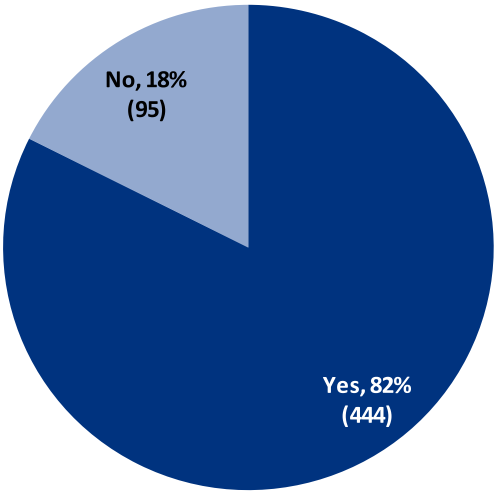


FIGURE 9 SOLUTIONS TO ISSUES AND ADOPTING STANDARDS

Results by sector

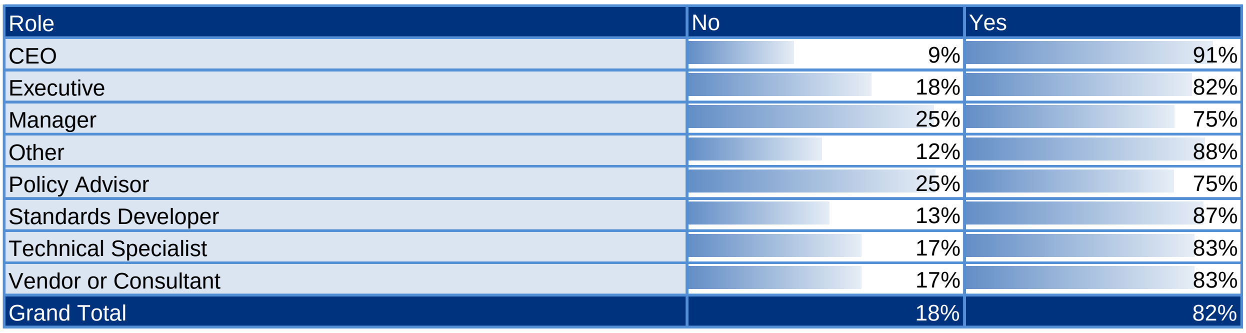
Analysis by sector supports the overall result. The majority of respondents across all sectors considered that the solutions to the major issue in their sector would involve adopting standards. The responses shown in Figure 10 do illustrate varying levels of commitment to standards based solutions. The results for the Transport sector in particular show a high percentage (38%) of respondents do not consider the solutions would involve standards. The negative responses from Health also seem quite high at 22%. Given the risks to the general population associated with these sectors, the results indicate that further investigation is warranted.

Sector	No	Yes
Communications (e.g. telecommunications, IT, postal services)	17%	83%
Energy (e.g. gas, electricity, petroleum fuels)	16%	84%
Essential Manufacturing	7%	93%
Finance	17%	83%
Food Supply	20%	80%
Government Services	19%	81%
Health	22%	78%
National Icons (e.g. buildings, cultural, sport and tourism)	0%	100%
Other	12%	88%
Transport	38%	62%
Utilities (e.g. water, water waste management)	19%	81%
Grand Total	18%	82%

FIGURE 10 SOLUTIONS TO ISSUES AND ADOPTING STANDARDS BY SECTOR

Results by role

Comparison by role sheds even further light on whether respondents do consider standards based solutions to be relevant. Responses from CEOs show that 91% are committed to standards based solutions, however the results indicate that the message is being diluted as it moves through the organization. Figure 11 indicates that 18% of Executives responded in the negative and this increases to 25% for the Manager group and Policy Advisors. It follows that there would be an associated impact on the level of awareness and understanding at an operational level.



Role	No	Yes
CEO	9%	91%
Executive	18%	82%
Manager	25%	75%
Other	12%	88%
Policy Advisor	25%	75%
Standards Developer	13%	87%
Technical Specialist	17%	83%
Vendor or Consultant	17%	83%
Grand Total	18%	82%

FIGURE 11 SOLUTIONS TO ISSUES AND ADOPTING STANDARDS BY ROLE

Conclusion

The analysis indicates the necessity to raise awareness of the relevance of standards, especially at technical and operational levels. CEOs and executives may also wish to consider strategies to address communication issues within organizations.

Recommendations:

- SCSC to consider the creation of protocols to enable data to be securely shared between organizations, such as those established for the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) in Australia.

  If such protocols are already in existence, SCSC to consider communicating these to the owners and operators of critical infrastructure in the region.
- ABAC to consider liaising with APEC (SCSC) on holding a high-level workshop to allow CEOs and executives across the region an opportunity to prioritize common security issues and consider regional strategies.

  An outcome of this workshop could be the development of a regional security plan, based on the workshop outputs and the results from this survey.
- SCSC to consider engaging with industry bodies to develop a set of security officer qualification guidelines to raise standards and attract professionals to the industry. These guidelines would need to be promoted for adoption throughout the region.
- SCSC to consider introducing education and awareness raising programs in the region to ensure that personnel at technical and operational levels understand the importance of standards to the protection of critical infrastructure. The programs could initially be targeted to particular sectors, such as transport and health, and linked to capacity building.

11. Understanding the impact from disruption to services

The following questions assess respondents' knowledge of the systems in place to protect their organization and the impact on customers and suppliers should these systems fail.

How well do you understand the systems that are in place to protect your organization when there is a significant disruption to normal services?

This was a mandatory question and there were 539 responses. Figure 12 shows that 27% of respondents considered they understood these systems 'very well'[1] and 46% 'well'. The majority of respondents were therefore relatively confident about their understanding of these systems, although this could be improved. There were 7% of respondents who indicated that they did not understand these systems well.

[1] Please note that the scale on this and the following question runs as follows: very well, well, neutral, not well and unsure.

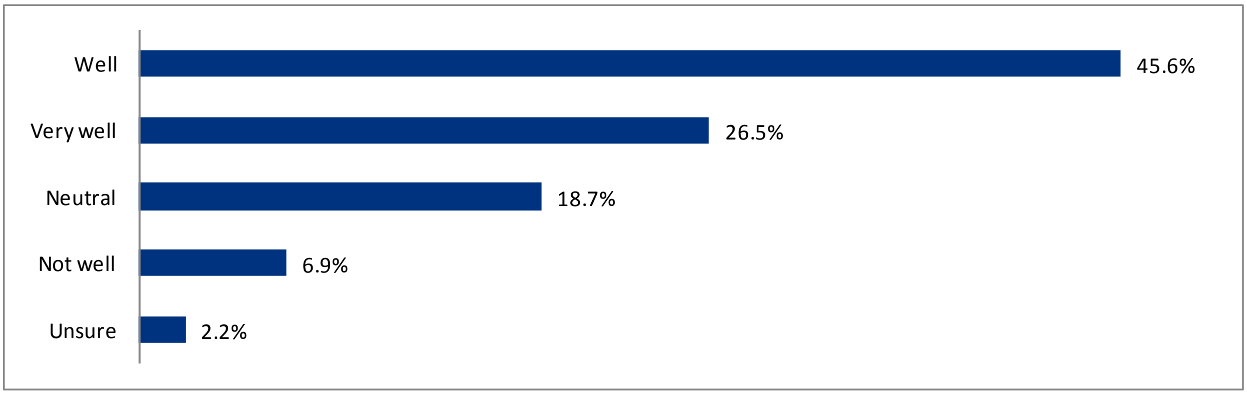


FIGURE 12 UNDERSTANDING OF THE SYSTEMS THAT ARE IN PLACE TO PROTECT ORGANIZATIONS

Results by sector

Analysis by sector (shown in Figure 13) supports the overall result. The majority of respondents across all sectors considered that they understood these systems either 'well' or 'very well'. Certain sectors had a high level of confidence, such as Energy and Food supply. A significant proportion of respondents from certain sectors indicated 'not well', particularly in the areas of Essential manufacturing, Health and National icons. As in the overall results, there was generally a higher percentage of respondents indicating they understood these systems 'well', rather than 'very well', with the exception of the National icons sector. This shows that the level of understanding could be improved across all sectors.

Sector	Unsure	Not well	Neutral	Well	Very well
Communications (e.g. telecommunications, IT, postal services)	0%	3%	20%	43%	33%
Energy (e.g. gas, electricity, petroleum fuels)	0%	4%	8%	60%	28%
Essential Manufacturing	0%	14%	21%	50%	14%
Finance	2%	6%	10%	52%	29%
Food Supply	0%	0%	20%	60%	20%
Government Services	3%	7%	23%	47%	20%
Health	0%	12%	24%	39%	24%
National Icons (e.g. buildings, cultural, sport and tourism)	0%	29%	0%	14%	57%
Other	4%	5%	16%	43%	32%
Transport	0%	4%	19%	42%	35%
Utilities (e.g. water, water waste management)	3%	5%	24%	35%	32%
Grand Total	2%	7%	19%	46%	27%

FIGURE 13 UNDERSTANDING OF THE SYSTEMS THAT ARE IN PLACE TO PROTECT ORGANIZATIONS BY SECTOR

How well do you understand the impact on your organization's customers and suppliers if there is a significant disruption to normal services?

This was a mandatory question and there were 539 responses. Figure 14 shows that 33% of respondents considered that they understood these systems 'very well' and 46% 'well'. This indicates that the majority of respondents were relatively confident about their knowledge in this area. There were 4% of respondents who were not confident about their level of understanding. As in the results for the previous question, a higher proportion of respondents indicated they understood these systems 'well', rather than 'very well'. The overall level of understanding in this area could also be improved.

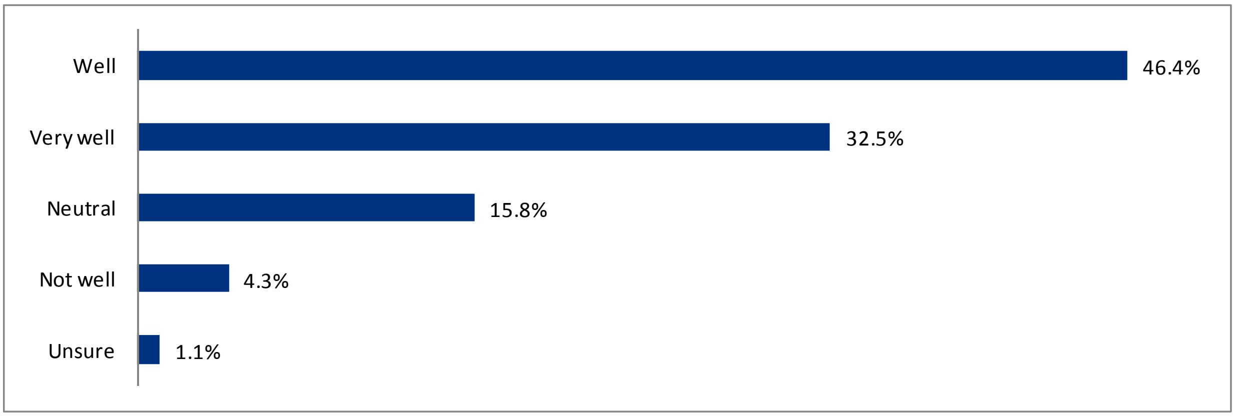
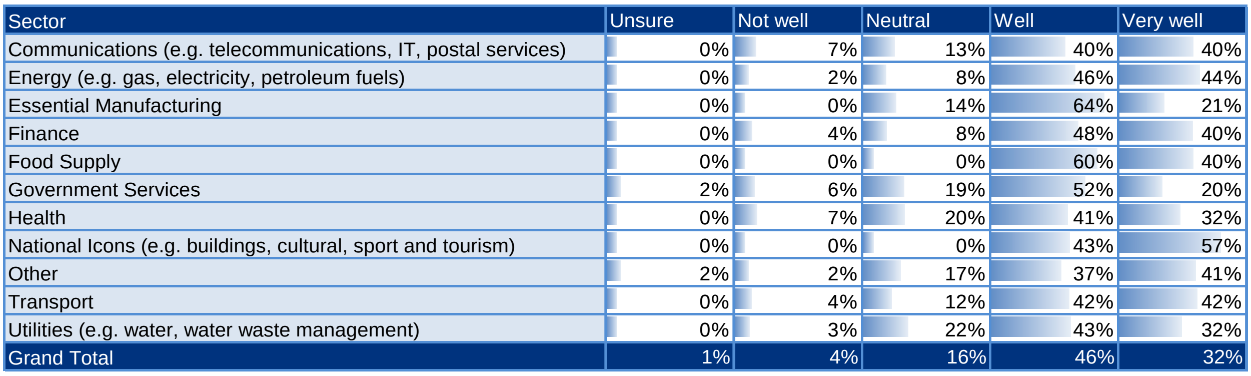


FIGURE 14 UNDERSTANDING OF THE IMPACT ON ORGANIZATION'S CUSTOMERS AND SUPPLIERS OF A SIGNIFICANT DISRUPTION

Results by sector

Analysis by sector shown in Figure 15 supports the overall result. The majority of respondents across all sectors considered that they understood the impact on customers and suppliers either 'well' or 'very well', however this could be improved. In certain sectors the level of understanding is quite high, such as Essential manufacturing, Food supply and National icons. There was a higher proportion of respondents indicating 'not well' in the Communications, Health and Government services sectors. A lack of understanding of the impact on customers and suppliers is a concern, even when the proportion of responses indicating 'not well' is low. Comparison of the results for 'well' and 'very well' by sector shows that the breakdown varies significantly. For example, although the level of understanding is quite high in the Essential manufacturing sector, a much higher proportion of respondents indicate 'well', rather than 'very well'.



Sector	Unsure	Not well	Neutral	Well	Very well
Communications (e.g. telecommunications, IT, postal services)	0%	7%	13%	40%	40%
Energy (e.g. gas, electricity, petroleum fuels)	0%	2%	8%	46%	44%
Essential Manufacturing	0%	0%	14%	64%	21%
Finance	0%	4%	8%	48%	40%
Food Supply	0%	0%	0%	60%	40%
Government Services	2%	6%	19%	52%	20%
Health	0%	7%	20%	41%	32%
National Icons (e.g. buildings, cultural, sport and tourism)	0%	0%	0%	43%	57%
Other	2%	2%	17%	37%	41%
Transport	0%	4%	12%	42%	42%
Utilities (e.g. water, water waste management)	0%	3%	22%	43%	32%
Grand Total	1%	4%	16%	46%	32%

FIGURE 15 UNDERSTANDING OF THE IMPACT ON ORGANIZATION'S CUSTOMERS AND SUPPLIERS OF A SIGNIFICANT DISRUPTION BY SECTOR

Conclusion

The analysis shows that the level of understanding in these areas could be improved on an overall level and within the various sectors. This could be addressed by including specific modules in the education and awareness programs that were recommended earlier in this report. CEOs and executives may also wish to consider organizational strategies to raise the level of understanding in these areas.

12. Funding and development of standards

The following questions assess the level of interest in funding and /or participation in the development of standards critical to the security of critical infrastructure in the region.

Would your organization help to fund the development of standards that are considered critical to the security of your sector?

This was a mandatory question and there were 539 responses.

Overall results

Figure 16 shows that 24% of respondents considered their organization would[2] help to fund the development of standards and 35% thought this was a possibility. There were 18% of respondents who considered this was not a possibility or unlikely.

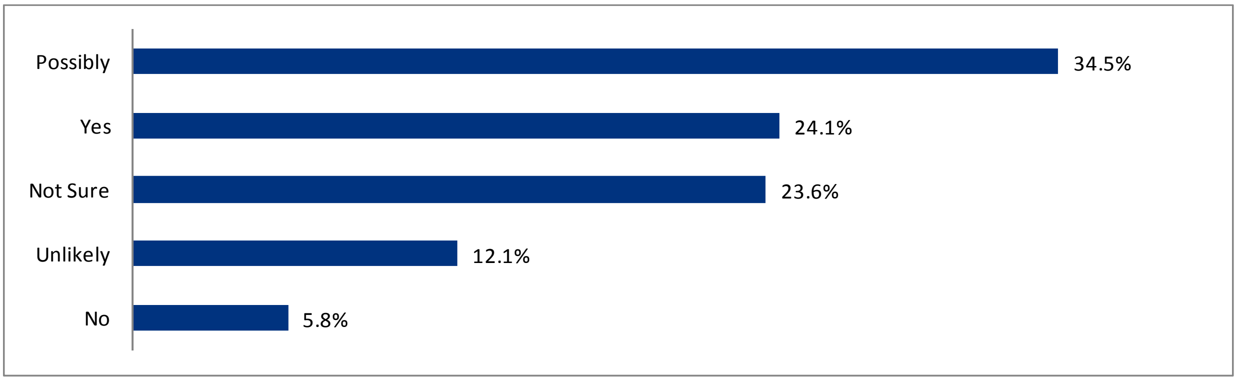


FIGURE 16 FUNDING STANDARDS DEVELOPMENT

Results by sector

Analysis by sector (shown in Figure 17) supports the overall result. The majority of respondents considered their organization would help to fund the development of standards or that this was a possibility. There are variations in results indicating differing levels of interest. The Energy, Finance and Government services sectors show the highest level of interest based on the 'yes' responses. The proportion of 'unlikely' responses from the Energy sector is however quite high at 18%. The highest proportion of 'unlikely' responses is from the Transport sector. Given the earlier results for Transport in relation to standards based solutions for issues, this lower level of interest may be related to perceptions in this sector about the relevance of standards. This may also apply to the results for Health, although Health may also be reflected in the results for Government services.

[2] Please note the scale on this and the following question runs as follows: yes, possibly, not sure, unlikely and no.

Sector	No	Unlikely	Unsure	Possibly	Yes
Communications (e.g. telecommunications, IT, postal services)	3%	10%	20%	47%	20%
Energy (e.g. gas, electricity, petroleum fuels)	0%	18%	10%	40%	32%
Essential Manufacturing	0%	14%	43%	36%	7%
Finance	4%	10%	31%	23%	31%
Food Supply	0%	0%	20%	60%	20%
Government Services	5%	12%	23%	29%	30%
Health	17%	15%	27%	34%	7%
National Icons (e.g. buildings, cultural, sport and tourism)	0%	14%	29%	43%	14%
Other	6%	11%	28%	36%	19%
Transport	12%	23%	15%	35%	15%
Utilities (e.g. water, water waste management)	5%	3%	22%	49%	22%
Grand Total	6%	12%	24%	35%	24%

FIGURE 17 FUNDING STANDARDS DEVELOPMENT BY SECTOR

Results by role

The results by role support the overall results. Figure 18 shows that the groups most open to funding standards development, are CEOs, policy advisors and standards developers. Support for funding standards lessens in the executive and manager groups. The proportion of 'unlikely' responses from standards developers is also interesting, although this is balanced by a very high proportion (48%) of 'yes' responses.

Role	No	Unlikely	Unsure	Possibly	Yes
CEO	5%	5%	23%	36%	32%
Executive	0%	19%	21%	37%	23%
Manager	5%	18%	24%	36%	16%
Other	9%	6%	31%	28%	27%
Policy Advisor	0%	8%	17%	33%	42%
Standards Developer	0%	13%	13%	26%	48%
Technical Specialist	8%	8%	20%	38%	27%
Vendor or Consultant	8%	33%	8%	50%	0%
Grand Total	6%	12%	24%	35%	24%

FIGURE 18 FUNDING STANDARDS DEVELOPMENT BY ROLE

Conclusion

It does appear that there may be viable alternative funding streams for standards development in critical areas. Suggestions to explore private/public partnerships made by respondents in the survey may warrant further investigation. This could apply in the Asia-Pacific region more generally and to individual APEC Member Economies. As the results indicate that the CEOs are supportive towards funding standards development, this is another potential topic for the proposed workshop.

Recommendation:

- SCSC to consider exploring alternative sources of funding, such as private / public partnerships, for areas of standards development deemed critical to the security of particular sectors within the Asia-Pacific region.

Would your organization participate in the development of standards that are considered critical to the security of your sector?

This was a mandatory question and there were 539 responses. Of these, 44% of respondents considered that their organization would participate in the development of critical standards and 35% thought this was a possibility. This was not considered a possibility or unlikely by 6%.

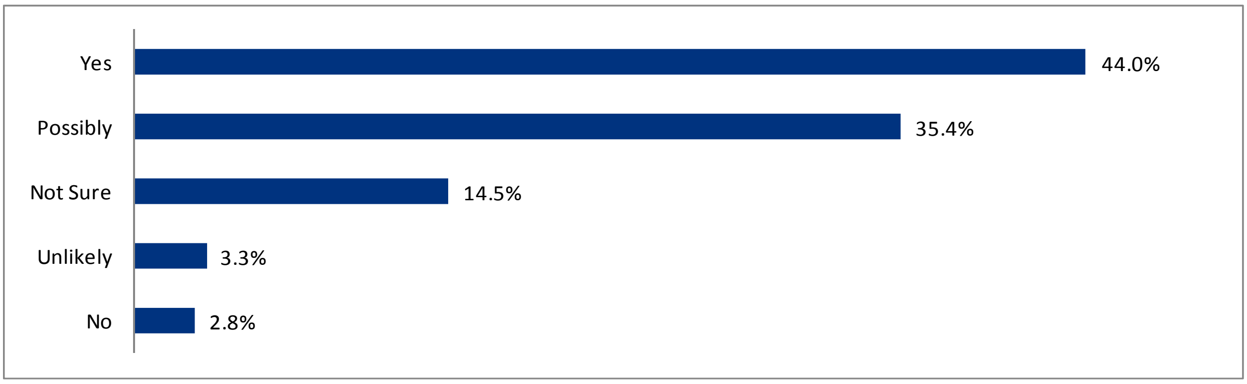
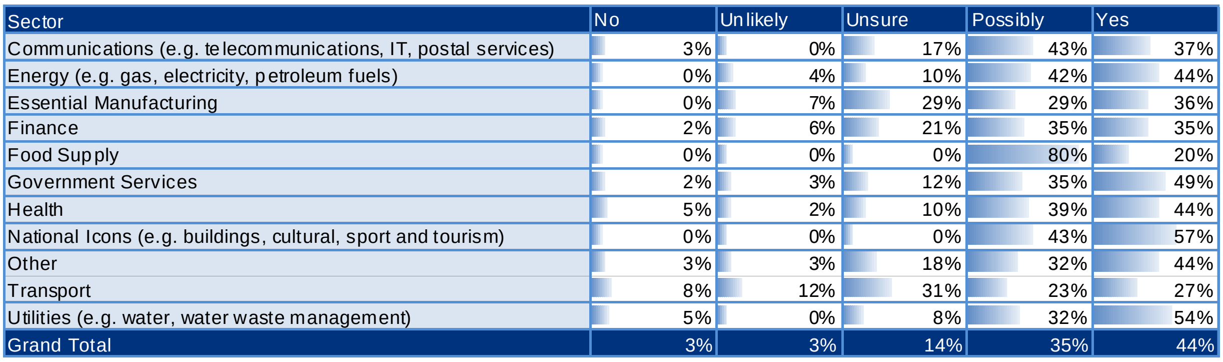


FIGURE 19 PARTICIPATION IN STANDARDS DEVELOPMENT

Results by sector

An analysis across sectors, shown in Figure 20, supports the overall result. The majority of respondents across all sectors considered their organization would participate in the development of standards critical to security in their sector or this was a possibility. The results indicate quite a high level of interest, particularly from the National icons, Utilities and Government services areas. There is also quite a high level of interest in this area from the Health sector. The proportions of 'no' and 'unlikely' responses from the Transport sector are again high in comparison with other sectors, indicating a lower level of support for standards development.

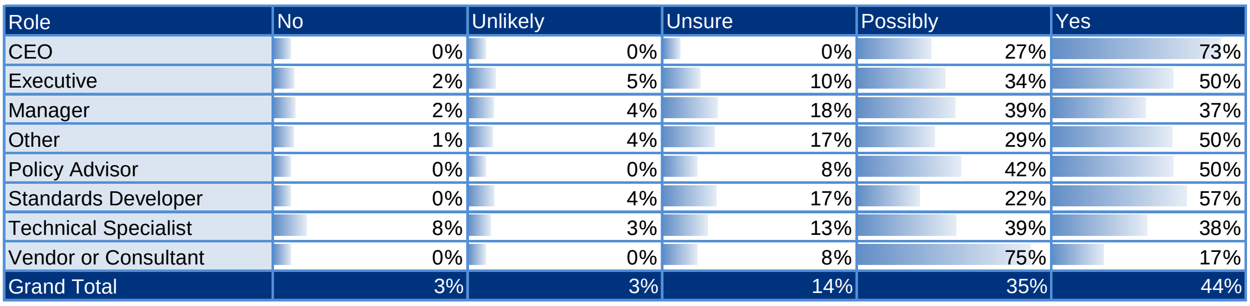


Sector	No	Unlikely	Unsure	Possibly	Yes
Communications (e.g. telecommunications, IT, postal services)	3%	0%	17%	43%	37%
Energy (e.g. gas, electricity, petroleum fuels)	0%	4%	10%	42%	44%
Essential Manufacturing	0%	7%	29%	29%	36%
Finance	2%	6%	21%	35%	35%
Food Supply	0%	0%	0%	80%	20%
Government Services	2%	3%	12%	35%	49%
Health	5%	2%	10%	39%	44%
National Icons (e.g. buildings, cultural, sport and tourism)	0%	0%	0%	43%	57%
Other	3%	3%	18%	32%	44%
Transport	8%	12%	31%	23%	27%
Utilities (e.g. water, water waste management)	5%	0%	8%	32%	54%
Grand Total	3%	3%	14%	35%	44%

FIGURE 20 PARTICIPATION IN STANDARDS DEVELOPMENT BY SECTOR

Results by role

The results for CEOs are even more striking in relation to this question. In Figure 21 73% of CEOs would be interested in being involved in standards development, compared to 50% of executives and 37% of managers. The executives and managers do appear to be more open to being consulted, nevertheless the level of interest is diminishing in comparison with the CEO results. Across all organizational roles, there were strong levels of support for participation in standards development and only a low proportion of ‘no’ and ‘unlikely’ responses.



Role	No	Unlikely	Unsure	Possibly	Yes
CEO	0%	0%	0%	27%	73%
Executive	2%	5%	10%	34%	50%
Manager	2%	4%	18%	39%	37%
Other	1%	4%	17%	29%	50%
Policy Advisor	0%	0%	8%	42%	50%
Standards Developer	0%	4%	17%	22%	57%
Technical Specialist	8%	3%	13%	39%	38%
Vendor or Consultant	0%	0%	8%	75%	17%
Grand Total	3%	3%	14%	35%	44%

FIGURE 21 PARTICIPATION IN STANDARDS DEVELOPMENT BY ROLE

Conclusion

With the exception of the Transport sector, there is a high level of interest in relation to participation in standards development. In general, consultation with industry would be expected when developing and revising standards. There is however an important message here for standards developers to involve owners and operators of critical infrastructure and support systems in the development and revision of standards that are critical to security in their sectors. The variation in results for CEOs, executives and managers may warrant further consideration in the proposed workshop.

13. Common approaches supporting security processes

The purpose of this section of the survey was to investigate approaches that are common to supporting security processes across sectors and within the region. The difference in total number of responses to mandatory questions from previous sections in the report is due to skipped responses. As mentioned in the methodology section of this report, skipped responses are due to partially completed surveys.

How important do you believe common and agreed approaches, standards, methods, protocols and procedures are to improved security?

This was a mandatory question and there were 535 responses. The majority of respondents considered these areas to be ‘very important’[3] (58%) or ‘important’ (38%).

[3] Please note the scale on this and similar questions runs as follows: very important, important, neutral, unimportant and very unimportant.

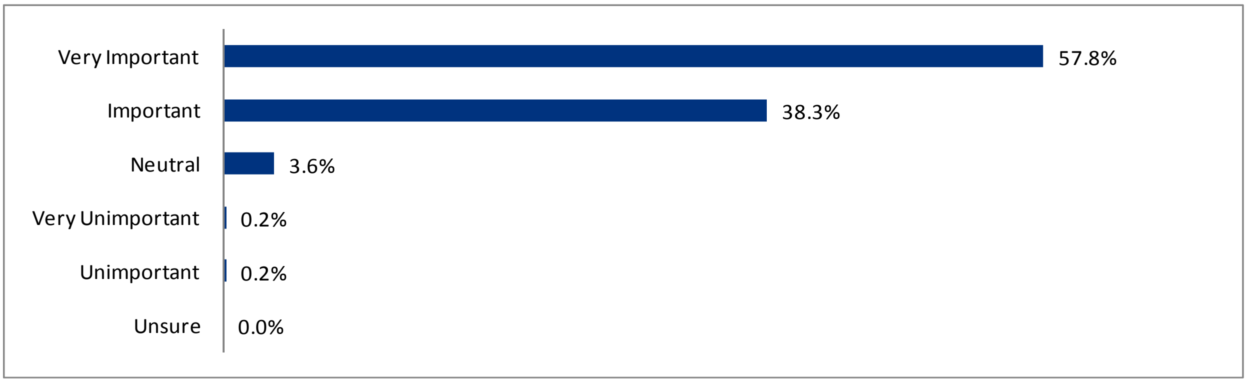


FIGURE 22 IMPORTANCE OF STANDARDS

Results by sector

Comparison by sector supports the overall results. The strongest results were from the National icons and Communications sectors, based on the proportion of 'very important' responses. Very few respondents considered these areas to be unimportant.

Sector	Very unimportant	Unimportant	Neutral	Important	Very important
Communications (e.g. telecommunications, IT, postal services)	0%	0%	0%	27%	73%
Energy (e.g. gas, electricity, petroleum fuels)	0%	0%	2%	40%	58%
Essential Manufacturing	0%	0%	0%	38%	62%
Finance	0%	0%	8%	42%	50%
Food Supply	0%	0%	0%	60%	40%
Government Services	1%	0%	4%	42%	53%
Health	0%	0%	5%	32%	63%
National Icons (e.g. buildings, cultural, sport and tourism)	0%	0%	0%	14%	86%
Other	0%	0%	3%	36%	61%
Transport	0%	0%	4%	38%	58%
Utilities (e.g. water, water waste management)	0%	3%	3%	35%	59%
Grand Total	0%	0%	4%	38%	58%

FIGURE 23 IMPORTANCE OF STANDARDS BY SECTOR

Results by role

The variations between the views of CEOs, executives and managers are again clear in the results. In this question, managers rate the importance level higher than executives and this is an unusual result. Results for policy advisors are in line with the CEO ratings. Across roles, the proportion of respondents considering these areas to be unimportant was almost zero.

Role	Very unimportant	Unimportant	Neutral	Important	Very important
CEO	0%	0%	0%	36%	64%
Executive	0%	0%	5%	48%	48%
Manager	0%	1%	1%	36%	62%
Other	1%	0%	4%	35%	60%
Policy Advisor	0%	0%	8%	25%	67%
Standards Developer	0%	0%	0%	57%	43%
Technical Specialist	0%	0%	4%	41%	55%
Vendor or Consultant	0%	0%	17%	25%	58%
Grand Total	0%	0%	4%	38%	58%

FIGURE 24 IMPORTANCE OF STANDARDS BY ROLE

Conclusion

There was a high level of agreement that common and agreed approaches, standards, methods, protocols and procedures are important to improved security. The results again show variations in commitment and / or awareness below the CEO level. In relation to this question one respondent cautioned that, from a proactive perspective, it is important to avoid cascading failures from weak links to strong links in highly interdependent critical infrastructures.

Within your organization or sector what are the major sources of guidance when developing security products, installations, processes or systems?

This was a mandatory question and there were 535 responses. Respondents could choose multiple answer choices. The percentage rates refer to the percentage of total respondents who chose the particular category.

The major sources of guidance indicated by respondents were international standards (62%), Government guidelines (53%) and national standards (48%) of respondents.

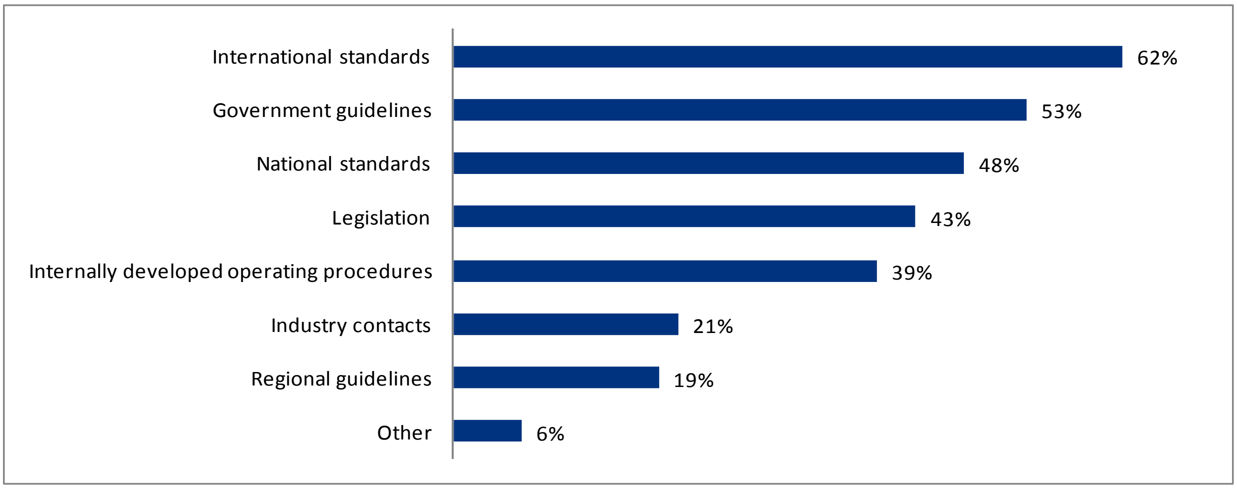


FIGURE 25 SOURCES OF GUIDANCE WHEN DEVELOPING SECURITY SYSTEMS

Results by sector

With the exception of Utilities, the majority of respondents from each sector chose international standards as a major source of guidance. A higher proportion of respondents from Utilities chose national standards. The results by sector show other variations from the overall results. For example, in the Communications sector more respondents chose internally developed operating procedures than Government guidelines. In the Energy sector, more respondents chose national standards than Government guidelines and internally developed operating procedures.

Conclusion

Particular sources of guidance will be more applicable to some sectors than others. Conclusions from the overall results should therefore be considered in accordance with the results for the particular sector (s).

In your experience what has been the outcome of using these major sources of guidance?

This was a mandatory question and there were 535 responses. Overall 50% of respondents indicated the outcome of using these major sources of guidance had been 'some improvements'[4], while 38% considered there had been 'substantial improvements'.

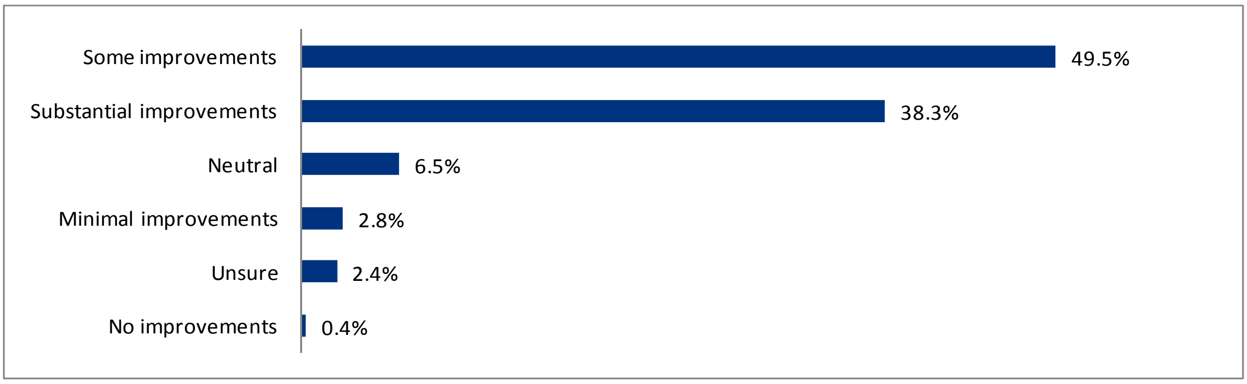


FIGURE 26 OUTCOME OF USING THESE MAJOR SOURCES OF GUIDANCE MATERIAL

Results by sector

Comparison by sector (see Figure 27) supports the overall results. The majority of respondents from all sectors considered that the outcome of using these major sources of guidance had either been 'some improvements' or 'substantial improvements'. The highest proportion of respondents experiencing 'substantial improvements' were from the National icons (57%), Finance (48%) and Communications (47%) sectors. The lowest proportion of respondents indicating an outcome of 'substantial improvements' were from Essential manufacturing (31%), Transport (31%) and Government services (33%).

Conclusion

Further investigation of why using major sources of guidance has not led to substantial improvement for these sectors may be warranted. Transport continues to be highlighted in results as a sector that may benefit from education and awareness raising programs.

[4] Please note that the scale in this question runs as follows: substantial improvements, some improvements, neutral, minimal improvements, no improvements and unsure.

Sector	Unsure	No improvements	Minimal improvements	Some improvements	Substantial improvements
Communications (e.g. telecommunications, IT, postal services)	13%	3%	0%	37%	47%
Energy (e.g. gas, electricity, petroleum fuels)	2%	2%	0%	54%	42%
Essential Manufacturing	0%	0%	8%	62%	31%
Finance	4%	0%	2%	44%	48%
Food Supply	20%	0%	0%	40%	40%
Government Services	8%	0%	3%	53%	33%
Health	0%	0%	0%	56%	39%
National Icons (e.g. buildings, cultural, sport and tourism)	14%	0%	0%	29%	57%
Other	8%	0%	4%	43%	41%
Transport	4%	0%	15%	50%	31%
Utilities (e.g. water, water waste management)	11%	0%	0%	51%	38%
Grand Total	7%	0%	3%	50%	38%

Figure 27 Outcome of using these major sources of guidance material

14. Prioritization of security standards and guidance

In the following sections of the survey, respondents were asked to prioritize standards and other sources of guidance. The standards were organized according to broad and specific categories derived from the Integrated Security Standards Framework that is described earlier in this report. Although the initial intention was to focus solely on standards, the approach was modified to meet the needs expressed by stakeholders during the consultation phase. In particular, it was pointed out that standards are often embedded in legislation and other documents such as policies, procedures and other guidelines. Views were also expressed that the initial approach focused too much on 'hard' security concepts and this did not reflect the full picture. The term 'other sources of guidance' was included to capture this related information.

Respondents were asked to rank each broad category or specific category on a scale from 'very important' to 'very unimportant'. Choice options were also provided on the scale for 'neutral' or 'unsure'. Weightings were then applied to the results to assess the overall level of priority and average scores were calculated. The categories were then sorted in descending order by score. These results were validated by comparison with results by sector and the combined results from the CEO and executive groups. As part of the validation process, comparison was also made with results from the preceding Australian 4(S) survey. It was not possible to map the two sets of results precisely as the Framework had been revised and the methodology was different. The comparison did show that there was some degree of consistency between the two sets of results.

Respondents were also asked to suggest areas that may not have been covered in the various categories. These suggestions were reviewed against the broad and specific categories of standards and other sources of guidance in the Framework that is the basis for the survey. Many of the suggestions for other areas to include under the various categories were well covered in the Framework. This may have been due to a language barrier or respondents completing the survey 'cold' online without first reviewing the supporting documents and PDF version of the survey.

The survey results and review of additional suggestions validated that the Framework is robust and comprehensive in relation to both broad and specific categories of security standards. References to particular standards and documents were included in the inventory of standards and other sources of guidance that formed the basis for a gap analysis.

Prioritization of broad categor ies of security standards and guidance

Respondents were asked to prioritize five broad categories of security standards and other sources of guidance and suggest whether other areas should be included with applicable ratings. This was a mandatory question and 532 responses were received.

Overall results

The highest score was for Governance, strategy and policy (4.53), followed by Risk management (4.52) and Information security (4.49). Personnel security and Physical security had identical scores of 4.33.

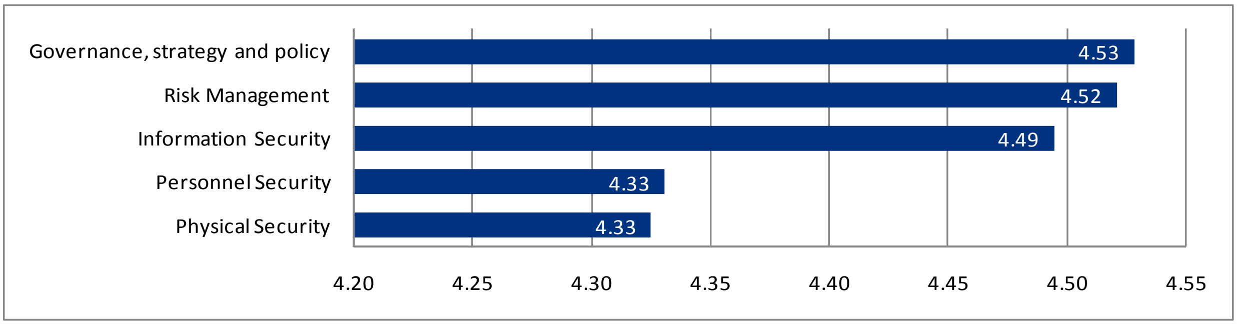


FIGURE 28 PRIORITIZATION OF BROAD CATEGORIES OF SECURITY STANDARDS

Results by CEOs and executives

There were 22 responses from CEOs and 61 responses from executives. Comparison of the overall results with responses from the CEO and executive group shows an almost identical ranking. The highest score is for Governance, strategy and policy (4.64), followed by Risk management (4.57), Information security (4.53), Personnel security (4.34) and Physical security (4.24). The score from this group is higher for Personnel security. It should also be noted that the score for Governance, strategy and policy (4.64) is significantly higher from this group than in the overall results (4.53). This shows the much higher emphasis on this area from the CEO and executive group.

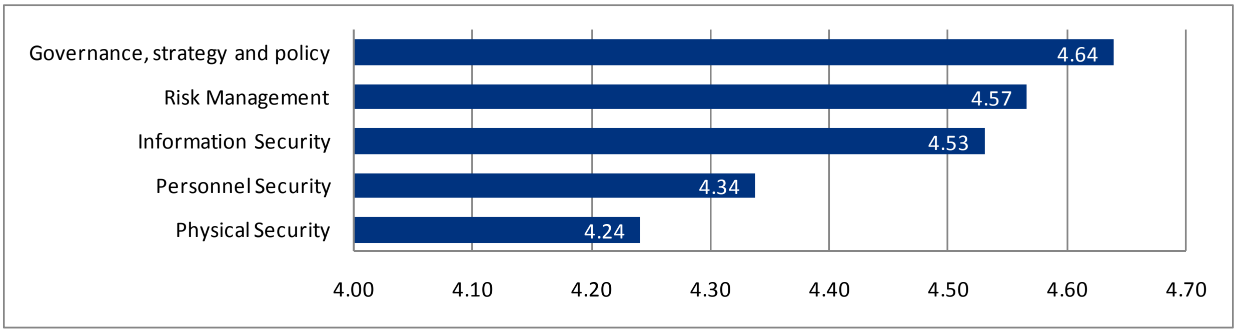
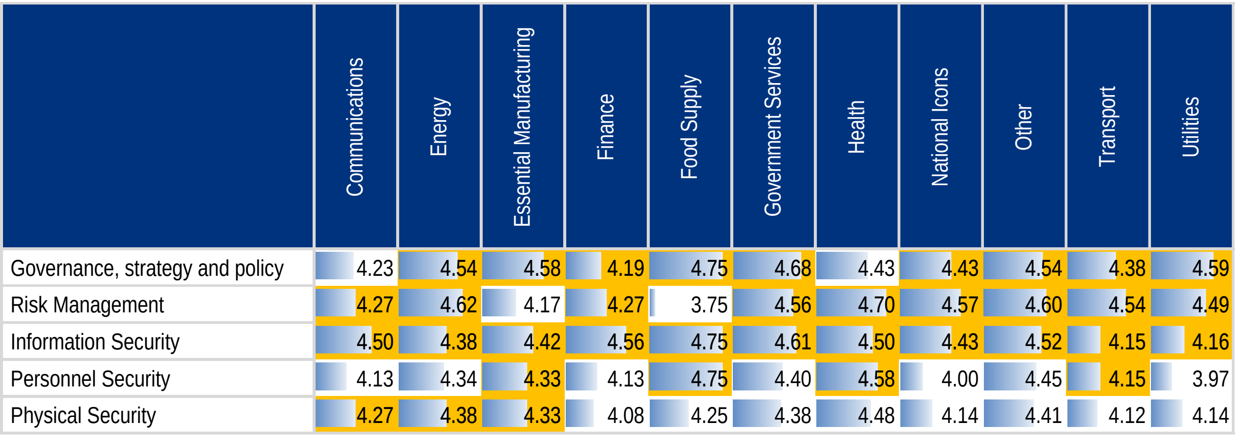


FIGURE 29 PRIORITIZATION OF BROAD CATEGORIES OF SECURITY STANDARDS BY CEOS AND EXECUTIVES

Results by sector

Comparison by sector in Figure 30 shows variations in scores from the overall results. These variations should be considered when drawing conclusions from the overall results that apply to particular sectors. For example, the highest score from Government services for Governance, strategy and policy (4.68) is in line with the overall results, however this is followed by Information security (4.61) and Risk management (4.56). In comparison, the highest score from Health (4.70) and Transport (4.54) sectors is Risk management.



	Communications	Energy	Essential Manufacturing	Finance	Food Supply	Government Services	Health	National Icons	Other	Transport	Utilities
Governance, strategy and policy	4.23	4.54	4.58	4.19	4.75	4.68	4.43	4.43	4.54	4.38	4.59
Risk Management	4.27	4.62	4.17	4.27	3.75	4.56	4.70	4.57	4.60	4.54	4.49
Information Security	4.50	4.38	4.42	4.56	4.75	4.61	4.50	4.43	4.52	4.15	4.16
Personnel Security	4.13	4.34	4.33	4.13	4.75	4.40	4.58	4.00	4.45	4.15	3.97
Physical Security	4.27	4.38	4.33	4.08	4.25	4.38	4.48	4.14	4.41	4.12	4.14

FIGURE 30 PRIORITIZATION OF BROAD CATEGORIES OF SECURITY STANDARDS[5]

Additional suggestions and comments

In relation to the category of Information security, one respondent commented:

> *"My personal point of view favors me to take a more open approach to the access of infrastructure data. I feel that by limiting access and by cocooning the information we are missing out on a whole other set of opportunities. Economic prosperity, crucial planning and environmental accessibility are aspects that are equally important to that of responding to crisis situations.*

[5] Note that the items in yellow in Figure 30 identify the top 3 items chosen by sector. Sometimes more than three items are shown, this occurs where there are multiple equal scores.

> *We would be much better served as a nation to not only limit access to respondents but it is of my view that this limited activity does not stimulate confidence and opportunity. Somehow we must try and strike a balance by opening up 'démocratisé' the access to the data and allow equal opportunity for all to move forward. (important)."*

This is an interesting topic for discussion in the industry and concerns about information sharing were a recurring theme in the survey results.

Further insights were offered by another respondent:

> *"Strategic Planning which incorporates infrastructure limitations. I.e. Towns used to be designed by engineers who knew about flooding, water sources and wastewater disposal. Unfortunately today, the pitfalls of poor town planning are only highlighted when cities physically start to run out of water or flood their streets with sewer. Sustainability. Very important, often overlooked in the past. A sustainability framework should be built into every decision making process. Protection of water rights. Very Important, a global water crisis is very near. Countries will seek to mine other countries for water unless ownership issues are resolved. A global model on the value of water would be very useful. Particularly when you start looking at the water footprint to produce various commodities."*

Strategic planning would fit under the broad category of Governance, strategy and policy, while sustainability is a consideration for Business continuity management under Risk management in the Framework. Issues around protection of water rights are outside the scope of the project however this is another topic for discussion in the industry, along with other environmental considerations.

Conclusion

The average scores for these broad categories are consistent at the overall level and in comparison with results from the CEOs and executives. There are variations in the score rankings when results are analysed by sector.

Overall, respondents rated governance, strategy and policy along with risk management as the key broad areas requiring standards development. This is at odds with the traditional view that standards should only focus on technical issues.

Prioritization of specific security standards and guidance

Respondents were asked to prioritize specific security standards and other sources of guidance. This information was organized by the five broad areas of security standards and other sources of guidance in the previous category. Respondents were also asked to suggest any other specific security standards and other sources of guidance that should be included under each category. These questions were mandatory and the differing number of responses in each category is due to skipped questions in partially completed surveys.

An analysis follows, which compares the scores from the overall results with scores from the combined CEO and executive group and also by sector. As the analysis will show, the overall results are supported by the results from the CEO and executive group and also by sector. There are variations within both these comparative sets of results and this is highlighted in the analysis. The variations in the results from CEOs and executives warrant further investigation and consideration on an organizational and industry level. The results indicate that priorities for CEOs and executives may be quite different from priorities for other areas of the organization(s). There are strategic considerations around ensuring that priorities at executive level are effectively communicated throughout the organization(s) and at operational levels.

Variations by sector should be considered when drawing conclusions from the results for particular sector(s). These no doubt reflect the challenges and priorities for the particular sector(s). Sectorial variations point to the need to tailor or adapt standards to the requirements of particular industries and sectors. This was a recurring theme in the commentary from respondents in relation to the relevance of standards. Consideration should also be given to the level of representation in the survey by role and by sector when interpreting results.

Governance, strategy & policy

Overall results

There were 525 responses to this mandatory question. The highest score was for Effective leadership (4.46), followed by Crisis management (4.41) and Security management (4.40).

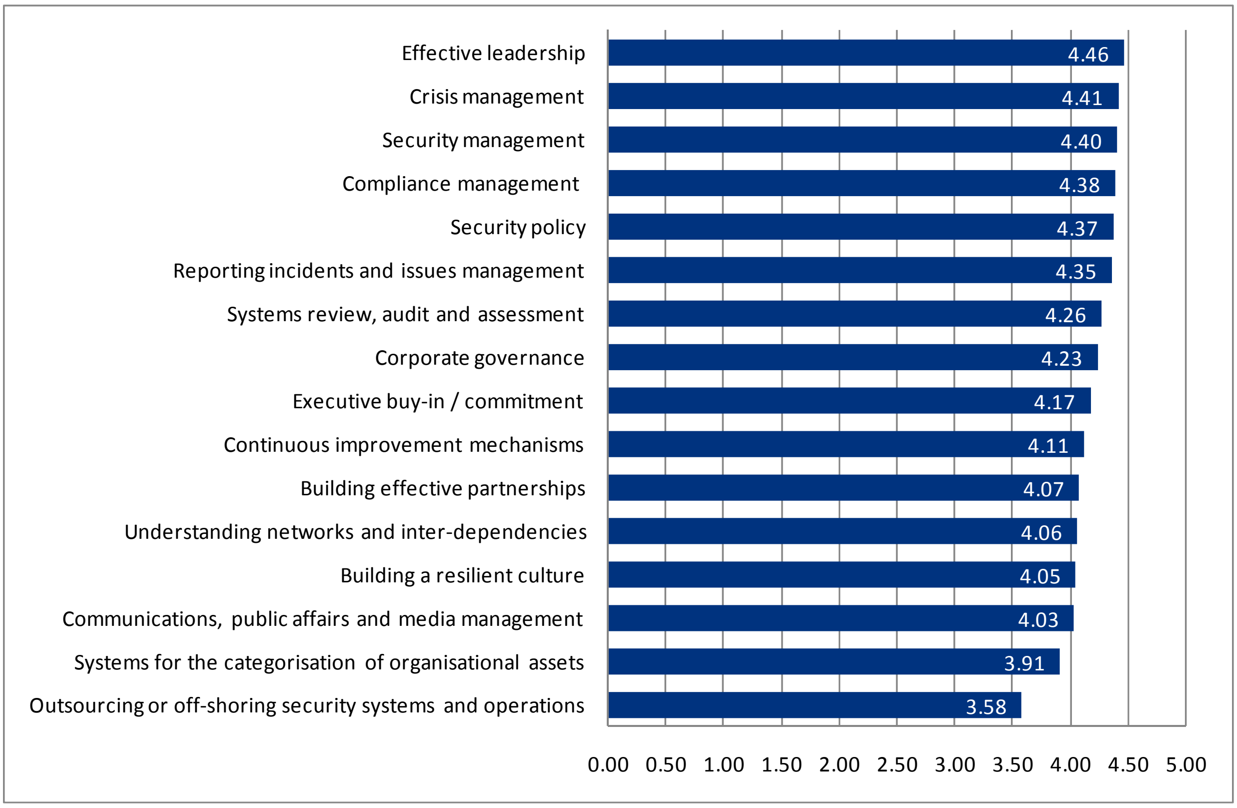


FIGURE 31 PRIORITIZATION OF GOVERNANCE, STRATEGY & POLICY STANDARDS

Results by CEOs and executives

There were 22 responses from CEOs and 60 responses from executives. The highest score for the CEO and executive group was Effective leadership (4.54), followed by Crisis management (4.51), then Reporting incidents and issues management (4.48). There is consistency with the ranking of the two highest scoring categories in the overall results then variations in rankings for other categories. In particular, the CEOs and executives placed much more emphasis on the importance of Reporting incidents and issues management and Corporate governance than shown in the overall results. As this group has overall responsibility for governance, strategy and policy, these results are important. The scores would reflect the group's in-depth knowledge and expertise in relation to this category.

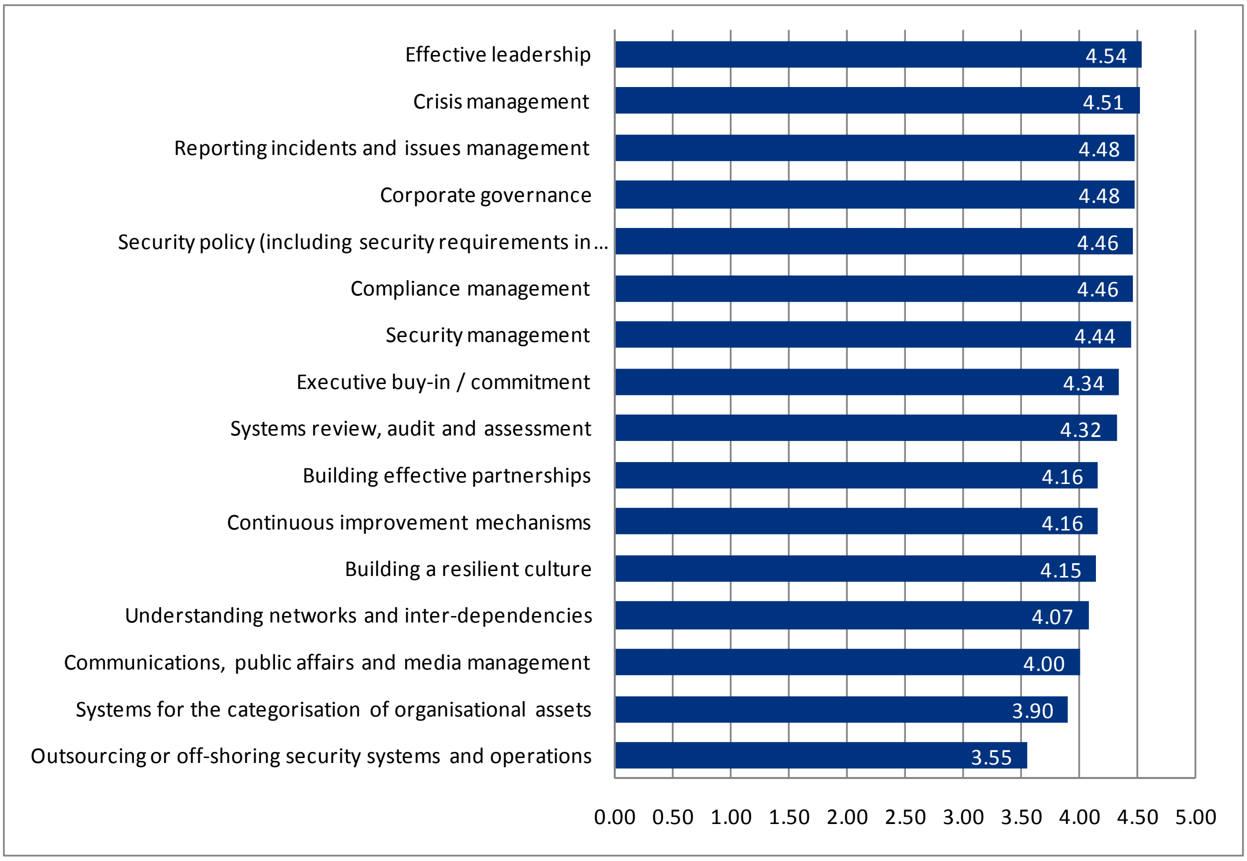


FIGURE 32 PRIORITIZATION OF GOVERNANCE, STRATEGY & POLICY STANDARDS CEOS AND EXECUTIVES

Results by sector

Although the highest scoring categories in the overall results are reasonably reflected in the results for most sectors, there are some significant variations. For example, as illustrated in Figure 33, the highest score for the Finance sector is Security management (4.46), followed by Reporting incidents and issues management (4.44), then Compliance management (4.40). The National icons sector gives identical scores of 4.71 to the three categories of Security management, Reporting incidents and issues management and Executive buy-in / commitment.

	Communications	Energy	Essential Manufacturing	Finance	Food Supply	Government Services	Health	National Icons	Other	Transport	Utilities
Effective leadership	4.37	4.50	4.58	4.27	4.75	4.45	4.56	4.57	4.52	4.60	4.38
Crisis management	4.30	4.54	3.92	4.33	3.75	4.43	4.51	4.57	4.44	4.40	4.32
Security management	4.33	4.58	4.33	4.46	4.25	4.42	4.33	4.71	4.42	4.24	4.14
Compliance management (including legal compliance and reporting to relevant authorities)	4.33	4.36	4.50	4.40	4.00	4.41	4.44	4.43	4.40	4.24	4.32
Security policy (including security requirements in contracts)	4.43	4.48	4.50	4.33	3.75	4.36	4.38	4.43	4.37	4.20	4.30
Reporting incidents and issues management	4.30	4.48	4.33	4.44	4.50	4.31	4.28	4.71	4.43	4.36	4.16
Systems review, audit and assessment	3.93	4.38	4.25	4.23	4.00	4.30	4.31	4.14	4.35	4.12	4.14
Corporate governance	4.10	4.40	4.67	4.25	4.25	4.30	4.15	4.00	4.17	4.32	3.78
Executive buy-in / commitment	4.50	4.36	4.75	4.13	4.25	4.04	4.28	4.71	4.20	3.84	4.05
Continuous improvement mechanisms	3.77	4.24	4.00	4.02	4.50	4.16	4.28	3.71	4.12	3.96	4.08
Building effective partnerships	4.17	4.10	4.33	3.96	4.25	4.11	4.13	4.29	4.12	3.68	3.86
Understanding networks and inter-dependencies	4.07	4.10	3.75	4.02	4.00	4.10	4.03	3.57	4.09	3.84	4.08
Building a resilient culture	4.10	4.22	4.17	3.90	4.25	4.01	4.26	4.00	4.17	4.04	3.57
Communications, public affairs and media management	3.67	4.16	3.67	3.83	4.00	4.13	4.13	3.71	4.04	3.68	4.19
Systems for the categorisation of organisational assets	3.70	3.98	3.42	3.94	3.50	3.92	4.08	3.71	3.98	3.76	3.86
Outsourcing (purchasing) or off-shoring security systems and operations	3.53	3.50	3.67	3.58	3.50	3.79	3.56	2.57	3.49	3.08	3.38

Figure 33 Prioritization of Governance, Strategy & Policy Standards by Sector[6]

Additional suggestions and comments

An additional category of ‘Internal operating procedures’ was suggested for inclusion and this was rated as very important. Although this is not covered in the above list, it is implied in the description of the Framework category. The description in the Framework refers to the necessity for a rigorous system, which would include robust internal operating procedures or standards.

In relation to the inclusion of ‘Building a resilient culture’ in the list, a respondent commented:

> *“Building a culture of high reliability is arguably more important than a resilient culture. Resilience assumes that the risk will not adequately be managed and thus may not put sufficient emphasis on prevention of a surprise. A high reliability culture attempts to prevent the surprise. Aircraft carriers and air*

[6] Note that the items in yellow in Figure 33 identify the top 3 items chosen by sector. Sometimes more than three items are shown, this occurs where there are multiple equal scores.

> *traffic control are examples of socio-technical systems that have achieved high reliability. A shift to high resilience may increase the number of accidents. Take care!"*

This may be another topic for further discussion in the industry. It can be argued that there should be a balance reached of both resilience and high reliability. High reliability can also be seen as an important component of resilience.

Conclusion

The scores for the top three areas in the overall results are supported by the results by CEOs and executives and the results by sector, with some variations. The variations in results from the CEOs and executives are particularly important due to their in-depth knowledge and expertise in this area.

Risk management

Overall results

There were 522 responses to this mandatory question. The highest score was Emergency management (4.60), followed by Risk management (4.54) and Command, control and communications (4.36).

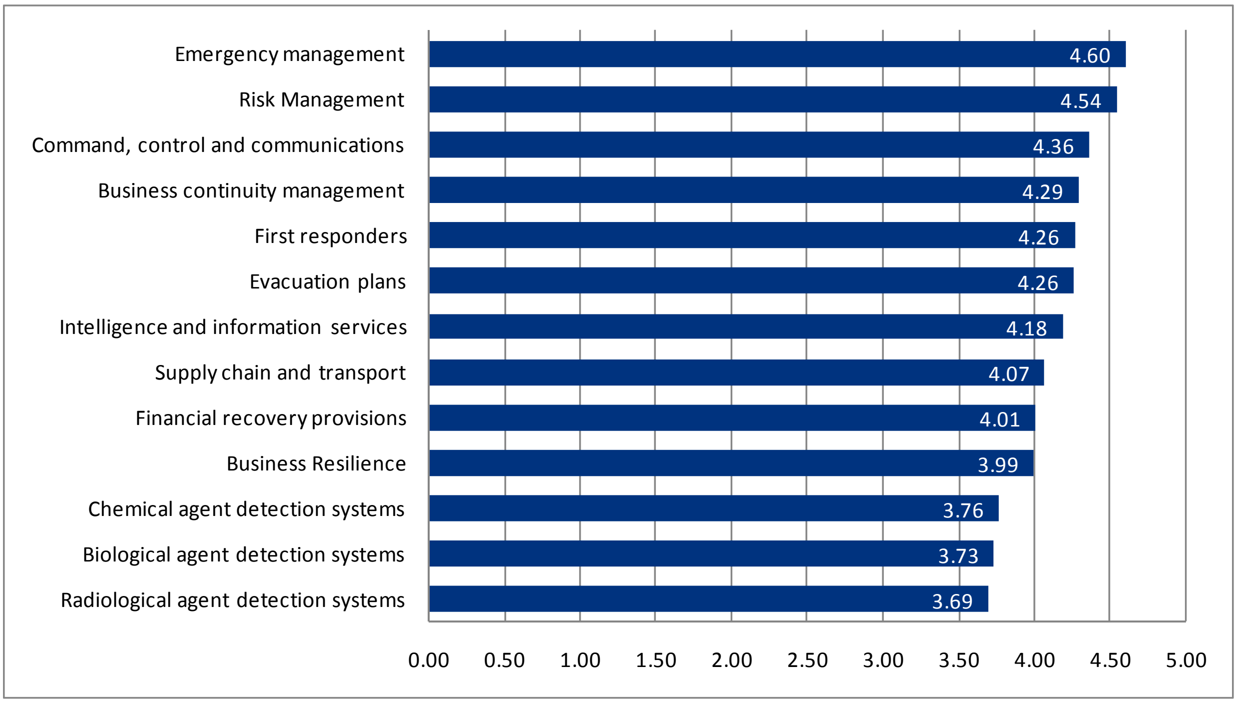


FIGURE 34 PRIORITIZATION OF RISK MANAGEMENT

Results by CEOs and executives

There were 22 responses from CEOs and 60 responses from executives. The highest score is Emergency management (4.72), followed by Business continuity management and Risk management with identical scores of 4.56, then Command, control and communications (4.45). The difference in the two sets of results is accounted for by the increased emphasis by this group on Business continuity management over Command, control and communications.

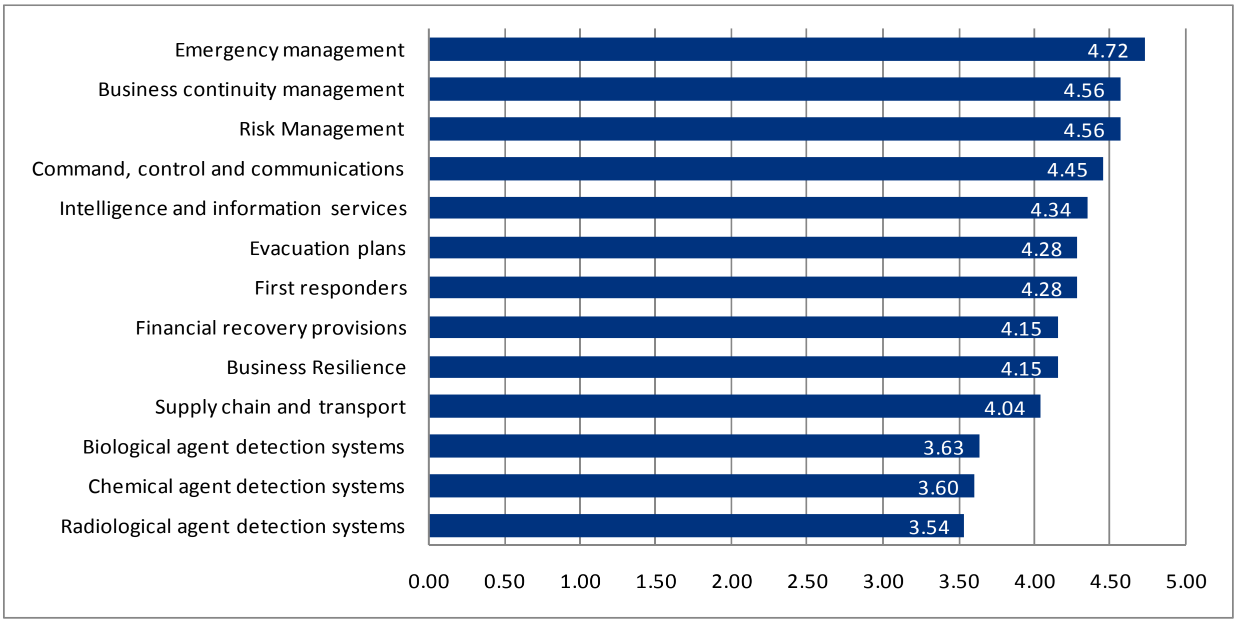


FIGURE 35 PRIORITIZATION OF RISK MANAGEMENT BY CEOS AND EXECUTIVES

Results by sector

Across all sectors the highest rating scores were supported on an overall level and by CEOs and executives. There were high scores in Food supply (4.50) and Health (4.54) for First responders, while Essential manufacturing scored Financial recovery provisions (4.25) highly.

	Communications	Energy	Essential Manufacturing	Finance	Food Supply	Government Services	Health	National Icons	Other	Transport	Utilities
Emergency management	4.43	4.62	4.42	4.60	4.50	4.59	4.67	4.86	4.60	4.58	4.70
Risk Management	4.40	4.64	4.17	4.42	3.75	4.56	4.54	4.86	4.58	4.58	4.62
Command, control and communications	4.13	4.38	4.25	4.35	4.50	4.34	4.38	4.71	4.41	4.54	4.27
Business continuity management	4.43	4.54	4.58	4.44	4.25	4.13	4.15	4.71	4.40	4.29	4.11
First responders	4.07	4.34	3.67	4.17	4.50	4.30	4.54	4.57	4.17	4.42	4.16
Evacuation plans	3.90	4.36	3.67	4.13	3.75	4.23	4.49	4.57	4.44	4.33	4.14
Intelligence and information services	4.00	4.18	3.58	4.33	4.00	4.20	4.13	4.14	4.38	4.29	3.81
Supply chain and transport	3.80	4.02	4.00	3.92	4.25	4.03	4.44	4.14	4.14	4.21	4.05
Financial recovery provisions	3.80	4.08	4.25	4.23	4.25	3.96	4.00	4.29	4.14	3.79	3.70
Business Resilience	4.20	4.18	3.58	4.13	4.00	3.96	3.77	4.29	4.05	4.08	3.70
Chemical agent detection systems	3.13	3.86	3.17	3.48	3.75	3.87	4.36	3.57	3.88	3.50	3.46

FIGURE 36 PRIORITIZATION OF RISK MANAGEMENT BY SECTOR[7]

[7] Note that the items in yellow in Figure 36 identify the top 3 items chosen by sector. Sometimes more than three items are shown, this occurs where there are multiple equal scores.

Additional suggestions and comments

A respondent requested *“Consideration to include another section regarding the usage of this data information for a forward looking approach and not limit it to immediate response needs – Important.”* This suggestion applies more to strategic planning considerations in relation to information. There are existing categories in the Framework for ‘Intelligence and information services’ and ‘Information security’. An important point is however being made here for consideration within the industry.

In relation to risk analysis, a respondent remarked:

> *Risk analysis is very important and currently poorly done. Many practitioners attempt to use AS/NZS 4360 for risk analysis and risk assessment, however of course this standard is not intended for that purpose. Thus many errors are made.”*

Risk analysis is covered under the specific category for Risk management in the Framework however this comment is included for consideration within industry.

One or two respondents stated that in their particular member economy they felt ‘safe’ and did not feel they were a likely target for terrorist attacks. The inclusion of categories for chemical detection systems etc did not appear to be relevant in their context, although there was recognition that this is *‘probably naïve’*.

Throughout the survey, respondents shared their ideas and insights, as shown in the following comment:

> *“I believe having an experienced task force that can be deployed within the APEC region would be very useful. Nothing counts more than experience in a natural or man-made disaster. Fortunately few of us have this experience, but it’s needed …. e.g. Having a specialized hurricane response team that is deployed whenever a disaster occurs would rapidly develop an experienced team that would be invaluable in future emergencies. Rather, than each area learning the first time when an emergency hits…”*

Conclusion

The overall ratings for the top three areas were supported by the results for CEOs and by sector with some variations for score rankings. It is also important to consider the views of the CEOs and executives, who ranked Business continuity management at the same level of importance as Risk management.

Recommendation:

- If deemed useful, ABAC to consider supporting the feasibility of deploying emergency response teams and / or security advisors in the region. If these options are already in existence, consideration to be given to communication about access to these within the region.

Information security

Overall results

There were 520 responses to this mandatory question. The highest score was Network security (4.40), followed by Systems access control and Information security with identical scores of 4.39, then General IT security management (4.32).

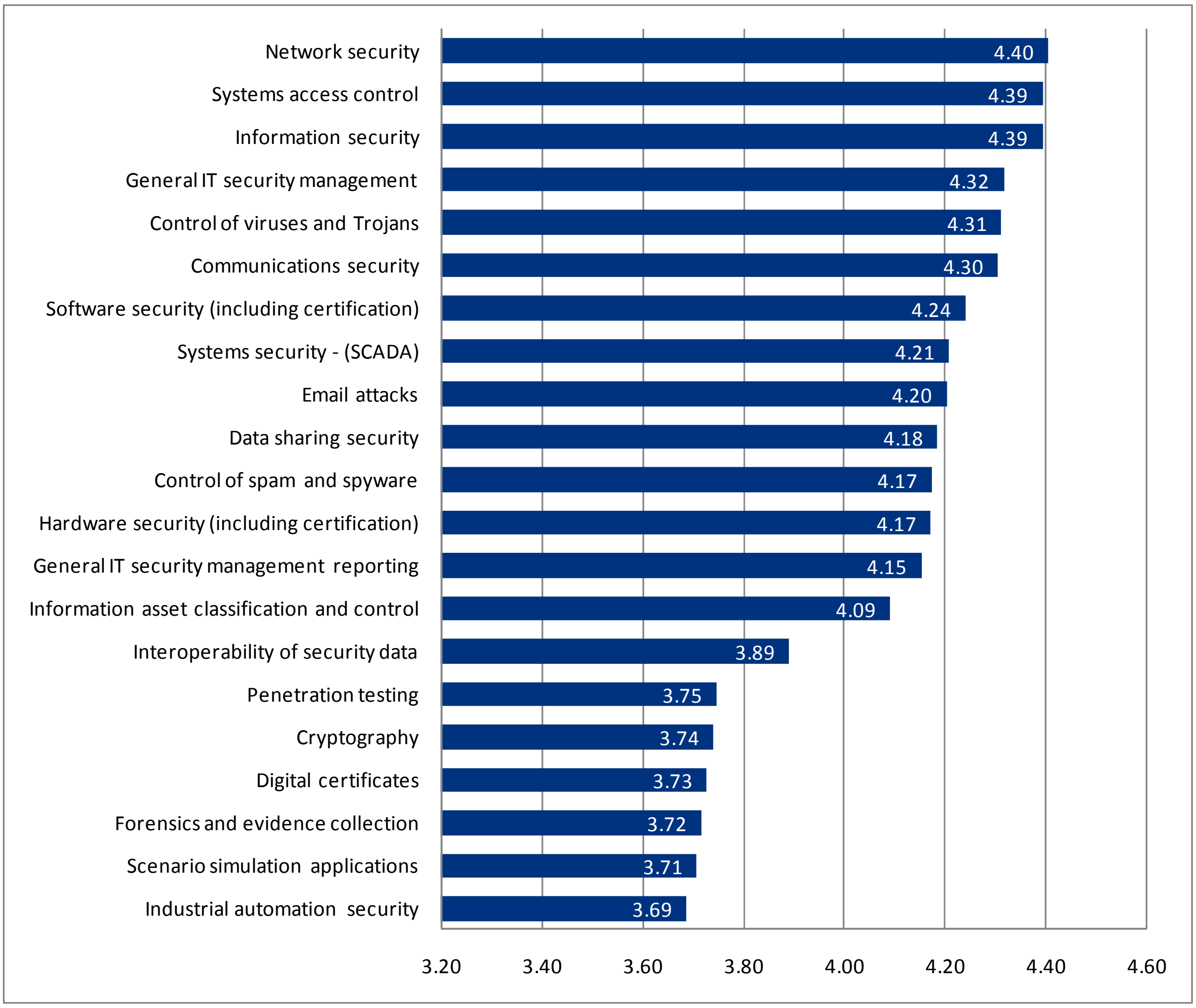


FIGURE 37 PRIORITIZATION OF INFORMATION SECURITY

Results by CEOs and executives

There were 22 responses from CEOs and 60 responses from executives. The highest score was Control of viruses and Trojans (4.48), followed by Network security and Systems access control with identical scores of 4.46, then Information security (4.45). The CEOs and executives placed higher importance on Control of viruses and Trojans, which attained a much lower score ranking in the overall results. Apart from this variation, the score rankings for the other top areas are very similar to the overall results.

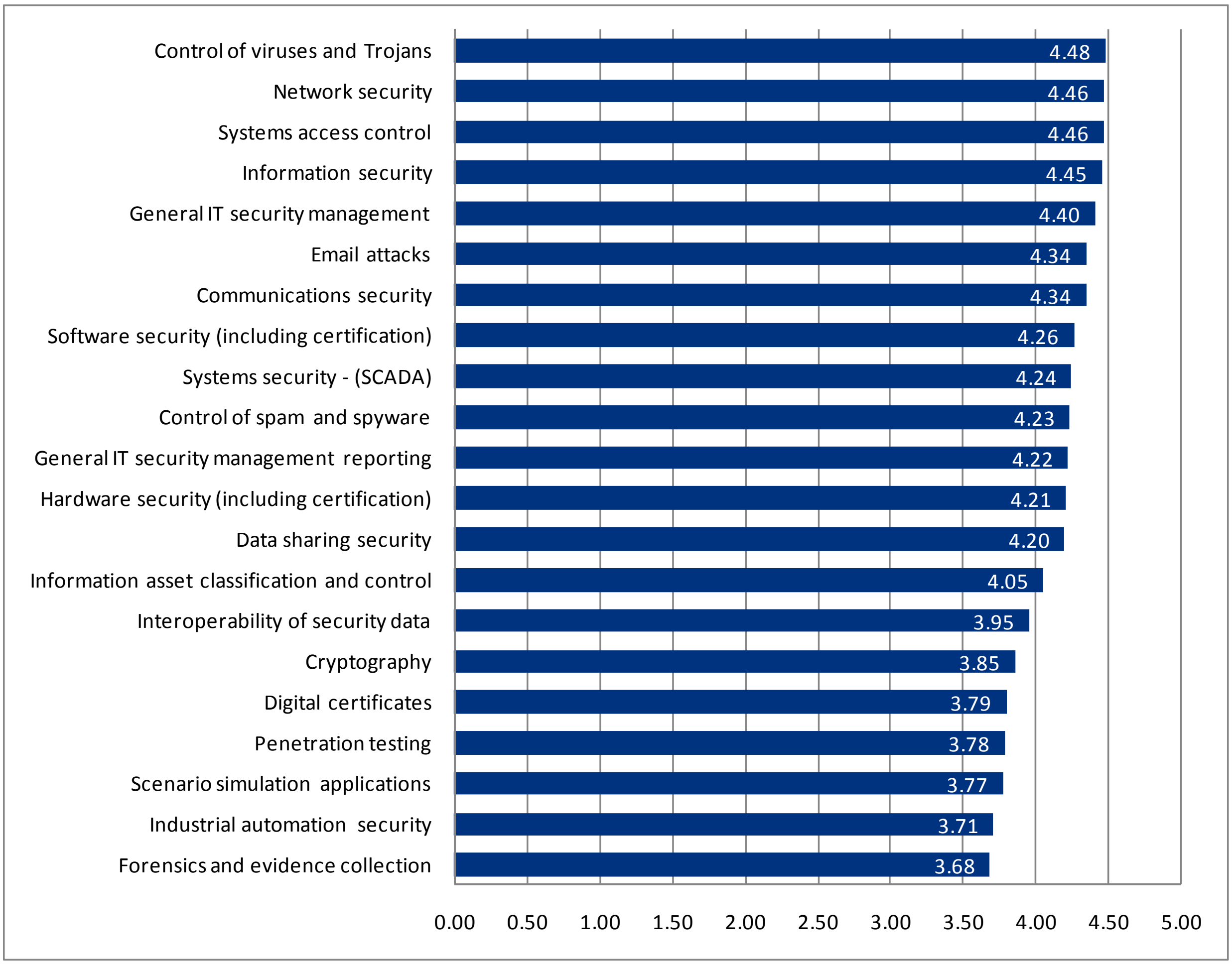


FIGURE 38 PRIORITIZATION OF INFORMATION SECURITY BY CEOS AND EXECUTIVES

Results by sector

There is a reasonably high level of consistency with the overall results, with Network security and Systems access control scoring highly across the majority of sectors. Information security only scores highly for 5 of the 10 major sectors (excluding 'Other'). As Information security is a specialized area applying to all sectors of industry, it is interesting to compare the results from the Communications sector (IT, telecommunications, postal services etc). There were 30 respondents from this sector, many of whom would have specialized knowledge and technical expertise in this area. In addition to CEOs, executives and managers, this group included systems analysts and support personnel, software engineers and other technical specialists. The highest score is for Control of viruses and Trojans (4.57) followed by Systems access control (4.53) then Network security (4.50). As the highest score is for Control of viruses and Trojans, the results for this group are more in line with the results from CEOs and executives. Information security has quite a high score (4.43) in the Communications sector results but it is scored below Control of spam and spyware (4.47). These results show an emphasis on IT issues whereas Information security is more generic.

	Communications	Energy	Essential Manufacturing	Finance	Food Supply	Government Services	Health	National Icons	Other	Transport	Utilities
Network security	4.50	4.51	4.42	4.44	4.67	4.46	4.26	4.43	4.30	4.42	4.24
Systems access control	4.53	4.39	4.25	4.60	4.33	4.42	4.33	4.57	4.36	4.38	4.05
Information security (storage and categorisation of sensitive information)	4.43	4.35	4.17	4.50	4.33	4.49	4.33	4.57	4.35	4.21	4.11
General IT security management	4.37	4.27	4.25	4.31	4.67	4.42	4.38	4.29	4.25	4.17	4.03
Control of viruses and Trojans	4.57	4.22	4.00	4.17	4.67	4.38	4.59	4.43	4.26	4.08	4.08
Communications security	4.30	4.37	3.92	4.50	4.00	4.37	4.28	4.29	4.26	4.17	4.00
Software security (including certification)	4.27	4.20	4.25	4.23	4.00	4.35	4.21	4.29	4.19	4.17	3.95
Systems security - Supervisory Control and Data Acquisition (SCADA)	4.17	4.41	3.83	4.35	4.33	4.27	4.18	4.29	4.11	3.96	4.00
Email attacks (e.g. scams and theft of online banking details)	4.40	4.16	3.83	4.00	4.67	4.34	4.41	4.00	4.13	4.04	3.84
Data sharing security	4.30	4.16	4.00	4.15	3.67	4.27	4.08	4.14	4.22	4.17	3.92
Control of spam and spyware	4.47	4.12	3.83	4.08	4.33	4.29	4.36	3.86	4.11	4.04	3.73
Hardware security (including certification)	4.13	4.29	4.00	4.33	4.00	4.21	4.10	4.29	4.10	4.08	3.97
General IT security management reporting	4.10	4.12	4.00	4.23	4.33	4.26	4.18	3.86	4.09	4.04	3.89
Information asset classification and control	4.20	4.22	3.75	4.02	4.33	4.19	3.97	4.14	4.01	3.96	3.89
Interoperability of security data	3.83	3.92	3.92	3.79	3.67	4.01	3.85	3.71	3.90	3.71	3.62
Penetration testing	4.13	3.73	3.42	3.88	4.33	3.81	3.74	3.43	3.77	3.46	3.19
Cryptography	3.93	3.71	3.58	3.75	3.67	3.89	3.79	3.00	3.77	3.29	3.22
Biological agent detection systems	3.17	3.68	3.08	3.54	3.75	3.88	4.38	3.57	3.83	3.42	3.30
Digital certificates	3.87	3.59	3.42	3.79	3.67	3.89	3.72	2.86	3.88	3.08	3.27
Forensics and evidence collection	3.70	3.55	2.83	3.67	4.33	3.87	3.97	3.43	3.88	3.29	3.14
Scenario simulation applications	3.87	3.94	2.67	3.79	4.00	3.72	3.46	3.86	3.83	3.46	3.54
Radiological agent detection systems	3.20	3.66	3.17	3.46	3.75	3.88	4.31	3.57	3.77	3.33	3.08
Industrial automation security	3.47	3.92	4.08	3.65	3.67	3.69	3.67	3.29	3.74	3.38	3.62

FIGURE 39 PRIORITIZATION OF INFORMATION SECURITY BY SECTOR[8]

[8] Note that the items in yellow in Figure 39 identify the top 3 items chosen by sector. Sometimes more than three items are shown, this occurs where there are multiple equal scores.

Additional suggestions and comments

One respondent commented:

> *"There are lots of information security standards already, so although I think they are very important, focus should be on communicating and meeting these rather than developing new standards."*

Following circulation of the draft report, a respondent suggested that consideration be given to including another element in the Framework (Figure 3) for 'Investigations' and made the following comments:

> *"Once an incident occurs, incident handling is necessary to manage this issue, but this procedure does not include investigations, relating with computer forensic process and recovery and using digital evidence or electronic stored information. I suggest reviewing HB 171 2003 Management of IT Evidence."*

This is an important point however investigations of this nature appear to fit under the Framework component for Information security.

Conclusion

The overall results are supported by the results from CEOs and executives and by sector. It is important to also consider the emphasis from the CEOs and executives on the importance of Control of viruses and Trojans, especially as this is supported by results from the Communications sector. This should also be tempered by an understanding that Information security is about the storage and categorization of sensitive information. The category therefore encompasses but goes beyond IT considerations.

Recommendation:

- SCSC to consider communication strategies to encourage adherence to existing standards related to the protection of critical infrastructure in the region.

Personnel security

Overall results

There were 520 responses to this mandatory question. The highest score was for Security training systems for staff (4.31), followed by Building and facility access control (4.26) and Pre-employment screening (4.21).

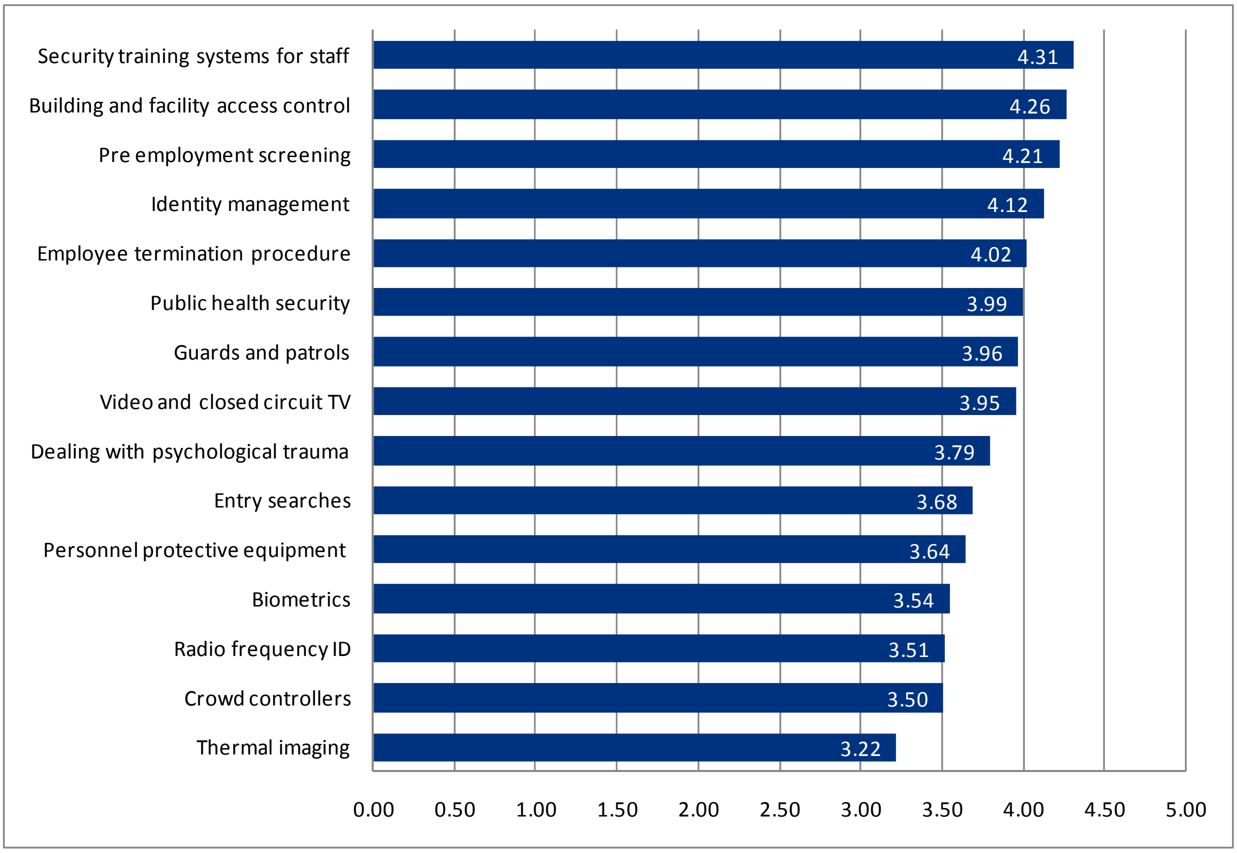


FIGURE 40 PRIORITIZATION OF PERSONNEL SECURITY

Results by CEOs and executives

There were 22 responses from CEOs and 60 responses from executives. The highest score was for Security training systems for staff (4.38), followed by Building and facility access control (4.34) and Pre-employment screening (4.30). The three top scoring categories are therefore identical to and ranked in the same order as the overall results.

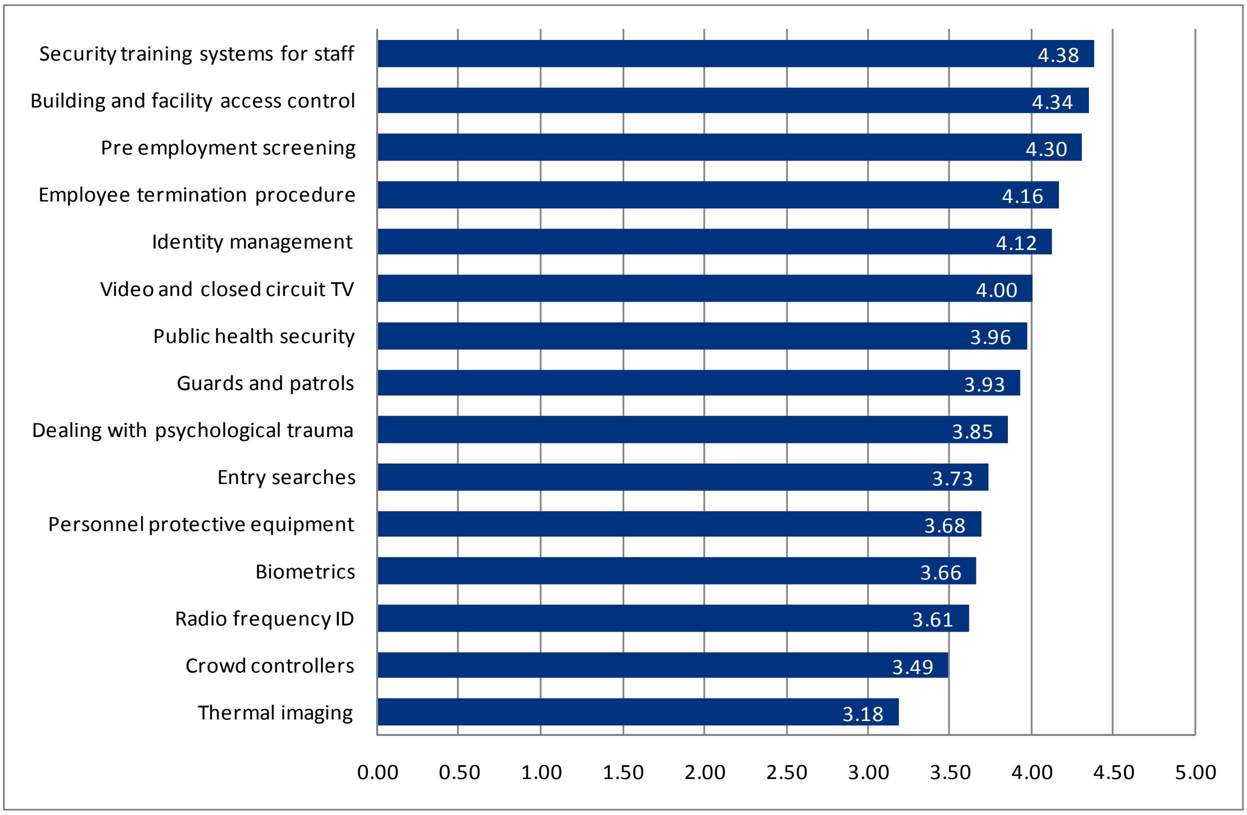


FIGURE 41 PRIORITIZATION OF PERSONNEL SECURITY BY CEOS AND EXECUTIVES

Results by sector

Results by sector, shown in Figure 42, support the overall results and the results by CEOs and executives. At least two of the three top scoring categories of Security training systems for staff, Building and facility access control and Pre-employment screening were also scored highly in the results for most sectors. There were variations, such as high scores for Video and closed circuit TV in results from the Essential manufacturing and National icons sectors. Public health security was scored highly by the Health and Utilities sectors.

	Communications	Energy	Essential Manufacturing	Finance	Food Supply	Government Services	Health	National Icons	Other	Transport	Utilities
Security training systems for staff	4.47	4.41	4.08	4.17	4.00	4.39	4.41	4.43	4.31	4.08	3.92
Building and facility access control	4.17	4.31	4.42	4.38	4.33	4.22	4.26	4.57	4.38	4.25	3.92
Pre employment screening	4.07	4.31	4.17	4.21	4.33	4.24	4.33	4.86	4.26	4.29	3.68
Identity management	4.10	4.22	3.92	4.27	4.33	4.19	4.21	4.43	4.15	3.92	3.46
Employee termination procedure	4.00	4.10	3.92	4.21	3.67	4.04	3.85	4.29	4.15	4.17	3.38
Public health security	3.53	3.92	3.42	3.96	2.00	4.08	4.31	4.14	4.06	3.67	4.11
Guards and patrols	3.70	4.14	4.17	3.94	4.67	3.98	3.90	4.29	4.03	4.08	3.51
Video and closed circuit TV	3.83	4.08	4.42	3.98	4.00	3.89	3.82	4.57	4.07	4.00	3.68
Dealing with psychological trauma	3.30	3.84	3.92	3.77	3.67	3.86	4.15	4.29	3.91	3.54	3.22
Entry searches	3.60	3.71	3.75	3.63	3.67	3.84	3.41	3.86	3.76	3.54	3.19
Personnel protective equipment (eg bullet proof vests, respirators etc)	3.23	3.73	3.50	3.52	3.00	3.69	4.13	3.57	3.78	3.54	3.05
Biometrics	3.47	3.41	3.00	3.56	3.67	3.60	3.77	3.71	3.75	3.54	2.86
Radio frequency ID	3.40	3.67	2.92	3.52	3.67	3.53	3.41	3.57	3.72	3.25	3.24
Crowd controllers	3.10	3.33	2.83	3.56	3.33	3.74	3.69	3.43	3.56	3.33	2.86
Thermal imaging (for human temperature screening)	2.80	3.31	2.58	3.19	3.33	3.40	3.38	3.14	3.35	2.83	2.51

FIGURE 42 PRIORITIZATION OF PERSONNEL SECURITY BY SECTOR[9]

Additional suggestions and comments

The inclusion of exit searches was suggested and the category currently refers only to entry searches.

Security training systems for staff was a recurring theme in the survey, along with the difficulties associated with recruiting and retaining personnel with appropriate skill sets and professional values. There were concerns raised about accessing current training in an area that is constantly evolving in terms of best practice and changing technology. Respondents also expressed a need for access to training on an international basis. The number of training institutions appeared to be an issue in at least one member economy. One respondent commented that private training organizations rarely qualify for funding and this would conceivably impact on the courses that are made available.

Practices observed in transit facilities worldwide particularly concerned one respondent who stated that "*a better system for training and the line duties of what to do need to be addressed*" in this area.

Another respondent pointed out the challenges for organizations responsible for the security of personnel who are travelling and not necessarily always based at a

[9] Note that the items in yellow in Figure 42 identify the top 3 items chosen by sector. Sometimes more than three items are shown, this occurs where there are multiple equal scores.

particular physical location. This would include field staff, transit workers and executives regularly travelling overseas. Concerns about occupational health and safety were also expressed in relation to the vulnerability of security personnel.

Conclusion

The overall results for the top areas are supported by results from CEOs and executives and results by sector. There are variations by sector to be considered.

Physical security

Overall results

There were 520 responses to this mandatory question. The highest scoring category was Security of facility utilities (4.41), followed by Perimeter security and Construction security with identical scores of 4.28, then Alarms, intruder alarms and detection devices (4.25).

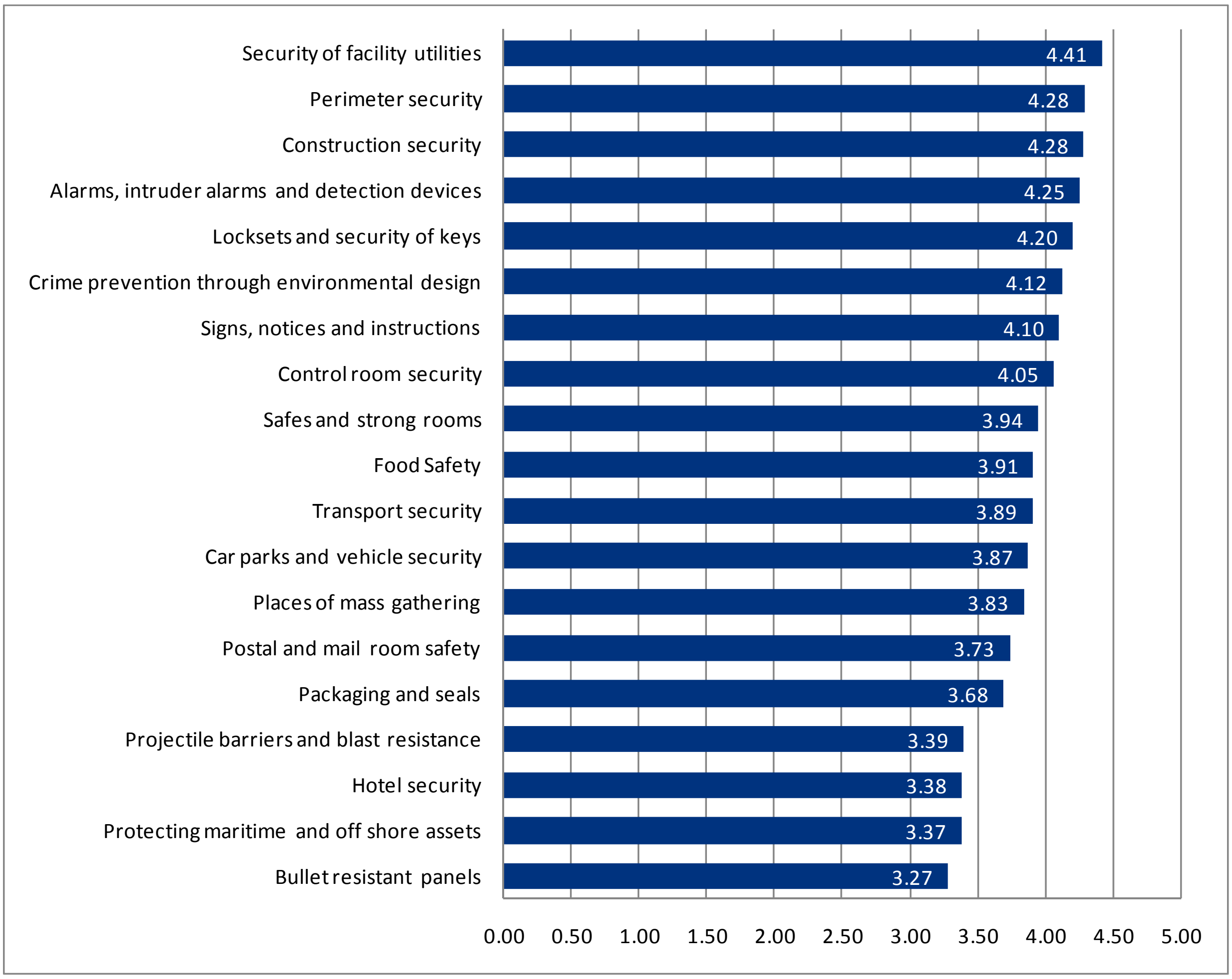


FIGURE 43 PRIORITIZATION OF PHYSICAL SECURITY

Results by CEOs and executives

There were 22 responses from CEOs and 60 responses from executives. The highest scoring category was Security of facility utilities (4.50), followed by the three categories of Alarm, intruder alarms and detection devices, Construction security and Perimeter security with identical scores of 4.33. The ranking for the top areas is therefore very similar to the overall results.

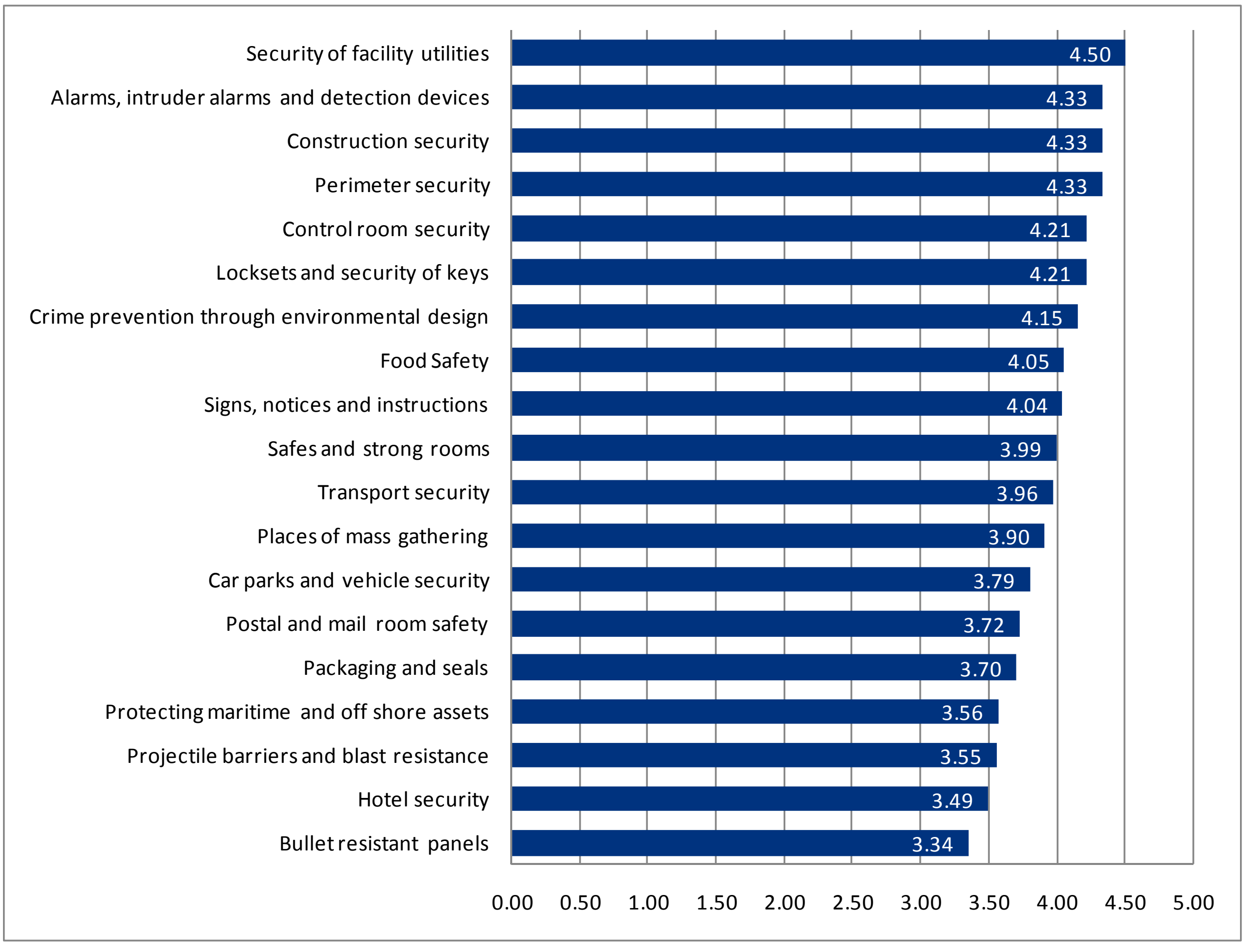


FIGURE 44 PRIORITIZATION OF PHYSICAL SECURITY BY CEOS AND EXECUTIVES

Results by sector

Comparison with results by sector in Figure 45 supports the overall results and results by CEOs and executives. All sectors scored at least two of the four top categories of Security of facility utilities, Perimeter security, Construction security and Alarms, intruder alarms and detection devices highly. Crime prevention through environmental design was particularly important to the Finance and National icons sectors. Signs, notices and instructions were important to the Food supply, Transport and Utilities sectors. There were identical scores for a number of categories in results from both the Food supply and National icons sectors.

	Communications	Energy	Essential Manufacturing	Finance	Food Supply	Government Services	Health	National Icons	Other	Transport	Utilities
Security of facility utilities (water, gas, electricity, telecommunications and waste)	4.47	4.53	4.50	4.19	3.67	4.41	4.54	4.86	4.39	4.42	4.41
Perimeter security (e.g. lighting, fencing, bollards, chains, doors, windows, gates)	4.50	4.41	4.42	4.17	4.00	4.26	4.13	4.86	4.31	4.46	4.00
Construction security (e.g. construction materials, building structure, fire protection)	4.30	4.39	4.08	3.96	4.00	4.36	4.28	4.57	4.32	4.04	4.19
Alarms, intruder alarms and detection devices	4.43	4.43	4.25	4.10	4.33	4.26	4.21	4.57	4.28	4.13	3.97
Locksets and security of keys	4.17	4.20	4.42	4.13	4.00	4.24	4.10	4.57	4.25	4.17	3.95
Crime prevention through environmental design	3.90	4.06	3.67	4.23	3.67	4.22	4.23	4.57	4.09	3.92	3.86
Signs, notices and instructions	4.10	4.20	3.92	3.88	4.00	4.10	4.18	4.14	4.08	4.25	4.11
Control room security	4.20	4.22	4.00	4.17	4.00	4.01	3.64	4.29	4.18	4.17	3.84
Safes and strong rooms	4.00	3.71	3.58	4.10	3.67	4.09	4.03	4.00	3.92	3.58	3.51
Food Safety	3.53	3.80	3.58	3.81	4.00	4.07	4.33	4.14	3.91	3.38	3.59
Transport security	3.77	3.94	3.75	3.90	3.67	3.95	3.87	4.29	3.98	4.00	3.43
Car parks and vehicle security (including vehicle control points)	3.87	3.92	3.67	3.88	3.67	3.87	3.95	4.57	3.95	3.75	3.49
Places of mass gathering (security of public spaces and events)	3.47	3.59	3.25	3.63	3.33	3.99	4.03	4.14	4.03	3.58	3.59
Postal and mail room safety	3.67	3.88	3.50	3.79	4.00	3.80	3.69	4.29	3.81	3.58	3.05
Packaging and seals	3.43	3.57	3.17	3.58	4.33	3.89	3.54	3.86	3.73	3.58	3.38
Projectile barriers and blast resistance	3.30	3.78	3.00	3.48	3.67	3.42	2.59	3.57	3.61	3.25	3.16
Hotel security	3.30	3.39	3.00	3.60	4.00	3.42	3.13	4.14	3.58	2.88	2.95
Protecting maritime and off shore assets (including boats and ships)	3.20	3.69	3.00	3.21	2.33	3.45	2.85	3.86	3.59	3.25	3.14
Bullet resistant panels	3.23	3.16	3.08	3.52	3.33	3.34	3.26	3.43	3.40	3.25	2.57

FIGURE 45 PRIORITIZATION OF PHYSICAL SECURITY BY SECTOR[10]

Additional suggestions and comments

Consideration of the inclusion of ‘Intelligent building’ was suggested and rated as very important. Design security was also suggested and this is included under the description of Physical security in the Framework.

Conclusion

The overall results for the top areas are supported by the results from the CEOs and executives and by sector. There are variations by sector to be considered.

[10] Note that the items in yellow in Figure 45 identify the top three items chosen by sector. Sometimes more than three items are shown, this occurs where there are multiple equal scores.

15. Priority areas for standards development

All categories in the Integrated Security Standards Framework are critical to ensuring the protection of critical infrastructure and should be considered accordingly. Due to the complexity of the security area it is essential to prioritize areas for initial focus. The recommended approach is to concentrate first on the three top scoring specific categories of standards under each broad category in the Framework, as summarized in the table below. This ensures a comprehensive approach to security standards based on the importance levels derived from the survey results.

The gap analysis in the following section focuses on the three top scoring areas under each category. The 15 specific categories included in the gap analysis are highlighted in the table below.

Standards Category	Score
Governance, strategy & policy	
Effective leadership	4.46
Crisis management	4.41
Security management	4.40
Risk management	
Emergency management	4.60
Risk management	4.54
Command, control and communications	4.36
Information security	
Network security	4.40
Systems access control	4.39
Information security (storage and categorization of sensitive information)	4.39
Personnel Security	
Security training systems for staff	4.31
Building and facility access control	4.26
Pre-employment screening	4.21
Physical security	
Security of facility utilities (water, gas, electricity, telecommunications and waste)	4.41
Perimeter security (e.g. lighting, fencing, bollards, chains, doors, windows, gates)	4.28
Construction security (e.g. construction materials, building structure, fire protection)	4.28

FIGURE 46 PRIORITY AREAS FOR STANDARDS DEVELOPMENT

16. Gap analysis

The gap analysis focuses on key international standards identified in the priority areas. The basis for this analysis is the standards inventory, which is available for reference in Section 20 of this report. It is acknowledged that there are national standards in existence and under development in relation to the priority categories. The gap analysis should also be considered in the context of important work undertaken and under development by major international organizations, such as the Red Cross, NFPA and ASIS International. References to relevant publications are included in the table below.

Specific area of standardization:	Effective leadership
Overview:	Effective leadership is based on many factors, including personal qualities, knowledge, skills and experience. In the context of the survey, it indicates from a governance and senior executive perspective that leaders feel they need additional guidance on preparing for and managing emergency and security situations.
Existing standards and handbooks	There are no specific international standards on effective leadership, however there are many sources of reference materials in relation to this area.
Gaps and additional work required:	Training and professional development should focus on standards relevant to the role, such as corporate governance and risk management, with particular emphasis on standards in the priority areas. Job descriptions or position guidelines are also of assistance in identifying effective leaders, such as the ASIS Chief Security Officer Guideline 2008 Edition (ASIS GDL CSO 04 2008)
Recommendations:	This is an area for further consideration at the CEO / Executive workshop recommended in this report.

FIGURE 47 GAP ANALYSIS: EFFECTIVE LEADERSHIP

Specific area of standardization:	Crisis management
Overview:	The focus of this category is on the governance perspective of crisis and emergency management from

	an organizational rather than community perspective. Often literature related to crisis and emergency management is aimed at a technical or emergency services level. In this category it is focused at a governance level and assisting the Board and Senior Executive of organizations to effectively manage a crisis situation from a leadership, operational, public relations and communications perspective to discharge their responsibilities.
Existing standards and handbooks	There are very few standards that specifically relate to this category.
Work in progress:	N/A
Gaps and additional work required:	Although there are few specific standards available, crisis management is generally addressed under risk management. The development of specific standards may help to focus attention on organizational obligations in relation to crisis management.
Recommendations:	Crisis management is a category for consideration in relation to future standards development.

FIGURE 48 GAP ANALYSIS: CRISIS MANAGEMENT

Specific area of standardization:	Security management
Overview:	This category addresses the need for holistic and graded security management systems based on criticality and risk.
Existing standards and handbooks:	There is very little available in this area at the moment, however often organizations retrofit ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management as a more general management system for security management.
Work in progress:	N/A
Gaps and additional work	An international standard appears to be required to

required:	address Security management.
Recommendations:	Security management is an area for consideration in future standards development.

FIGURE 49 GAP ANALYSIS: SECURITY MANAGEMENT

Specific area of standardization:	Emergency management
Overview:	Emergency management is a range of measures to manage risks to communities and the environment. The emphasis is on societal security, rather than on organizational security. This category covers the organizational interfaces with emergency services and the management of resources for dealing with all aspects of emergencies at an operational level. Emergency management involves the plans, structures and arrangements which are established to bring together the normal endeavors of government, voluntary and private agencies in a comprehensive and coordinated way to deal with the whole spectrum of emergency needs, including prevention, response and recovery.
Existing standards and handbooks:	The ISO TC 223 was established in response to an identified need for standards in this category. As a result , the following standard was developed: ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management The National Fire Protection Association (NFPA) has also developed the following standard: NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs There is also important work being done in this area by the SOM Special Task Forces on Emergency Preparedness (TFEP) and Counter-Terrorism (CTTF).

At the 2nd TFEP meeting in August 2008, APEC economies endorsed a Peru-initiated Strategy for Disaster Risk Reduction and Emergency Preparedness and Response in the Asia Pacific Region: 2009 to 2015 (TFEP 04/2008A). TFEP members also agreed to form a Steering Committee to assist the TFEP and its co-Chairs to advance the task force's mandate and workplans, and to assess TFEP projects. At the meeting APEC Member Economies were also encouraged to develop joint capacity building projects, to improve coordination with international organizations, to share best practices at all levels, to support train-the-trainer programs, and to collaborate with the Human Resource Development Working Group on integrating disaster risk reduction education into school curricula.

Recent TFEP activities include:

- A Study Course on Disaster Emergency Response and Recovery held in Beijing, China in April 2008.
- An APEC Workshop on Dialogue among APEC economies, the business community and key international and regional partners on emergency preparedness, held in Viet Nam in April 2008.
- A Workshop on Large Scale Disaster Recovery in APEC and related on-site visits, held in Chinese Taipei and Sichuan, China in September.

The achievements of the CTTF include the counter - terrorism action plans that were developed in 2003 and the Secure Trade in the APEC Region (STAR) initiative. The CTTF has endorsed a number of projects and new initiatives for implementation in 2009, which include:

- A Workshop on aviation security to be held in Viet Nam in April 2009.

	• Second Workshop on detecting and deterring cash couriering and bulk cash smuggling (early 2009) • Workshop to improve regulation of non-profit organizations to prevent misuse by terrorist groups (Bangkok, Thailand, early 2009) • Trade Recovery Program Pilot APEC Leaders have also emphasized the important role played by the UN and its Global Counter-Terrorism Strategy, and stressed the need for implementation, where applicable, of UN counter-terrorism measures and the Financial Action Task Force's (FATF) Special Recommendations on Terrorist Financing.
Work in progress:	ISO/WD 22300 Societal security - Fundamentals and vocabulary
Gaps and additional work required:	The ISO TC 223 is undertaking standards development to address gaps identified in this area.
Recommendations:	Awareness or training may be required in this area. This is also an area for consideration in future standards development.

FIGURE 50 GAP ANALYSIS: EMERGENCY MANAGEMENT

Specific area of standardization:	Risk Management
Overview:	Risk management is the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects.
Existing standards and handbooks:	This category is generally well covered in international standards although many seem to be aimed at generic risk management rather than addressing the specific requirements of security risk management. It is also an area that was addressed in national standards provided for the inventory.

Work in progress:	There are a number of risk management standards currently under development.
Gaps and additional work required:	Standards development in this category is ongoing. There are issues associated with the volume of material that is available and emerging. Survey respondents highlighted concerns about how to manage the large volume of standards and the need for standards to be tailored to local conditions and the requirements of organizations and sectors.
Recommendations:	Education and awareness raising initiatives in this area could be considered for inclusion in the program that is recommended in this report. Standards bodies may need to consider new approaches to organizing standards so that key security standards can be quickly and easily identified by topic. This may be a question of restructuring existing databases.

FIGURE 51 GAP ANALYSIS: RISK MANAGEMENT

Specific area of standardization:	Command, control and communications
Overview:	This category refers to systems to ensure the strategic, tactical and informed exercise of authority in accomplishing organizational goals and objectives particularly in an emergency situation.
Existing standards and handbooks:	The only existing standard identified is: IEC 62290-1 Ed. 1.0 b:2006 Railway applications - Urban guided transport management and command/control systems - Part 1: System principles and fundamental concepts
Work in progress:	ISO/NP 22320 Societal security - Principles for command and control, coordination and cooperation in resolving incidents ISO/NP 22322 Societal security - Inter/Intra organizational warning procedures
Gaps and additional work	The gaps should be addressed when the above

required:	standards are released.
Recommendations:	There are no specific recommendations under this category.

FIGURE 52 GAP ANALYSIS: COMMAND, CONTROL AND COMMUNICATIONS

Specific area of standardization:	Network security
Overview:	Networks need to be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
Existing standards and handbooks:	The key standard in this area is: ISO/IEC NP 27033 Information technology -- IT Network security
Work in progress:	There is work in progress related to security techniques around network security.
Gaps and additional work required:	Network security standards are covered comprehensively. There are issues with the volume of standards available as referred to above.
Recommendations:	No specific recommendations under this category however refer to recommendations in Figure 51, Risk management.

FIGURE 53 GAP ANALYSIS: NETWORK SECURITY

Specific area of standardization:	Systems access control
Overview:	Access to information and business processes should be controlled on the basis of business and security requirements.
Existing standards and handbooks:	The key source of guidance under this category is ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management (redesignation of ISO/IEC 17799:2005)

Work in progress:	There is no specific work in progress related to this category.
Gaps and additional work required:	There are no gaps identified. Non-IT security professionals may need to be made aware of the above code of practice.
Recommendations:	An overview of the above code of practice could be considered for inclusion in the education and awareness program that recommended in this report.

FIGURE 54 GAP ANALYSIS: SYSTEMS ACCESS CONTROL

Specific area of standardization:	Information security (storage and categorization of sensitive information)
Overview:	Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved
Existing standards and handbooks:	The key source of guidance under this category is ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management (redesignation of ISO/IEC 17799:2005) This category is well covered under existing IT standards. As in other categories the volume of standards needs to be manageable.
Work in progress:	There is further work under development in relation to security techniques.
Gaps and additional work required:	There is a focus on IT and document control in available standards with less emphasis on the management of sensitive information with the potential to impact on security. Survey respondents expressed concerns about how to share knowledge and best practice while ensuring the protection of sensitive national and organizational information.
Recommendations:	It is recommended in this report that ABAC consider the creation of protocols to enable data to be securely shared between organizations. This is also an area for

	consideration in future standards development.

FIGURE 55 GAP ANALYSIS: INFORMATION SECURITY

Specific area of standardization:	Security training systems for staff
Overview:	These systems include security training targeted to security personnel and more widely to increase awareness of security issues in the general workforce.
Existing standards and handbooks:	ISO/IEC 23988:2007 Information technology - A code of practice for the use of information technology (IT) in the delivery of assessments ISO 10015:1999 Quality management -- Guidelines for training
Work in progress:	There is further work in progress, particularly in relation to IT.
Gaps and additional work required:	No specific standards identified in relation to security training. It may not be appropriate to develop specific standards in this area however training should be provided on key standards related to security.
Recommendations:	An education and awareness program has been recommended in the report.

FIGURE 56 GAP ANALYSIS: SECURITY TRAINING SYSTEMS FOR STAFF

Specific area of standardization:	Building and facility access control
Overview:	Based on these standards, organizations develop systems to ensure that only authorized personnel have partial or full access to their buildings and facilities. For example, an organization might decide that only IT personnel are authorized to enter the area where the main server is located. Similarly, members of the public may not be admitted past the front desk. The systems would ensure there are no breaches to security in these areas.

Existing standards and handbooks:	ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management (redesignation of ISO/IEC 17799:2005)
Work in progress:	Draft Facilities Physical Security Measures Guideline (2008)
Gaps and additional work required:	An international standard does appear to be required in this area. Reference could be made to work already undertaken by security organizations such as the draft guideline under development by ASIS International above.
Recommendations:	Building and facility access control is an area for consideration in future standards development.

FIGURE 57 GAP ANALYSIS: BUILDING AND FACILITY ACCESS CONTROL

Specific area of standardization:	Pre-employment Screening
Overview:	Pre-employment screening refers to the process of verifying, with the consent of the individual, the identity, integrity and credentials of potential employees.
Existing standards and handbooks:	No existing international standards and handbooks could be identified. Standards Australia has undertaken work in this area and developed the following standard and handbooks: AS 4811-2006 Employment screening Employment Screening Handbook (HB 323 – 2007 Reference Checking in the Financial Services Industry Handbook (HB 322 - 2007) that was developed in conjunction with the Australian Securities and Investments Commission (ASIC) and a panel of industry experts.
Work in progress:	ASIS International Pre-employment Background Screening Draft Guideline
Gaps and additional work	An international standard appears to be required to

required:	address pre-employment screening.
Recommendations:	Pre-employment screening is an area for consideration in future standards development.

FIGURE 58 GAP ANALYSIS: PRE-EMPLOYMENT SCREENING

Specific area of standardization:	Security of facility utilities (water, gas, electricity, telecommunications and waste)
Overview:	Organizations rely on certain utilities in order to function. If these utilities were damaged or sabotaged, this would adversely impact on the organization(s) or bring operations to a halt. This area refers to standards that assist organizations to ensure the security of these utilities in their facilities. For example, based on these standards, organizations develop systems to protect their telecommunications lines from sabotage by intruders.
Existing standards and handbooks:	No standards could be identified that specifically relate to this category.
Work in progress:	ASIS GDL FPSM DRAFT Draft Facilities Physical Security Measures Guideline (2008)
Gaps and additional work required:	An international standard does appear to be required in this area. Reference could be made to work already undertaken by security organizations such as the draft guideline under development by ASIS International above.
Recommendations:	Security of facility utilities is an area for consideration in future standards development.

FIGURE 59 GAP ANALYSIS: SECURITY OF FACILITY UTILITIES

Specific area of standardization:	Perimeter security (e.g. lighting, fencing, bollards, chains, doors, windows, gates)
Overview:	This category refers to security standards for lighting, fencing and other materials used to protect perimeters in the grounds of organizations or public spaces.
Existing standards and	There are few standards in existence that specifically

handbooks:	relate to the aspect of perimeter security. There are standards providing specifications for lighting, fencing, gates, glass etc.
Work in progress:	N/A
Gaps and additional work required:	Further standards development in this area does appear to be required.
Recommendations:	Perimeter security is an area for consideration in future standards development.

FIGURE 60 GAP ANALYSIS: PERIMETER SECURITY

Specific area of standardization:	Construction security (e.g. construction materials, building structure, fire protection)
Overview:	This category refers to security embedded in general construction standards.
Existing standards and handbooks:	There are many standards in existence related to security issues for particular construction materials, building structure and fire protection. These standards do not satisfactorily address the aspect of graded security. Graded security refers to risk assessments of infrastructure to determine the graded layers or levels of risk. Work is currently being undertaken in this area by Standards Australia.
Work in progress:	There are many specific construction standards under development and the following are of particular interest: ISO/AWI 6240 Performance standards in building – Contents and presentation ISO/AWI TR 21932 Buildings and constructed assets – Sustainability in building construction – Terminology ISO/IEC/ITU-T SAG-S is also working on ISO/IEC Guide for the inclusion of security aspects in standards. This document is still to be published.
Gaps and additional work required:	An international standard appears to be required to cover graded security in relation to construction. Reference could be made to work undertaken by

	standards bodies in the region, such as that currently being undertaken by Standards Australia.
Recommendations:	Graded security is an area for consideration in future standards development.

FIGURE 61 GAP ANALYSIS: CONSTRUCTION SECURITY

- SCSC to consider engaging with the ISO/IEC/ITU-T Special Advisory Group on Security (SAG-S) to address the gaps in standards identified as critical to security in the region. It would also be important to communicate with the SOM Special Task Forces on Emergency Preparedness (TFEP) and Counter-Terrorism (CTTF) in relation to this dialogue.

17. Methods for improving the implem entation of security standards

What can be done to make the implementation of security standards more successful?

There were 513 responses to this mandatory multiple choice question. Respondents were asked to indicate their top three choices from the list provided. An ‘Other’ category was included to allow respondents to specify approaches that were not covered in the answer options.

Overall results

Training was chosen by 90% of respondents followed by Implementation handbooks and guidance material (47%) then Technical assistance from consultants (43%). The proportion of respondents choosing Training is very high compared to all other options.

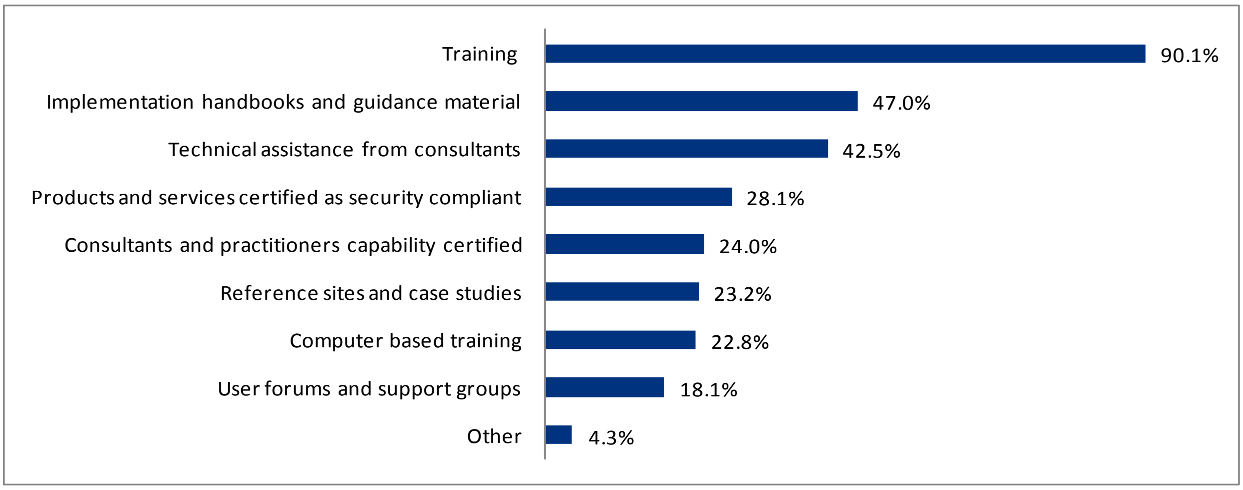


FIGURE 62 ASSISTING THE SUCCESSFUL IMPLEMENTATION OF STANDARDS

Additional suggestions and comments under the ’Other’ category included:

- hands-on training
- enforcement by government authorities
- regulatory bodies to have closer controls, audit and vigilance
- continuous monitoring of implementation policies, guidance, procedures and standards.
- funding
- planning process
- emphasis by leaders
- executive awareness, involvement and commitment
- installation of adequate hardware and software

- qualified and experienced security and safety managers
- making sure standards are relevant
- information sharing standards
- expansion of Sarbanes-Oxley practices for saving business records to security
- *"Giving security personnel protection by giving authority above a normal citizen when working".*

Results by CEOs and executives

Results from CEOs and executives support the overall results. Figure 62 shows 90% chose Training, followed by Implementation handbooks and guidance material (48%) then Technical assistance from consultants (40%). Again, there is a very high proportion of this group choosing Training over all other options and this matches the overall results.

Additional suggestions under the 'Other' category for this group were leadership, executive awareness and regulatory bodies to have closer controls, audit and vigilance.

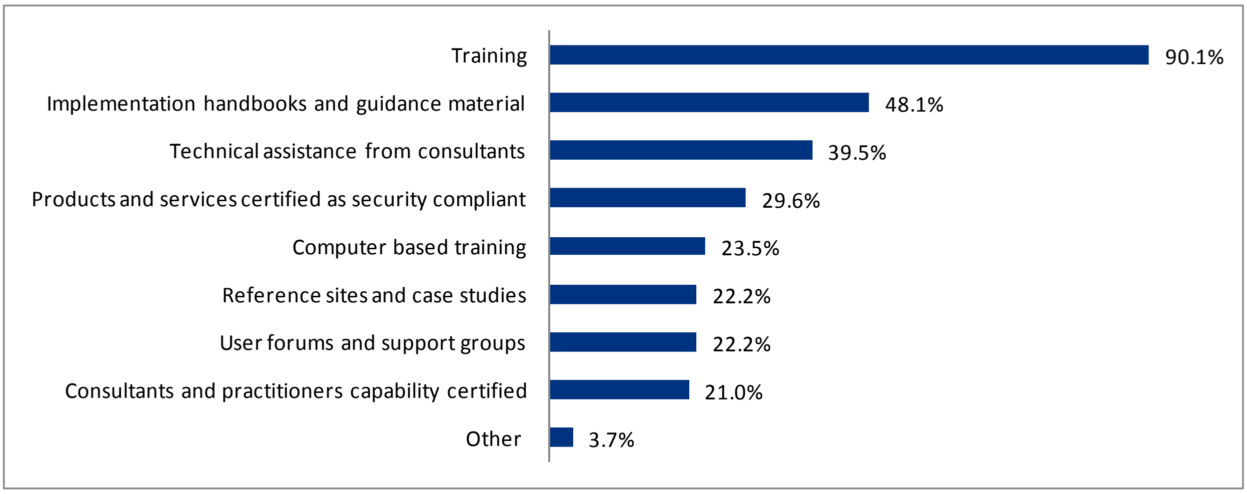


FIGURE 63 ASSISTING THE SUCCESSFUL IMPLEMENTATION OF STANDARDS BY CEOS AND EXECUTIVES

Results by sector

Results by sector also support the overall results and results from CEOs and executives. The three top areas are reflected in the results for the majority of sectors. The highest proportion of respondents in all sectors chose Training over all other options.

Conclusion

The three top areas for successful implementation of standards are consistent for overall results, results by CEOs and executives and by sector. Training is clearly the preferred approach to the successful implementation of standards in the region. This covers induction, workshops, exercises, professional development and mentoring.

18. Commentary overview

This section summarizes commentary from respondents in the open-ended sections of the survey. Due to the large amount of information collected in the survey it is not possible to cover all the comments and insights in this report. Similar views were expressed by a number of respondents. The overview of the commentary presented here pays particular attention to issues for consideration in standards development.

Views were expressed about the sheer volume of standards that are available. Some respondents find the standards system quite difficult to navigate, particularly from an operational perspective. There are also considerable cost and resourcing issues for organizations in meeting standards. Private organizations in particular may be concerned about their bottom line and returns on investment. As one respondent commented*, “organizations don’t believe that a failure in critical infrastructure is truly possible”* and this will affect the level of investment. Integration of standards and regulations was also raised as an issue, along with currency of standards. There was also a view expressed about the importance of standards mandated by government in particular industries.

International standards were often seen as too generic and needed to be adapted to local conditions and industry sectors. This was a particular issue for organizations that operated internationally. Some respondents raised concerns about the lack of national standards specific to security in particular countries.

One respondent stated that *“It is important that standards are written by people who are recognised by their peers as leaders in the field.”* This is probably not practical as standards writing is a specialized field. It does highlight the importance of consulting widely with appropriate industry experts when developing or revising standards. To fail to do so may lead to the standard(s) not being taken seriously by industry.

The pace of technological change was a recurring theme in survey responses. This appears to be presenting serious security concerns as highlighted in the comment below:

> *“Those who aim to damage society and infrastructure always manage to stay ahead of those trying to protect society and infrastructure.”*

Respondents are finding it difficult to keep up with technological advances and this was exacerbated by funding, resource and training considerations. Interestingly, responses indicate that an increased focus on information security may have led to vulnerabilities in other areas, such as physical security, in some organizations or sectors. This highlights the importance of rigorous risk management systems.

Suggestions were made for a national focal point for coordinating and facilitating responses to national threats and a common international platform for sharing information and best practice.

The importance of appropriately qualified security personnel was stressed by one respondent who was concerned about an erroneous mindset in the industry that *"ex-services are best"*. The particular qualifications required will vary according to the work involved.

Concerns about the need to raise the profile of the industry and change public perceptions were also raised. This was seen as especially important in attracting professionals, rather than casual workers to the industry. An interesting point was made by one respondent about perceived public support for police officers and lack of sympathy for security guards. In many ways both professions share similar responsibilities yet the police force has a more positive public profile. Another respondent thought a marketing campaign would be helpful, such as commercial advertisements or even a movie about the importance of security.

The importance of establishing a security culture within organizations was also highlighted, particularly in relation to information security.

Effective implementation of standards was linked to quality training from qualified and/or certified training professionals, qualified internal auditors with solid references, adequate supervision, executive buy-in, continuous improvement, sufficient funding, adequate resources and access to current technology. Emphasis was also placed on the need for standards to be simple to understand, practical and tailored to local conditions and industry sectors.

Based on comments, Transport and Health are areas that may warrant further investigation in relation to security standards development on national and international levels.

19. Challenges

Language

Although the APEC Member Economies involved were asked to nominate individuals with moderate to good English skills, some key contact points identified language as a barrier to collecting a sufficient number of responses. Language also proved to be an issue with the content of the draft survey as some of the terms were industry specific and therefore not easily understood by people from non-English speaking backgrounds. This is not a reflection on the English skills of the respondents but simply an acknowledgement of the subtleties of any language. For this reason, some of the more difficult technical terms were removed from the draft survey.

The key contact points also requested that the survey be made available in different languages. The feasibility of this was investigated but unfortunately the costs were prohibitive and there was no allowance made for this in the project budget. An offer was made to set up the survey in different languages if the key contact points arranged their own translations. Although some of the representatives indicated at the workshop that they may have been able to do this, the offer was not subsequently taken up.

It is possible that the language barrier may have contributed to some of the instances of incomplete responses.

Cultural

Following notification that the survey had been launched, it became apparent that the timing coincided with the celebration of the end of Ramadan. This may have impacted on the initial availability of some of the key contact points to promote the survey.

During the project workshop the group raised the importance of anonymity and confidentiality for survey responses. Privacy and security had been considered in the development of the survey and this was the reason for applying SSL encryption to the survey tool. The concerns raised however went further than this and there was a risk that potential respondents may not have been prepared to complete the survey if required to provide certain personal information. This was addressed by including information in the survey instructions to clarify what information was required, the reasons for this and how it would be used. The application of SSL encryption to the survey was also highlighted in the survey instructions and the introductory section of the online tool. Mandatory contact details were reduced to a minimum in the survey tool so that only the respondent’s name and email address were required information. It was not possible for the survey to be completely anonymous as there would be no way to verify that the data was genuine. It was also necessary to have some means of contacting the respondents if the data entered was incomplete or incorrect.

Technical

There were intermittent problems with the delivery of emails to some members of the key contact point group. This seemed to be related to server firewalls blocking particular emails. It was not always clear what was causing this to happen. It may have been related to the size or type of attachments. Participants at the workshop advised that some servers would only accept text emails and any communication containing a hyperlink would be blocked. It was difficult to know whether emails containing key project information had been received by all representatives. Read receipts were requested to address this issue. Although read receipts were useful in determining whether delivery of emails had been successful, it was sometimes difficult to know whether progress was being maintained. Mail undeliverable receipts were also occasionally received then recipients would subsequently confirm by read receipt that they had received the email.

Email addresses would work on some occasions and not on others. Messages were received that the recipients were not recognized by the server then recipients would communicate later by the same email address. Delivery would also depend on whether mailboxes were full.

This meant that considerable resources and time had to be dedicated to resending and following up on correspondence.

In these times of information overload, there were also the usual issues that individuals face with the management and prioritization of high volumes of emails. Regular two-way communication is critical to the success of any project of this nature and this point was highlighted during the training workshop. The majority of delegates took this on board and communication greatly improved in the subsequent period.

Maintaining momentum

Maintaining momentum on the project was crucial during the project and particularly during the time that the survey was live. The key contact point group was comprised of executives, senior managers and technical experts with high-level portfolios. This project was just one of their many daily priorities and responsibilities and this is perfectly understandable.

Managing the project remotely simplified the process but presented challenges as outlined above. The provision of regular project updates by email was the primary approach to ensuring that the project was kept in the forefront of people's minds.

These update emails were generally sent on the same day each week so that the representatives expected communications at that time. Delegates at the workshop confirmed that they appreciated the regular communication. Follow-up telephone calls were made as necessary and this was particularly important when organizing the workshop within a tight timeframe.

When the survey was launched on 1 October 2008 there was an initial flurry of activity and it appeared that the targets would soon be met. By the third week responses had dwindled to only one or two a day and this was a cause for concern. Information was urgently required on how the key contact points were progressing with the marketing of the survey. A reminder about sending activity reports was sent in the regular project update email. Outstanding activity reports were then followed up by personalized emails. Where reports still remained outstanding follow-up was made by telephone. The necessity for regular follow-up using diverse approaches was highlighted throughout the project. It is doubtful that momentum could have been maintained without these efforts.

During quieter periods, such as the earlier delay in the timetable, the project team dedicated time to reviewing the survey and developing essential support materials. Much of the planning and development work for the workshop took place during these periods. While the survey was live, the background detail on the report was drafted. Maintaining momentum in this way ensured that critical timelines were met and that any impact on the project from delays was kept to a minimum.

Level of involvement

At the commencement of the project, correspondence was sent to the National Standards Bodies in the APEC Member Economies requesting nominations for key contact points on the project. This correspondence outlined the responsibilities of the key contact points in relation to the project as follows:

- become thoroughly informed about the project, including its scope and objectives, along with the content of a security standards and support systems survey and supporting materials;
- attend a one-day training workshop to be held in a host APEC Member Economy (details to be advised following confirmation of attendee numbers). The purpose of this workshop was to provide training to participants about how to conduct the survey in their own APEC Member Economy;
- provide ongoing information and training to their deputy on all aspects of the project;

- identify approximately 200 representatives in security-related areas to participate in the survey and to provide contact details for these individuals to the project management team;
- provide ongoing support and advice to survey participants with the assistance of the project management team; and
- a commitment of time and effort until approximately late December 2008, after which collation and analysis of the survey results would commence.

The responsibilities of the key contact points were reinforced in project update emails throughout the period leading up to the survey.

The majority of the key contact points were committed to the process and made every effort to meet their obligations, however there were exceptions. The project team invested a great deal of time and resources in following up some individuals by email, fax and telephone. Some key contact points rarely responded to any communication during the project period, other than to provide read receipts. Although attendance at the project training workshop was acceptable with 13 out of 21 economies present, the project team would have preferred a higher level of participation. It was also apparent that a few representatives were not actively promoting the survey in their member economies. The minimal number of responses received from these member economies appeared to be in response to mail-outs from international security organizations, rather than the efforts of the representatives concerned. The level of analysis that could be provided from the data was limited as a consequence of targets not being met by all member economies. For example, analysis by APEC Member Economy would highlight the performance of individual member economies and this was not seen to be appropriate.

In the current uncertain global financial climate, it is even more important to ensure that funding and resources allocated to benefit the region are used wisely and well. The issues described above have the potential to impact on scoping for future APEC projects. For these reasons, it would be beneficial for member economies to consider the level of involvement that can be reasonably met when participating in projects and state this upfront. This may be a definite commitment to active involvement or simply a request to be included on communication mailing lists. Certainly, it is acknowledged that priorities and individual role responsibilities may change during the course of a project. Should a nominated representative be unable to fulfil their obligations due to changed circumstances, early advice of this would greatly assist project teams. This would provide an opportunity to identify an alternative representative on the project.

20. Key existing standards related to security

The following tables outline some existing international standards and guidelines related to security in the priority areas identified for each category. There are also a number of other standards that have security as an integrated component. Examples of such standards include construction, food safety, dangerous goods and the management of biological and radiological hazards.

Due to the volume of international standards available, it is not feasible to provide a complete list. There are many other specific international technical standards that meet particular industry requirements. In cases where international standards could not be identified, other sources of guidance are included in the table below as sources of reference. It is acknowledged that there are also national standards, legislation and other sources of guidance available under particular categories. As stated earlier, the inventory and gap analysis should also be considered in the context of important work undertaken and under development by major international organizations, such as the Red Cross, NFPA and ASIS International. References to relevant publications are included in the table below. Reference should also be made to the work undertaken by the SOM Special Task Forces on Emergency Preparedness (TFEP) and Counter-Terrorism (CTTF).

GOVERNANCE, STRATEGY & POLICY	
Effective Leadership	
	No international standards were identified that specifically related to Effective Leadership
Crisis Management	
Document #	**Title**
ISO/PAS 22399:2007	Societal security - Guideline for incident preparedness and operational continuity management
IWA 6:2008	Guidelines for the management of drinking water utilities under crisis conditions
Under development	
Document #	**Title**
ISO/WD 22300	Societal security - Fundamentals and vocabulary
Security Management	
Document #	**Title**
ISO 20828:2006	Road vehicles - Security certificate management
ISO 27799:2008	Health informatics - Information security management in health using ISO/IEC 27002

ISO 28000:2007	Specification for security management systems for the supply chain
ISO 28001:2007	Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance
ISO 28003:2007	Security management systems for the supply chain - Requirements for bodies providing audit and certification of supply chain security management systems
ISO 28004:2007	Security management systems for the supply chain - Guidelines for the implementation of ISO 28000
ISO/IEC 27005:2008	Information technology - Security techniques - Information security risk management
ISO/IEC 27006:2007	Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems
Under development	
Document #	**Title**
ISO/WD 22300	Societal security - Fundamentals and vocabulary
ISO/IEC FDIS 27011	Information technology -- Information security management guidelines for telecommunications organizations
ISO/IEC NP 27037	Information technology - Security techniques -- on Information security management: Sector to sector interworking and communications for industry and government
ISO/IEC NP 29146	Information technology - Security techniques - A framework for access management
ISO/IEC WD 24760	Information Technology -- Security Techniques -- A Framework for Identity Management
ISO/IEC WD 27007	Guidelines for Information security management systems auditing
RISK MANAGEMENT	
Emergency Management	
Document #	**Title**
ISO/PAS 22399:2007	Societal security - Guideline for incident preparedness and operational continuity management
ISO 21243:2008	Radiation protection - Performance criteria for laboratories performing cytogenetic triage for assessment of mass casualties in radiological or nuclear emergencies - General principles and application to dicentric assay
ISO 23269-1:2008	Ships and marine technology - Breathing apparatus for ships - Part 1: Emergency escape breathing devices (EEBD) for shipboard use
ISO 27991:2008	Ships and marine technology - Marine evacuation systems - Means of communication

ISO 30061:2007	Emergency lighting
ISO 7240-19:2007	Fire detection and alarm systems - Part 19: Design, installation, commissioning and service of sound systems for emergency purposes
ISO 8201:1987	Acoustics -- Audible emergency evacuation signal
IWA 5:2006	Emergency preparedness
ISO 8421-6:1987	Fire protection -- Vocabulary -- Part 6: Evacuation and means of escape
Under development	
Document #	**Title**
ISO/WD 22300	Societal security - Fundamentals and vocabulary
Risk Management	
Document #	**Title**
ISO/IEC TR 18044:2004 :	Information technology - Security techniques - Information security incident management
ISO 28000 - Supply Chain Security Management Systems Package	Specification for security management systems for the supply chain
ISO 28001:2007	Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance
IEC 60300-3-9 Ed. 1.0 b:1995	Dependability management - Part 3: Application guide - Section 9: Risk analysis of technological systems
IEC 62198 Ed. 1.0 b:2001	Project risk management - Application guidelines
ISO/IEC 27005:2008	Information technology - Security techniques - Information security risk management
ISO/IEC Guide 73:2002	Risk management -- Vocabulary -- Guidelines for use in standards
ISO/TS 16732:2005	Fire Safety Engineering -- Guidance on fire risk assessment
IEC 62305-2 Ed. 1.0 b:2006	Protection against lightning - Part 2: Risk management
ISO 14971:2007	Medical devices - Application of risk management to medical devices
ISO 15743:2008	Ergonomics of the thermal environment - Cold workplaces - Risk assessment and management
ISO 17666:2003	Space systems -- Risk management
ISO 22442-1:2007	Medical devices utilizing animal tissues and their derivatives - Part 1: Application of risk management
ISO/IEC 16085:2006	Systems and software engineering - Life cycle processes - Risk management
ISO/IEC TR 18044:2004	Information technology - Security techniques - Information security incident management
ISO/TS 20993:2006	Biological evaluation of medical devices - Guidance on a risk-management process
ISO/TS 22367:2008	Medical laboratories - Reduction of error through risk management and continual improvement

Under development	
Document #	**Title**
ISO/DIS 31000	Risk management - Principles and guidelines on implementation
IEC/DIS 31010	Risk management -- Risk assessment guidelines
ISO/DIS 13824	General principles on risk assessment of systems involving structures
ISO/IEC CD Guide 73	Risk management -- Vocabulary -- Guidelines for use
ISO/IEC NP 27033-4	Information technology -- Security techniques -- IT network security -- Part 4: Securing communications between networks using security gateways - Risks, design techniques and control issues
ISO/IEC NP 27033-5	Information technology -- Security techniques -- IT network security -- Part 5: Securing Remote Access - Risks, design techniques and control issues
ISO/IEC NP 27033-6	Information technology -- Security techniques -- IT network security -- Part 6: Securing communications across networks using Virtual Private Networks (VPNs) -- Risks, design techniques and control issues
ISO/IEC WD 27033-3	Information technology -- Security techniques -- IT network security -- Part 3: Reference networking scenarios -- Risks, design techniques and control issues
ISO/NP 28680	Health informatics -- Application of risk management for IT -- Networks incorporating medical devices
ISO/PRF TR 29322	Health informatics -- Guidance on the management of clinical risk relating to the deployment and use of health software systems
ISO/PRF TS 29321	Health Informatics -- Application of clinical risk management to the manufacture of health software
ISO/CD TS 10303-1467	Industrial automation systems and integration -- Product data representation and exchange -- Part 1467: Application module: Risk management
ISO/DIS 31000	Risk management -- Principles and guidelines on implementation
ISO/FDIS 10993-1	Biological evaluation of medical devices -- Part 1: Evaluation and testing within a risk management process
Command, control and communications	
Document #	**Title**
IEC 62290-1 Ed. 1.0 b:2006	Railway applications - Urban guided transport management and command/control systems - Part 1: System principles and fundamental concepts
Under development	
Document #	**Title**

ISO/NP 22320	Societal security - Principles for command and control, coordination and cooperation in resolving incidents
ISO/NP 22322	Societal security - Inter/Intra organisational warning procedures
INFORMATION SECURITY	
Network Security	
Document #	**Title**
ISO/IEC NP 27033	Information technology -- IT Network security
IEC/PAS 62443-3 Ed. 1.0 en:2008	Security for industrial process measurement and control - Network and system security
IEC/TS 62351-1 Ed. 1.0 en:2007	Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues
IEC/TS 62351-2 Ed. 1.0 en:2008	Power systems management and associated information exchange - Data and communications security - Part 2: Glossary of terms
IEC/TS 62351-3 Ed. 1.0 en:2007	Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP
IEC/TS 62351-4 Ed. 1.0 en:2007	Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS
IEC/TS 62351-6 Ed. 1.0 en:2007	Power systems management and associated information exchange - Data and communications security - Part 6: Security for IEC 61850
System Access Control	
Document #	**Title**
ISO/IEC 27002:2005	Information technology - Security techniques - Code of practice for information security management (Redesignation of ISO/IEC 17799:2005)
ISO/IEC 10164-9:1995	Information technology - Open Systems Interconnection - Systems Management: Part 9: Objects and attributes for access control
ISO/IEC 10181-3:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Part 3: Access control framework
ISO/IEC NP 29146	Information technology - Security techniques - A framework for access management
Information Security	
Document #	**Title**

ISO/IEC FDIS 27000	Information technology - Security techniques - Information security management systems – Overview and vocabulary
ISO/IEC 27001 Series including (1, 2, 5 & 6) published and (0, 3, 4, 7, 8, 11, 31, 33 & 34) under development.	Information technology - Security techniques - Information security management systems
ISO/IEC 27002:2005	Information technology - Security techniques - Code of practice for information security management (Redesignation of ISO/IEC 17799:2005)
ISO/IEC 38500:2008	Corporate governance of information technology
ISO/IEC 23988:2007	Information technology - A code of practice for the use of information technology (IT) in the delivery of assessments
ISO/IEC 10181-1:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Part1: Overview
ISO/IEC 10181-2:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Part 2: Authentication framework
ISO/IEC 10181-3:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Part 3: Access control framework
ISO/IEC 10181-4:1997	Information technology - Open Systems Interconnection - Security frameworks for open systems: Part 4: Non-repudiation framework -
ISO/IEC 10181-5:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Part 5: Confidentiality framework
ISO/IEC 10181-6:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Part 6: Integrity framework
ISO/IEC 10181-7:1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Part 7: Security audit and alarms framework
ISO/IEC 10164-8:1993	Information technology - Open Systems Interconnection - Systems Management: Part 8: Security audit trail function
ISO/IEC 23988:2007	Information technology - A code of practice for the use of information technology (IT) in the delivery of assessments
ISO/IEC DIS 20886	Information technology - International Security, Trust, and Privacy Alliance - Privacy Framework
ISO/TR 13569:2005	Financial services -- Information security guidelines
ISO 22857:2004	Health informatics -- Guidelines on data protection to facilitate trans-border flows of personal health information
ISO 27799:2008	Health informatics - Information security management in health using ISO/IEC 27002
ISO/TR 22221:2006	Health informatics - Good principles and practices for a clinical data warehouse
ISO/IEC 18028-1:2006	Information technology - Security techniques - IT network

	security - Part 1: Network security management
ISO/IEC 18028-2:2006	Information technology - Security techniques - IT network security - Part 2: Network security architecture
ISO/IEC 18028-3:2005	Information technology - Security techniques - IT network security - Part 3: Securing communications between networks using security gateways
ISO/IEC 18028-4:2005	Information technology - Security techniques - IT network security - Part 4: Securing remote access
ISO/IEC 18028-5:2006	Information technology - Security techniques - IT network security - Part 5: Securing communications across networks using virtual private networks
HB 171-2003 [11]	Guidelines of Management of IT Evidence
PERSONNEL SECURITY	
Security Training Systems for Staff	
Document #	**Title**
ISO 10015:1999	Quality management – Guidelines for training
ISO/IEC 23988:2007	Information technology - A code of practice for the use of information technology (IT) in the delivery of assessments
Building and Facility Access Control	
Document #	**Title**
ASIS GDL FPSM DRAFT	Draft Facilities Physical Security Measures Guideline (2008)
ISO/IEC 27002:2005	Information technology - Security techniques - Code of practice for information security management
Pre-Employment Screening	
Document #	**Title**
	No international standards could be identified however Standards Australia has developed the following standard and guidelines: AS 4811-2006 Employment screening Employment Screening Handbook (HB 323 – 2007) Reference Checking in the Financial Services Industry Handbook (HB 322 - 2007) - developed in conjunction with the Australian Securities and Investments Commission (ASIC) and a panel of industry experts.

[11] This handbook added following a suggestion during the comment period on the draft report.

Under development	
Document #	**Title**
ASIS GDL PBS 09 2006	ASIS International Pre-employment Background Screening Draft Guideline
PHYSICAL SECURITY	
Security of facility utilities	
Document #	**Title**
ISO 24511:2007	Activities relating to drinking water and wastewater services - Guidelines for the management of wastewater utilities and for the assessment of wastewater services
IWA 6:2008	Guidelines for the management of drinking water utilities under crisis conditions
IEC/TS 61085 Ed. 1.0 b:1992	General considerations for telecommunication services for electric power systems
IEC/TR 62210 Ed. 1.0 en:2003	Power system control and associated communications - Data and communication security
Perimeter security	
Document #	**Title**
ISO/CIE FDIS 26182	Lighting of outdoor work places - Lighting requirements for safety and security
ISO/CIE 8995-3:2006	Lighting of work places - Part 3: Lighting requirements for safety and security of outdoor work places
ISO 10333-5:2001	Personal fall-arrest systems -- Part 5: Connectors with self-closing and self-locking gates
ISO 5996:1984	Cast iron gate valves
ISO 6002:1992	Bolted bonnet steel gate valves
Construction security	
Document #	**Title**
IEC 60371-3-8 Amd.1 Ed. 1.0 en:2007	Amendment 1 - Insulating materials based on mica - Part 3: Specifications for individual materials - Sheet 8: Mica paper tapes for flame-resistant security cables
IEC 60371-3-8 Ed. 1.0 b:1995	Insulating materials based on mica - Part 3: Specifications for individual materials - Sheet 8: Mica paper tapes for flame-resistant security cables
IEC 62305-3 Ed. 1.0 b:2006	Protection against lightning - Part 3: Physical damage to structures and life hazard
ISO 14520-1/Cor1:2007	Gaseous fire-extinguishing systems - Physical properties and system design - Part 1: General requirements - Corrigendum
ISO 14520-1:2006	Gaseous fire-extinguishing systems -- Physical properties and system design -- Part 1: General requirements

ISO 14520-2:2006	Gaseous fire-extinguishing systems -- Physical properties and system design -- Part 2: CF3I extinguishant
ISO 14520-5:2006	Gaseous fire-extinguishing systems -- Physical properties and system design -- Part 5: FK-5-1-12 extinguishant
ISO 14520-6:2006	Gaseous fire-extinguishing systems -- Physical properties and system design -- Part 6: HCFC Blend A extinguishant
ISO 14520-8:2006	Gaseous fire-extinguishing systems -- Physical properties and system design -- Part 8: HFC 125 extinguishant
ISO 14520-9:2006	Gaseous fire-extinguishing systems -- Physical properties and system design -- Part 9: HFC 227ea extinguishant
ISO 14520-10:2005	Gaseous fire-extinguishing systems -- Physical properties and system design -- Part 10: HFC 23 extinguishant
ISO 14520-11:2005	Gaseous fire-extinguishing systems -- Physical properties and system design -- Part 11: HFC 236fa extinguishant
ISO 14520-12:2005	Gaseous fire-extinguishing systems -- Physical properties and system design -- Part 12: IG-01 extinguishant
ISO 14520-13:2005	Gaseous fire-extinguishing systems -- Physical properties and system design -- Part 13: IG-100 extinguishant
ISO 14520-14:2005	Gaseous fire-extinguishing systems -- Physical properties and system design -- Part 14: IG-55 extinguishant
ISO 14520-15:2005	Gaseous fire-extinguishing systems -- Physical properties and system design -- Part 15: IG-541 extinguishant
ISO 3049:1974	Gypsum plasters -- Determination of physical properties of powder
ISO 3129:1975	Wood -- Sampling methods and general requirements for physical and mechanical tests
ISO 3130:1975	Wood -- Determination of moisture content for physical and mechanical tests
ISO 3131:1975	Wood -- Determination of density for physical and mechanical tests
ISO 6742-1:1987	Cycles -- Lighting and retro-reflective devices -- Photometric and physical requirements -- Part 1: Lighting equipment
ISO 6742-2:1985	Cycles -- Lighting and retro-reflective devices -- Photometric and physical requirements -- Part 2: Retro-reflective devices
ISO 7345:1897	Thermal insulation -- Physical quantities and definitions
ISO 9288:1989	Thermal insulation -- Heat transfer by radiation -- Physical quantities and definitions
ISO 9346:2007	Hygrothermal performance of buildings and building materials - Physical quantities for mass transfer - Vocabulary
ISO/CIE 23539:2005	Photometry -- The CIE system of physical photometry
ISO/TR 15655:2003	Fire resistance -- Tests for thermo-physical and mechanical properties of structural materials at elevated temperatures for fire engineering design
ISO 16932:2007	Glass in building - Destructive-windstorm-resistant security glazing - Test and classification

ISO 16933:2007	Glass in building - Explosion-resistant security glazing - Test and classification for arena air-blast loading
ISO 16934:2007	Glass in building - Explosion-resistant security glazing - Test and classification by shock-tube loading
ISO 16935:2007	Glass in building - Bullet-resistant security glazing - Test and classification
ISO 16936-1:2005	Glass in building -- Forced-entry security glazing -- Part 1: Test and classification by repetitive ball drop
ISO 16936-2:2005	Glass in building -- Forced-entry security glazing -- Part 2: Test and classification by repetitive impact of a hammer and axe at room temperature
ISO 16936-3:2005	Glass in building -- Forced-entry security glazing -- Part 3: Test and classification by manual attack
ISO 16936-4:2005	Glass in building -- Forced-entry security glazing -- Part 4: Test and classification by pendulum impact under thermally and fire stressed conditions
ISO/TS 13474:2003	Acoustics -- Impulse sound propagation for environmental noise assessment
ISO 3009:2003	Fire-resistance tests -- Elements of building construction -- Glazed elements
ISO 16852:2008	Flame arresters - Performance requirements, test methods and limits for use
ISO 6184-1:1985	Explosion protection systems -- Part 1: Determination of explosion indices of combustible dusts in air
ISO 6184-2:1985	Explosion protection systems -- Part 2: Determination of explosion indices of combustible gases in air
ISO 6184-3:1985	Explosion protection systems -- Part 3: Determination of explosion indices of fuel/air mixtures other than dust/air and gas/air mixtures
ISO 6184-4:1985	Explosion protection systems -- Part 4: Determination of efficacy of explosion suppression systems
ISO 10077-2:2003	Thermal performance of windows, doors and shutters -- Calculation of thermal transmittance -- Part 2: Numerical method for frames
ISO 10137:2007	Bases for design of structures - Serviceability of buildings and walkways against vibrations
ISO 10721-1:1997	Steel structures -- Part 1: Materials and design
ISO 16587:2004	Mechanical vibration and shock -- Performance parameters for condition monitoring of structures
ISO 16670:2003	Timber structures -- Joints made with mechanical fasteners -- Quasi-static reversed-cyclic test method
ISO 21927-1:2008	Smoke and heat control systems - Part 1: Specification for smoke barriers
ISO 22111:2007	Bases for design of structures - General requirements
ISO 22846-1:2003	Personal equipment for protection against falls -- Rope access systems -- Part 1: Fundamental principles for a system of work

ISO 22965-1:2007	Concrete - Part 1: Methods of specifying and guidance for the specifier
ISO 22965-2:2007	Concrete - Part 2: Specification of constituent materials, production of concrete and compliance of concrete
ISO 4356:1977	Bases for the design of structures -- Deformations of buildings at the serviceability limit states
ISO 4435:2003	Plastics piping systems for non-pressure underground drainage and sewerage -- Unplasticized poly(vinyl chloride) (PVC-U)
ISO 6781:1983	Thermal insulation -- Qualitative detection of thermal irregularities in building envelopes -- Infrared method
ISO 6897:1984	Guidelines for the evaluation of the response of occupants of fixed structures, especially buildings and off-shore structures, to low-frequency horizontal motion (0,063 to 1 Hz)
ISO 7240-16:2007	Fire detection and alarm systems - Part 16: Sound system control and indicating equipment
ISO 7626-2:1990	Vibration and shock -- Experimental determination of mechanical mobility -- Part 2: Measurements using single-point translation excitation with an attached vibration exciter
ISO 8772:2006	Plastics piping systems for non-pressure underground drainage and sewerage - Polyethylene (PE)
ISO 8773:2006	Plastics piping systems for non-pressure underground drainage and sewerage - Polypropylene (PP)
ISO/DIS 13824	General principles on risk assessment of systems involving structures
ISO/IEC Guide 50:2002	Safety aspects -- Guidelines for child safety
ISO/TS 16733:2006	Fire safety engineering - Selection of design fire scenarios and design fires
ISO/TS 22559-1:2004	Safety requirements for lifts (elevators) -- Part 1: Global essential safety requirements (GESRs)
ISO 16368:2003	Mobile elevating work platforms -- Design calculations, safety requirements and test methods
ICC IFC-2006	International Fire Code, 2006

21. Abbreviations and Acronyms

ABAC	APEC Business Advisory Council
APEC	Asia-Pacific Economic Cooperation
ASIC	Australian Securities and Investments Commission
ASIS	ASIS International
CCTV	Closed circuit television
CEO	Chief Executive Officer
CEOs	Chief Executive Officers
CISSS	Critical Infrastructure and Support Systems Standardization
CTTF	Counter Terrorism Task Force
NFPA	National Fire Protection Association
PASC	Pacific Area Standards Congress
SAG-S	ISO/IEC/ITU-T Strategic Advisory Group on Security
SCSC	APEC Sub-Committee on Standards and Conformance
SOM	Senior Officials' Meeting
TFEP	Task Force for Emergency Preparedness
TISN	The Trusted Information Sharing Network for Critical Infrastructure Protection

22. Attachments

Please note that the attachments are available for reference as a separate .zip file.

1. Project plan
2. Background paper
3. Instructions
4. Glossary
5. Hard copy of online survey instrument
6. About Standards Australia

APEC
Asia-Pacific
Economic Cooperation

Project Plan

Critical Infrastructure and Support Systems Standardization Project

A Standards Australia and APEC initiative to promote a better standards infrastructure for security

June 2008
Prepared by: Mark Bezzina

Table of Contents

Project data

Purpose

This document has been created to provide Standards Australia with a detailed project plan for the Critical Infrastructure and Support Systems Standardization Project.

Project duration

The project will run for 12 months.

Key contacts

The Critical Infrastructure and Support Systems Standardization Project is managed by Standards Australia. The funding for this project has been provided by APEC and Standards Australia. StanCert Pty Ltd is the Project Manager.

The Project Supervisor is:

Karen Hitchiner
Manager International Development
Standards Australia
Phone: +64 4 498 5945
Mobile: +64 2102 475 926 (New Zealand)
+61 404 806 241 (Australia)
Email: Karen.hitchiner@standards.org.au

The APEC Project Sponsor is:

Brian Phillips
Manager, Standards & International Liaison
Industry & Small Business Policy Division
Department of Innovation, Industry, Science and Research
Phone: +61 2 6213 6156
Mobile: +61 402 438426
Email: brian.phillips@innovation.gov.au

The Team Leader is:

Mark Bezzina
Managing Director of StanCert Pty Ltd
Consultant to Standards Australia
Phone: +61 2 8721 6434
Mobile: +61 413 101 096
Email: bezzina@stancert.com

The Lead Consultant is:

Clare Morrison
Stancert Pty Ltd
Phone: +61 2 8721 6434
Mobile: + 61 430 333 008
Email: cmorrison@stancert.com

Project scope and objectives

The Critical Infrastructure and Support Systems Standardization Project is designed to assist in the development of a framework to address the need to protect critical infrastructure in times of emergencies, whether these be caused by natural disasters or criminal activity.

This is an agreed Sub-Committee on Standards and Conformance (SCSC) APEC's Second Trade Facilitation Action Plan (TFAP II) activity. In particular, it will promote security standards and systems capacity which support business. Building technical capacity for developing APEC member economies will be a key focus. The project will also promote the harmonization of related standards across the APEC region. This will help improve the interoperability, and compatibility of systems related to securing critical infrastructure.

The project aims to:

- Identify and detail some of the issues, barriers and solutions related to protecting critical infrastructure and identify user perceptions of the importance of standards related to securing critical infrastructure. Critical infrastructure includes, but is not limited to:
  - Power supply
  - Water
  - Telecommunications
  - Financial Services Sector
  - Banking and finance
  - Public events and mass gathering
  - Transport
  - Health
  - Operation of government
  - Food
  - Essential manufacturing

- Identify and prioritise the standards required by the owners and operators of critical infrastructure and identify the gaps between existing standards and the needs of the owners and operators of critical infrastructure.

- Make recommendations on how the gaps in standards may be addressed and develop a blueprint for the development of a standards framework that is essential in identifying and categorising security standards.

Project methodology overview

In brief, the Project methodology will take the following form:

0. Project management
1. Preparation
2. Capacity building
3. Consultation
4. Analysis and validation
5. Reporting and communicating results

The project facilitators will conduct a workshop to provide guidance to participating APEC members on how to carry out their own member economy survey to establish a baseline. Ongoing instruction and support will be provided remotely during the project.

At the completion of the in-member economy survey, the Project leaders will interpret the survey data and report on the results.

A report will be created addressing the Project aims and possible follow up activities will be identified.

Much of this work will be based on the methodology used in a similar project previously undertaken by Australia.

Project timeline

The detailed project timeline is shown in Appendix 1.

The duration in the bars shows the amount of time allowed to complete each task rather than effort.

This project plan does not take into consideration the human resources required by the APEC Member Economy National Standards Bodies to carry out the project or attend meetings.

Project Tasks

A detailed overview of the project tasks is outlined in Table 1 below.

TABLE 1 EXPLANATION OF PROJECT TASKS

Stage	Activity Name	Activity Description
0	Project management	This activity is aimed at the effective management of the Project and runs for the duration of the Project. It includes such activities as progress reporting, accounting, project meetings and legal review.
1	Preparation	The project will be administered by Standards Australia and StanCert however APEC Member Economy National Standards Bodies will be required to administer a survey and carry out analysis within their own economy. Standards Australia and StanCert will provide the tools and support to assist with this process. Each APEC Member Economy National Standards Body will be asked to nominate a key contact point to work on the project. Whilst this project's objectives are entirely focused on technical issues and are neutral regarding gender criteria the project will ask for preference to be given for women to act as contact points from APEC Member Economy National Standards Bodies in conducting the Critical Infrastructure and Support Systems Standardisation Project. The initial phase of the Project will involve the development of a project plan and background paper. The project plan and background paper will be used to communicate the project and seek support and commitment from key parties. The project plan will identify the detailed steps and responsibilities involved in the project. The background paper will be developed to provide background and overview for the project. After receiving the support of APEC Member Economy National Standards Bodies, a survey based on the Australian survey will be developed.

Stage	Activity Name	Activity Description
		The purpose of the survey will be to seek structured feedback on the priorities for security related standards from the owners and operators of critical infrastructure within the APEC region. APEC Member Economy National Standards Bodies will be asked to review and approve the project plan (by correspondence). At the same time, feedback will be sought on the background paper and survey. Both the background paper and survey will be updated as a result of the feedback received. **Outputs:** • Detailed project plan • Project background paper • Survey instrument
2	Capability building	APEC Member Economy National Standards Bodies will each be instructed by Standards Australia and StanCert on how to conduct the survey assessment. This instruction will be done at a 1 day workshop in a central location attended by the nominated contact points of each APEC Member Economy National Standards Body. **Outputs:** • Development of a 1 day workshop including presentations and guidance material on carrying out the survey in the member economy.
3	Consultation	APEC Member Economy National Standards Bodies will administer their survey and encourage their stakeholders to complete the survey. It is anticipated that the survey will be completed by the owners and operators of critical infrastructure within the APEC Member Economy. **Outputs:** • Completed survey results
4	Analysis and validation	Standards Australia and StanCert will assist APEC Member Economy National Standards Bodies to follow up late and incomplete survey responses.

Stage	Activity Name	Activity Description
		After a sufficient number of surveys are received work will begin on consolidating and interpreting the results. A draft report will be produced. **Outputs:** • Interim project draft report
5	Reporting and communicating results	The consolidated responses to the survey will be published in a report. An APEC/industry event (adjacent to an ABAC/regional standards meeting) will be planned to communicate the draft results from the project to APEC member economies and the Asia-Pacific Standards Community. Stakeholders will be given 4 weeks following the presentation to make any final comments before the report is finalised for consideration at SOM III. The report will identify a number of recommendations and these will form the basis of a future work plan for APEC member economies in conjunction with ABAC. **Outputs:** • Meeting to discuss results • Final draft report • Launch of report

Further Information

For further information please contact:

Clare Morrison, Lead Consultant, StanCert Pty Ltd cmorrison@stancert.com

Mark Bezzina, Executive Director, StanCert Pty Ltd bezzina@stancert.com

Background Paper

Critical Infrastructure and Support Systems Standardization Project

2008

Authored by: Mark Bezzina

Table of Contents

Purpose

This background paper has been prepared to communicate to key stakeholders the purpose, methodology and expected outcomes of the Critical Infrastructure and Support Systems Standardization Project (The Project).

Background and introduction

Standards play a number of important roles in supporting efforts to achieve security. For example standards can be used to:

- promulgate best practices and methodologies for security management.
- specify test methods and parameters to aid in detection of threats.
- specify performance requirements to ensure equipment and systems provide the necessary performance and protection in extreme conditions.

The Project will assist in the development of a proposed framework of standards to address the need to protect critical infrastructure in times of emergencies, whether these be caused by natural disasters or criminal activity.

It will also promote security standards and systems capacity which support business as well as critical infrastructure in government control.

Building technical capacity for developing Asia-Pacific Economic Cooperation (APEC) member economies will be a key focus. This capacity building will involve assisting developing economies survey the needs of standards users to ascertain key areas of standardisation focus as well as help target programs for the development of security standards.

The project will also promote the harmonisation of related standards across the APEC region - this will help improve the interoperability, and compatibility of systems related to securing critical infrastructure.

The main beneficiary of this project is the business community of APEC Member Economies, as it will contribute to a higher degree of security of critical infrastructure as a result of standardised and tested security management systems needed to meet emergency situations.

The standards identified as a result of this project will also assist member economies and the owners of critical infrastructure to make more informed choices about effective security solutions through better access to information on tested and consistent methods to protect critical infrastructure.

This project is the result of a proposal by APEC Business Advisory Council (ABAC) presented at CTI III 2007 that the SCSC undertake work to assist with business continuity through periods of natural disaster and other major disruptions.

This proposal was endorsed by the APEC Sub-Committee on Standards and Conformance (SCSC) and the APEC Committee on Trade and Investment (CTI). The agreed proposal stems from similar work recently undertaken by Standards Australia. ABAC presented the proposal at the April 2007 Pacific Area Standards Congress (PASC), where it was also unanimously supported. Australia believes that APEC is the most appropriate organisation to assist in funding the project given the project's regional focus - all APEC members stand to benefit from its outcomes should they choose to participate, particularly developing members for whom the project will be an important capacity building exercise. Australia through its National Standards Body, Standards Australia has committed to contribute significant funding to the project in addition to valuable intellectual property and expertise.

This project will build on other surveys conducted by the ISO/IEC/ITU-T Strategic Advisory Group on Security (SAG-S) as well as ISO TC 223 that focuses on societal security. Additionally, the project will liaise closely with these two bodies throughout the conduct of the project.

This APEC project proposal is based on a similar initiative funded by the Critical Infrastructure Protection Branch of the Australian Commonwealth Attorney-Generals Department. This earlier project was initiated to complement Australia's critical infrastructure protection arrangements. The Australian Government takes an indirect approach to helping businesses manage their security risks by influencing and encouraging the development of best practice policies and procedures as an alternative to regulation. Standards Australia worked with the Australian Government to examine gaps in the existing library of security standards, and to develop an integrated security standards framework. This has produced several new and revised standards and guidelines applicable to safeguarding critical infrastructure and managing business continuity, and mapped the direction and priority for future standards development.

The Project

Key objectives

The key project objectives are:

1. Identify and detail some of the issues, barriers and solutions related to protecting critical infrastructure and identify user perceptions of the importance of standards related to securing critical infrastructure;

2. Identify and prioritise the standards required by the owners and operators of critical infrastructure and identify the gaps between existing standards and the needs of the owners and operators of critical infrastructure;

3. Make recommendations on how the gaps in standards may be addressed and develop a blueprint for the development of a security standards framework that is essential in identifying and categorising security standards.

An all hazards approach is being taken to threats. This approach includes security threats such as where someone has the capability, intent and opportunity to exploit a vulnerability to do harm; and accidents and natural disasters that may also cause inadvertent harm due to the existence of vulnerability.

The reason for this all hazards approach is to ensure that where possible multiple risks are dealt with by effective and integrated treatments, such as standardised products and services. The resultant standards can be developed in a modular fashion or in such a way as to not cause additional vulnerabilities by describing key aspects of security that can form the basis for new attacks.

Critical infrastructure can be damaged or destroyed by a number of factors including the following:

- Natural disasters
- Negligence
- Accidents
- Terrorism
- Hacking and vandalism
- Criminal activity
- Malicious damage

The standards identified under this project should assist the owners and operators of privately owned critical infrastructure to:

- provide adequate security for their assets
- actively apply risk management techniques to their planning processes
- conduct regular reviews of risk management plans
- report any incidents or suspicious activities to the police
- develop and regularly review business continuity plans, and
- participate in any exercises to test plans conducted by government authorities.

A very important aspect of this project is that it needs to be supported and driven by the owners and operators of critical infrastructure.

It is anticipated that the project will focus on elements of critical infrastructure as shown in Table 1.

TABLE 1 ELEMENTS OF CRITICAL INFRASTRUCTURE

Sectors	Sub Sectors
Energy	Gas, petroleum fuels, electricity generation, transmission and distribution.
Utilities	Water, waste water and waste management.
Transport	Air, road, sea, rail and inter-modal (cargo distribution centres)
Communications	Telecommunications (phone, fax, Internet, cable, satellites), electronic mass communications and postal services.
Health	Hospitals, public health and research and development laboratories.
Food supply	Bulk production, storage and distribution.
Finance	Banking, insurance and trading exchanges.
Government services	Defence and intelligence facilities, houses of parliament, key government departments, foreign missions, key residences, emergency services (police, fire, ambulance and others) and nuclear facilities.
National icons	Buildings, cultural, sport and tourism.
Essential manufacturing	Defence industry, heavy industry and chemicals.

Project Output

The major project output will be a final report that contains the following elements:

1. An outline of some of the issues, barriers and solutions related to protecting critical infrastructure and a summary of user perceptions of the importance of standards related to securing critical infrastructure.

2. A suggested list of the standards required by the owners and operators of critical infrastructure and the identification of gaps between existing standards and the needs of the owners and operators of critical infrastructure.

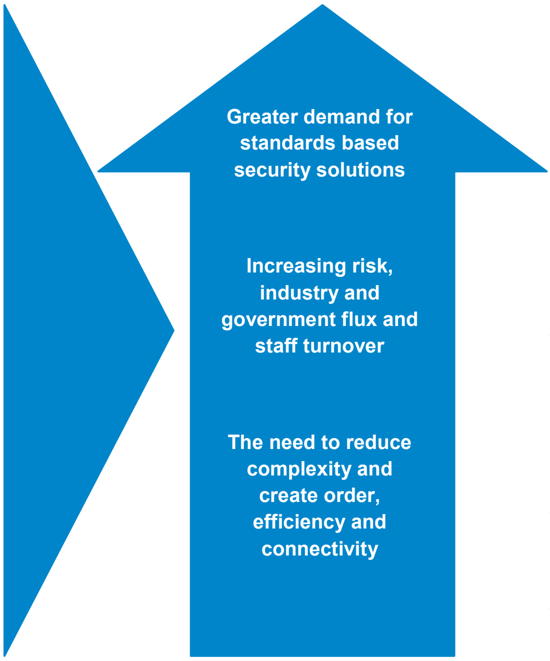
3. Clear recommendations on how the gaps in standards may be addressed and a blueprint for the development of a standards framework that is essential in identifying and categorising security standards.

Drivers for the Project

The Critical Infrastructure and Support Systems Standardisation Project is necessary because there is a very real need for simple and agreed standards to protect infrastructure. This guidance is necessary due to the many drivers that are shown in Figure 1.

FIGURE 1 DRIVERS FOR SECURITY STANDARDS

- Demand to manage security risks and compliance to protect assets and the community
- Transfer of infrastructure from public to private companies
- The need for documents with authority that have been developed through a formal process of openness, transparency and consensus
- The need for documents developed by an impartial body not bound by any jurisdiction
- The need for simple and agreed guidance
- The heightened threat of terrorist attack
- Community concerns about security and privacy
- Regulation (light touch)
- Demand for food and supply chain security
- Demand for indicative assurance confidence and consensus
- The need for collaboration in the development of systems


Greater demand for standards based security solutions
Increasing risk, industry and government flux and staff turnover
The need to reduce complexity and create order, efficiency and connectivity

Integrated security standards framework

Traditionally standards develop in a bottom up fashion. This occurs because industry experts working in a particular field identify a need for a new standard. For example an Information Technology (IT) expert may want to exchange secure data, so they recommend the development of a new cryptography standard. This is a valid approach to standards development, however such an approach makes it difficult to prioritise and resource standards development projects. Additionally there may be whole new areas where standards are required but work does not proceed because there is not an existing committee in place. It is also difficult to ensure coordination within and among committees responsible for preparing standards on different products, processes or services which is necessary to achieve a coherent approach to the treatment of security.

To address this problem a top down approach should complement the bottom up approach to standards development. A top down approach would involve looking at the entire area of security and identifying where standards are required and should have priority.

It is impossible to effectively and comprehensively apply a top down approach without some framework to identify all the areas covered by standards development. For this purpose it is suggested that a security standards framework be established.

The use of a framework is recommended to ensure that each specialised standard is restricted to specific aspects and makes reference to wider ranging standards for all other relevant aspects. The structure is built on the following types of standards:

- Basic security standards, comprising fundamental concepts, principles and requirements with regard to general security applicable to a wide range of products, processes and services.
- Group security standards, comprising security applicable to several or a family of similar products, processes or services dealt with by more than one committee, making reference, as far as possible, to basic security standards.
- Security product standards, comprising security aspect(s) for a specific, or a family of product(s), process(es) or service(s) within the scope of a single committee, making reference, as far as possible, to basic security standards and group security standards.
- Product standards containing security aspects but which do not deal exclusively with security aspects; these should make reference to basic security standards and group security standards.

Keeping in mind the purpose, it is important that any framework addresses the following criteria.

1. Identify the broad areas that require security standards.

2. Simple, communicable and easily understood.

3. Provide the basis for categorising, managing the scope and taking stock of existing standards activities as well as identifying gaps and priority areas.

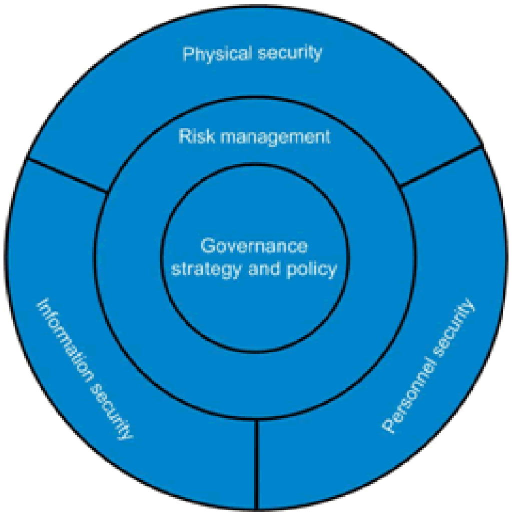
4. Supported by key stakeholders.

5. Widely used, openly available and unencumbered by intellectual property protection.

Standards Australia's National Centre for Security Standards (NCSS) Model

Standards Australia's National Centre for Security Standards (NCSS) has commenced work on developing an integrated security standards framework. A proposed revised framework was recommended on the basis of results from the Australian Security Standards and Support System. The proposed revised framework is presented in Figure 2. It is anticipated that this project will utilise and extend this framework. The key components of the model are explained below.

FIGURE 2 INTEGRATED SECURITY STANDARDS FRAMEWORK



Governance, strategy and policy

This element encapsulates product and systems standards related to the overall governance and management of an organisation with respect to security.

The focus of this element is on the continued ability of an organisation to achieve its strategy, objectives and targets.

To achieve the organisational strategy it is necessary to have in place a rigorous system that assists with the identification, quantification and categorisation of tangible (physical) and intangible (information and people) assets in relation to their importance in achieving the organisational strategy. The reason why such a process is necessary is that it ensures the level of security chosen for a given asset is fit for purpose or based on the value of the asset in terms of its impact on the organisation.

Other important aspects of this element include legal compliance management, communications and media management, audit, compliance and management review mechanisms for the purposes of continuous improvement. This element also includes standards designed to manage outsourcing and the purchasing of security services or services that impact on security as well as reporting incidents and issues management.

Risk management

The risk management element includes all standards and supporting material associated with risk management including:

- Systems to assist with monitoring the environment and intelligence gathering, such as examining the social, political and economic environment.
- Understanding interdependencies, intents, capabilities and threats.
- Tools to help establish the security context.
- Risk identification, analysis, evaluation, treatment, communication and monitoring.

This element encompasses business continuity management, which is one possible risk mitigation strategy. Business continuity management involves preparing for the eventuality of an event or incident by having in place a pre-developed and practiced emergency response, continuity response and ultimate recovery strategy.

Information security

The information security element includes all standards and supporting material associated with an integrated system for the management of information security. This element deals with the confidentiality, integrity and availability of information and encompasses such things as document, data and records control. It also addresses the security of networks, hardware, software, communications and supporting processes.

Personnel security

Personnel security involves a procedural system implemented to ensure that only those people whose work responsibilities require them to access official information and assets have such access. This is done by limiting the number of people who have access to those who can demonstrate a need to know or a need to have access and whose eligibility has been determined after an evaluation of their history, attitudes, values and behaviour.

The personnel security element includes all standards and supporting material associated with an integrated system for the management of personnel security. Personnel security standards encompass occupational health and safety, pre-employment screening, privacy, administrative records, security roles and responsibilities, induction and training, identity management, access control (employees and other), protecting individuals, working from home and the security of employees when working overseas.

Physical security

Physical security is the part of security concerned with the provision and maintenance of a safe and secure environment for the protection of the organisation's employees and clients. This includes physical measures designed to prevent unauthorised access to official resources and to detect and respond to intruders.

The physical security element includes all standards and supporting material associated with an integrated system for the management of physical security. Physical security standards include access to security advice from professionals, security equipment requirements, site selection, design security, building security, perimeter security, lighting, alarms, safes and strong rooms, guards, patrols and control rooms, CCTV and emergency planning and incident procedures.

Conclusion

The impetus for this Project came from the need to refocus on security in the Asia-Pacific Region following events such as natural disasters and criminal activity in recent times. It builds on the outcomes of a similar initiative that was undertaken in Australia.

The pressure on security professionals and businesses to manage and respond appropriately to security threats has never been greater. Good security standards provide essential information, advice and benchmarks to guide reasonable and prudent decisions. Fundamentally, standards articulate best practice.

The Project will aim to identify where gaps exist in the existing standards and recommend priorities for the development of future standards. There will be a solution oriented approach to barriers identified relating to protecting critical infrastructure. Most importantly, the Project will provide a blueprint for the development of a standards framework for identifying and categorising security standards.

The benefits to APEC Member Economies from participation in this project are:

- a more consistent approach to security along with emergency and disaster management in the APEC region;
- the promotion of security standards and systems capacity which support business as well as critical infrastructure in times of emergency, helping to minimise impact on economies;
- harmonisation of related standards across the APEC region, which will help improve the interoperability and compatibility of systems related to securing critical infrastructure;
- improved technical capacity through assistance in ascertaining key areas of standardisation focus so that programs may be targeted for the development of security standards; and
- the capacity to make more informed choices about effective security solutions through better access to information on tested and consistent methods to protect critical infrastructure.

The success of this project will, to a large extent, depend on each APEC Member Economy’s commitment to engaging actively in the process in order to achieve shared objectives for security in the Asia-Pacific Region.

Asia-Pacific
Economic Cooperation

Instructions

Critical Infrastructure and Support Systems Standardization Survey

Year 2008
Authored by: Mark Bezzina
StanCert Pty Ltd

TABLE OF CONTENTS

Critical Infrastructure and Support Systems Standardization Survey

Survey - Page 1

1. Introduction

This page is an introduction to the survey. The key project documents can be viewed, downloaded and printed from this page. In addition to these instructions the project documents include:

- a .PDF version of the survey for reference
- Project Plan
- Background Paper
- Glossary of definitions for the key terms used in the survey.

You will require a software application for viewing .PDF files, such as Adobe Reader, in order to access these documents.

It is recommended that you become familiar with the project documents before commencing the survey.

The survey must be completed in one sitting. Estimated time for completion is 15 minutes. The survey is not limited to one respondent per organisation. There are no limits to the number of responses from people working for the same organisation. We are seeking responses from well informed individuals rather than organisational responses.

The survey does not have a spell checker. If you require a spell checker it is suggested that you draft responses to the open ended questions in Word before commencing the survey. Some internet browsers have a spell checking feature. Another option is the latest Google toolbar, which has a built-in spell checker.

The survey does not have a print preview or print option. However the survey can be printed page by page from your internet browser. A PDF version of the survey can be downloaded and printed from the Introduction page. The PDF version is for reference only and it is not possible to complete this document as a form in soft copy. If you attempt to do this the information that has been entered will not be saved. If you do not have access to the internet and are unable to complete the survey online please email Clare Morrison, Lead Consultant, at cmorrison@stancert.com about other options.

SSL encryption has been applied to the survey to protect the confidentiality of responses. The data will be analysed and reported to Asia-Pacific Economic Cooperation (APEC) and will not identify individuals. It will form the basis for a blueprint or framework for future

Survey - Page 1 (continued)

standards development across the Asia Pacific Region related to the protection of critical infrastructure and support systems. Refer to the project plan and background paper for further information.

When questions are marked by an asterisk * this means that a response is required or mandatory. There will be an error message if the question is not answered or the information is not entered in accordance with the instructions. It will not be possible to move forward in the survey until the question is answered or the error corrected.

The answer choices for multiple choice questions include an ‘Unsure’ option. Choose the ‘Unsure’ button if you are not sure of the answer or if you consider that this question is not applicable to your sector.

The answer choices for multiple choice questions also include a ‘Neutral’ option. This is the mid-range or average option. Choose the ‘Neutral’ button if you consider the level of importance for the item is average on the scale or if you are neutral on the rating for the issue. If the scale was numerical (1, 2, 3, 4, 5) ‘Neutral’ would be 3. For example the score on an importance scale is neither towards important nor towards unimportant.

As the survey aims to collect reliable information please do not choose the ‘Neutral’ and ‘Unsure’ buttons unless absolutely necessary. Many of the questions are about ratings and we are interested in finding out how you rate the various issues and standards.

We also ask that you consider your ratings carefully as this will affect the quality of the data collected. For instance, if you rate every item as “Important’ for a particular question (or throughout the survey) it will be difficult to assess the priority of particular issues in the data analysis.

There are optional comment boxes throughout the survey for the entry of additional information. Comments should be entered in English. It will not be possible to translate entries in other languages.

Survey - Page 2

2. Contact details and background information

1. Mandatory information has been kept to a minimum in this question. Only the name of the person completing the survey and their email address is required information. This information is required in case the project team needs to check the accuracy or meaning of responses entered. This is important because many survey respondents will be from a non English speaking background. The survey results will not identify survey respondents or their organisations. This information will be kept confidential. Security is further ensured by the SSL encryption that has been applied to the survey.

2. Country

This question is mandatory / an answer is required.

This information is required because the survey results will be reported by country.

3. Gender

This question is mandatory / an answer is required.

This information is required for all projects that are funded by APEC. The survey results will be reported by gender.

4. Respondent sector(s)

This question is mandatory / an answer is required.

This information is required because the survey results will be reported by respondent sector (s). The sectors listed here match the Integrated Security Framework that was developed following the Australian survey that was the basis for this project. An ‘other (please specify)’ option is provided if you cannot identify your sector from the choices listed.

5. Respondent role within organisation

This question is mandatory / an answer is required.

This information is required because the survey results will be reported by respondent role. The roles listed here match the Integrated Security Framework that was developed following the Australian survey that was the basis for this project. An ‘other (please specify)’ option is provided if you cannot identify your role from the choices listed.

Survey - Page 2 (continued)

6. **Briefly describe the role of your organisation in your sector (500 character limit)**

This question is non mandatory / an answer is optional.

This question requires contextual information about where your organisation fits within the sector identified in 5. Above. For example, is the organisation a standards development organisation, private security firm, government defence authority etc?

Survey - Page 3

3. Security objectives, issues and solutions

1. **Security issues and solutions**

   This question is non mandatory / an answer is optional.

   This question collects information about security issues and solutions relating to critical infrastructure and support systems.

   Select the major security issue in your sector by choosing from the list provided (one choice only).

   Enter solution (s) for the major issue in the Solutions box below.

   If the major sector issue for your sector is not listed, enter it with the solution (s) in the Additional comments box in Q 7 at the bottom of the page. Identify both the issue and solution (s) clearly.

   For example:

   Issue -
   Solution (s) -

2. **Would the solutions to addressing these issues involve adopting standards?**

   This question is mandatory / an answer is required.

   This question collects information about whether solutions to the security issues would involve adopting standards.

   Enter Yes or No.

   Note: The term 'standards' in this question refers to formal standards:

   > Standards are defined by the International Organization of Standardization (ISO) as "documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purpose."

   The focus of this survey is standards based and therefore questions using this term should be read in this context. A simpler open source definition of the term 'standard' is included in the Glossary for easy reference.

Survey – Page 3 (continued)

3. **How well do you understand the systems that are in place to protect your organisation when there is a significant disruption to normal services?**

   This question is mandatory / an answer is required.

   This question collects information about respondents' understanding of the systems in place to ensure business continuity in times of crisis.

   Assign your level of understanding by checking exactly one button for your choice.

   As stated earlier, please do not choose the "Neutral' or 'Unsure' buttons unless absolutely necessary. "Unsure' also means not applicable to your sector.

   If you do not choose one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

4. **How well do you understand the impact on your organisation's customers and suppliers if there is a significant disruption to normal services?**

   This question is mandatory / an answer is required.

   This question collects information about respondents' understanding of how their organisation's customers and suppliers would be affected if there was a significant disruption to normal business services.

   Assign your level of understanding by checking exactly one button for your choice.

   As stated earlier, please do not choose the "Neutral' or 'Unsure' buttons unless absolutely necessary. "Unsure' also means not applicable to your sector.

   If you do not choose one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

Survey – Page 3 (continued)

5. **Would your organisation help to fund the development of standards that are considered critical to the security of your sector?**

   This question is mandatory / an answer is required.

   This question collects information about whether organisations would be prepared to contribute funding to the development of standards that are considered critical to the security of their sector.

   Survey respondents are only being asked to give an opinion here, based on their knowledge of their organisation. The information collected will be used to gain an overall impression of the level of commitment to funding standards development. It is not binding in any way and the results will not be reported by organisation.
   Answer this question by checking exactly one button for your choice.

   As stated earlier, please do not choose the “Neutral’ or ‘Unsure’ buttons unless absolutely necessary. “Unsure’ also means not applicable to your sector.

   If you do not choose one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

6. **Would your organisation participate in the development of standards that are considered critical to the security of your sector?**

   This question is mandatory / an answer is required.

   This question collects information about whether organisations would be prepared to contribute intellectually to the development of standards that are considered critical to the security of their sector.

   As in 5. above, survey respondents are only being asked to give an opinion here, based on their knowledge of their organisation. The information collected will be used to gain an overall impression of the level of commitment to participation in standards development. It is not binding in any way and the results will not be reported by organisation.

   Answer this question by checking exactly one button for your choice.
   As stated earlier, please do not choose the “Neutral’ or ‘Unsure’ buttons unless absolutely necessary. “Unsure’ also means not applicable to your sector.

   If you do not choose one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

Survey – Page 3 (continued)

7. **Additional Comments**
   (500 character limit)

   This question is non mandatory / an answer is optional.

   The comments box has been provided to allow survey respondents to make additional comments about security objectives, issues and solutions (including existing standards and development of new standards).

Survey - Page 4

4. Common approaches supporting security processes

1. **How important do you believe common and agreed approaches, standards, methods, protocols and procedures are to improved security?**

   This question is mandatory / an answer is required.

   Assign the level of importance (including level of urgency) you attach to these by checking exactly one button for your choice.

   As stated earlier, please do not choose the "Neutral' or 'Unsure' buttons unless absolutely necessary. "Unsure' also means not applicable to your sector.

   If you do not choose one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

2. **Within your organisation or sector what are the major sources of guidance when developing security products, installations, processes or systems?**

   This question is mandatory / an answer is required.

   This question collects information about the major sources of guidance by organisation or sector.

   Check at least one button. More than one button can be checked on this question. An "Other (please specify)' button is provided if you consider that there should be other options included in the choices.

   If you do not choose at least one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

3. **In your experience what has been the outcome of using these major sources of guidance?**

   This question is mandatory / an answer is required.

   This question collects information about outcomes of using major sources of guidance.

   Check exactly one button.

   As stated earlier, please do not choose the "Neutral' or 'Unsure' buttons unless absolutely necessary. "Unsure' also means not applicable to your sector.

   If you do not choose one option there will be an error message. You will not be able to move forward in the survey until you check one option to correct the error.

Survey – Page 4 (continued)

4. Additional Comments
(500 character limit)

This question is non mandatory / an answer is optional.

The comments box has been provided to allow survey respondents to make additional comments about common approaches supporting security processes.

Survey - Page 5

5. Assessing Priorities for broad categories of security standards and other sources of guidance

1. **Please rate the level of importance for the following broad categories of security standards and other sources of guidance.**
   Consider the level of urgency when rating the importance level for each category.

   This question is mandatory / an answer is required.

   Note that this section focuses on the importance of broad categories of security standards and other sources of guidance. Information about the importance of specific security standards and other sources of guidance under these broad categories will be collected in the following pages of the survey.

   Note:
   The term ‘other sources of guidance’ refers to documentation, guidelines, legislation etc that are used for reference.

   Assign the level of importance (including level of urgency) you attach to these by checking exactly one button on each line for your choice.

   As stated earlier, please do not choose the “Neutral’ or ‘Unsure’ buttons unless absolutely necessary. “Unsure’ also means not applicable to your sector.

   If you do not check one button on every line there will be an error message. You will not be able to move forward in the survey until you check one button on every line to correct the error.

2. **Are there any other broad categories of security standards and other sources of guidance that you believe should have been included in this category?**
   If so, please identify these below and rate the level of importance.
   (500 character limit)

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make additional comments about broad categories of security standards and other sources of guidance that they believe should have been included in this category.

Survey - Page 6

6. Governance, Strategy & Policy - Assessing priorities for specific security standards and other sources of guidance

1. **Assessing priorities for specific security standards and other sources of guidance**

   This question is mandatory / an answer is required.

   Note that this section focuses on the importance of specific security standards and other sources of guidance.

   Assign the level of importance (including level of urgency) you attach to these by checking exactly one button on each line for your choice.

   As stated earlier, please do not choose the "Neutral' or 'Unsure' buttons unless absolutely necessary. "Unsure' also means not applicable to your sector.

   If you do not check one button on every line there will be an error message. You will not be able to move forward in the survey until you check one button on every line to correct the error.

2. **Are there any other specific security standards and other sources of guidance that you believe should have been included in this category?**
   If so, please identify these below and rate the level of importance.
   (500 character limit)

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make additional comments about specific security standards and other sources of guidance that they believe should have been included in the Governance, Strategy & Policy category.

Survey - Page 7

7. Risk Management - Assessing priorities for specific security standards and other sources of guidance

1. **Assessing priorities for specific security standards and other sources of guidance**

   This question is mandatory / an answer is required.

   Note that this section focuses on the importance of specific security standards and other sources of guidance.

   Assign the level of importance (including level of urgency) you attach to these by checking exactly one button on each line for your choice.

   As stated earlier, please do not choose the “Neutral’ or ‘Unsure’ buttons unless absolutely necessary. “Unsure’ also means not applicable to your sector.

   If you do not check one button on every line there will be an error message. You will not be able to move forward in the survey until you check one button on every line to correct the error.

2. **Are there any other specific security standards and other sources of guidance that you believe should have been included in this category?**
   If so, please identify these below and rate the level of importance.
   (500 character limit)

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make additional comments about specific security standards and other sources of guidance that they believe should have been included in the Risk Management category.

Survey - Page 8

8. Information Security - Assessing priorities for specific security standards and other sources of guidance

1. **Assessing priorities for specific security standards and other sources of guidance**

   This question is mandatory / an answer is required.

   Note that this section focuses on the importance of <u>specific</u> security standards and other sources of guidance.

   Assign the level of importance (including level of urgency) you attach to these by checking <u>exactly</u> one button on <u>each line</u> for your choice.

   As stated earlier, please do not choose the "Neutral' or 'Unsure' buttons unless absolutely necessary. "Unsure' also means not applicable to your sector.

   If you do not check <u>one</u> button on <u>every line</u> there will be an error message. You will not be able to move forward in the survey until you check one button on every line to correct the error.

2. **Are there any other specific security standards and other sources of guidance that you believe should have been included in this category?**
   If so, please identify these below and rate the level of importance.
   (500 character limit)

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make additional comments about specific security standards and other sources of guidance that they believe should have been included in the Information Security category.

Survey - Page 9

9. Personnel Security - Assessing priorities for specific security standards and other sources of guidance

1. **Assessing priorities for specific security standards**

   This question is mandatory / an answer is required.

   Note that this section focuses on the importance of specific security standards and other sources of guidance.

   Assign the level of importance (including level of urgency) you attach to these by checking exactly one button on each line for your choice.

   As stated earlier, please do not choose the “Neutral’ or ‘Unsure’ buttons unless absolutely necessary. “Unsure’ also means not applicable to your sector.

   If you do not check one button on every line there will be an error message. You will not be able to move forward in the survey until you check one button on every line to correct the error.

2. **Are there any other specific security standards and other sources of guidance that you believe should have been included in this category?**
   If so, please identify these below and rate the level of importance.
   (500 character limit)

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make additional comments about specific security standards and other sources of guidance that they believe should have been included in the Personnel Security category.

Survey - Page 10

10. Physical Security - Assessing priorities for specific security standards and other sources of guidance

1. **Assessing priorities for specific security standards and other sources of guidance**

   This question is mandatory / an answer is required.

   Note that this section focuses on the importance of specific security standards and other sources of guidance.

   Assign the level of importance (including level of urgency) you attach to these by checking exactly one button on each line for your choice.

   As stated earlier, please do not choose the "Neutral' or 'Unsure' buttons unless absolutely necessary. "Unsure' also means not applicable to your sector.

   If you do not check one button on every line there will be an error message. You will not be able to move forward in the survey until you check one button on every line to correct the error.

2. **Are there any other specific security standards and other sources of guidance that you believe should have been included in this category?**
   If so, please identify these below and rate the level of importance.
   (500 character limit)

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make additional comments about specific security standards and other sources of guidance that they believe should have been included in the Physical Security category.

Survey - Page 11

11. Methods for improving the implementation of security standards

1. **What could be done to make the implementation of security standards more successful?**
   Check <u>exactly</u> 3 boxes to indicate your top 3 choices from the list below

   This question is mandatory / an answer is required.

   This question collects information about what survey respondents consider to be their top 3 choices of methods for improving the implementation of security standards. This information will be reported but not ranked.

   This question requires <u>exactly</u> 3 boxes to be checked from the list provided.
   An “Other (please specify)’ button is provided if you consider that there should be other options included in the choices.

   If you do not check <u>exactly</u> 3 boxes there will be an error message. You will not be able to move forward in the survey until you check exactly 3 boxes.

2. Final comments

   This question is non mandatory / an answer is optional.

   The box has been provided to allow survey respondents to make any final comments they wish to make about the survey.

The survey has by now been completed. Respondents may go back to previous pages and edit their responses if they wish to do so.

To submit the survey, click on the ‘Done’ button at the bottom of the screen.

<u>Note</u>
It will not be possible to go back and edit the survey responses after it has been submitted.

Asia-Pacific
Economic Cooperation

Glossary

Critical Infrastructure and Support Systems Standardization Project

2008
Authored by: Mark Bezzina
StanCert Pty Ltd

Table of Contents

Introduction

This Glossary of key terms used in the Critical Infrastructure and Support Systems Standardization Project survey is not intended to be exhaustive.

Only the terms that are most likely to cause difficulty are included in this document.

If a definition is required for a term that is not included in the Glossary, reference to a dictionary such as Encarta (included in Microsoft applications) is suggested. Alternatively, online encyclopaedias such as Wikipedia are available or definitions can be found through search engines such as Google and Yahoo.

A	
Access control	Access control is the ability to permit or deny the use of a particular resource by a particular entity. Access control mechanisms can be used in managing physical resources (such as a movie theater, to which only ticketholders should be admitted), logical resources (a bank account, with a limited number of people authorized to make a withdrawal), or digital resources (for example, a private text document on a computer, which only certain users should be able to read). *Source: Wikipedia (online encyclopedia)*
Asset	A property to which a value can be assigned. *Source: Encarta Dictionary*
B	
Barrier	Something that hinders progress. *Source: Encarta Dictionary*
Biological agent	A biological agent is an infectious disease or toxin that can be used in bioterrorism or biological warfare. *Source: Wikipedia (online encyclopedia) Source: Wikipedia (online encyclopedia)*
Biometrics	The study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. *Source: Wikipedia (online encyclopedia)*
Business continuity	Business Continuity is the activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions. These activities include many daily chores such as project management, system backups, change control, and help desk. Business Continuity is not something implemented at the time of a disaster; Business Continuity refers to those activities performed daily to maintain service, consistency, and recoverability. The foundation of Business Continuity is the policies, guidelines, standards, and procedures implemented by an organization. *Source: Wikipedia (online encyclopedia)*

C	
Capability certified	Certification to confirm the ability to perform actions. Professional certification is where a person is certified as being able to competently complete a job or task, usually by the passing of an examination. *Source: Wikipedia (online encyclopedia)*
Car park	Parking lot (called a car park in Australia and the UK) is a cleared area that is intended for parking vehicles. Usually, the term refers to a dedicated area that has been provided with a durable or semi-durable surface. *Source: Wikipedia (online encyclopedia) (modified)*
Chemical agent	A substance used in or produced by the processes of chemistry. A chemical has a defined atomic or molecular structure that results from, or takes part in, reactions involving changes in its structure, composition, and properties. *Source: Encarta Dictionary*
Closed circuit TV	Closed Circuit Television, often abbreviated and referred to as CCTV, is "a television transmission circuit with a limited number of reception stations and no broadcast facilities”. (yourdictionary.com, 2004). It is used for video surveillance in public and private spaces. Cameras are linked to a central control room where the images can be remotely monitored by a single person (Norris and Armstrong, 1999, p. 18). Permanent records of the images can be kept for later use. *Source: M/Cyclopedia of New Media*
Command and control	The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. *Source: The Free Dictionary by Farlex*
Compliance management	Compliance with external laws and guidelines for corporate structures and processes. This includes legal compliance and reporting to relevant authorities. *Source: Google web definition (modified)*

Continuous improvement	Continually improving all functions, standardized activities and processes of a business, from manufacturing to management and from the CEO to the assembly line workers. *Source: Wikipedia (online encyclopedia) (modified)*
Crime prevention through environmental design	Crime prevention through environmental design (CPTED) is a multi-disciplinary approach to deterring criminal behavior through environmental design. CPTED strategies rely upon the ability to influence offender decisions that precede criminal acts. *Source: Wikipedia (online encyclopedia)*
Crisis management	The practice of crisis management involves attempts to eliminate technological failure as well as the development of formal communication systems to avoid or to manage crisis situations (Barton, 2001), and is a discipline within the broader context of management. Crisis management consists of skills and techniques required to assess, understand, and cope with any serious situation, especially from the moment it first occurs to the point that recovery procedures start. *Source: The Free Dictionary by Farlex*
Critical infrastructure and support systems	Critical infrastructure comprises those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the [country] or affect [its] ability to conduct national defence and ensure national security. Based on Australian Government definition (modified) Support systems refer to systems for maintaining and protecting critical infrastructure. *Source: Encarta Dictionary (modified)*
Cryptography	The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use. *Source: [ISO 7498-2: 1989] [ISO 8732: 1988]*

D	
Data sharing	The ability to share the same data resource with multiple applications or users. Data sharing is a primary feature of a database management system (DBMS). *Source: The Free Dictionary by Farlex*
Detection system	System to find what is otherwise apt to elude notice. *Source: based on Oxford English Dictionary definition of 'detection' (modified)*
Digital certificate	An encrypted and digitally signed attachment that authenticates a user on the Internet or an intranet. *Source: YourDictionary.com*
E	
Email attacks	Refers to scams (schemes for making money by dishonest means), theft of online banking details and other practices designed to harm individuals through accessing their emails. *Source: based on Encarta Dictionary definitions*.
Emergency management	Emergency Management is a range of measures to manage risks to communities and the environment. *Source: Emergency Management Australia, Australian Emergency Manuals Series, Part 1, The Fundamentals, Manual 3, Australian Emergency Management Glossary, 1998, page 39.*
Entry search	A search of an individual or vehicle on entry to a building or facility. *Source: based on definitions in Encarta Dictionary*
Executive buy-in / commitment	Support, agreement, approval, commitment, engagement - at the executive level of an organization. *Sources: Based on Wiktionary (online dictionary)and Encarta Dictionary definitions*

F	
Financial recovery	Restoration to a former or better financial condition. *Source: Based on The Free Dictionary by Farlex*
First responder	The first person, e.g. an emergency medical technician or a police officer, who arrives at the scene of a disaster, accident, or life-threatening medical situation. *Source: Encarta Dictionary*
Forensics and evidence collection	Computer forensics is the application of scientifically proven methods to gather, process, interpret, and to use digital evidence to provide a conclusive description of cyber crime activities. *Source: Webopedia*
G	
Governance	The term 'governance' means the processes, customs, policies, laws and institutions affecting the way people direct, administer or control an organisation or corporation. It is about consistent management and effective decision making, as well as cohesive policies and processes. *Source: Wikipedia (online encyclopedia)*
H	
Hazard	Potential danger; something that is potentially very dangerous. *Source: Encarta Dictionary*
I	
Identity management	Identity management (ID management) is a broad administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity. *Source: Whatis.com*

Incident	Event with potentially serious consequences; event that may result in a crisis. *Source: Encarta Dictionary*
Induction	The act or process of inducting somebody into a position or an organization. To introduce somebody to new beliefs, knowledge, or ideas. *Source: Encarta Dictionary*
Information asset classification	Classification of a collection of data that has recognised value to an agency in performing its business function/s and meeting agency requirements. *Source: Based on definition by Queensland Government (modified)*
Information security	Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. It also includes the storage and categorisation of sensitive information. *Source: Wikipedia (online encyclopedia) (modified)*
Intelligence	The gathering of information, which may be secret e.g. about foreign governments, the armed forces, business competitors, or criminals. *Source: Wikipedia (online encyclopedia) (modified)*
M	
Maritime	Related to the sea or oceans. *Source: Wikipedia (online encyclopedia)*
Mentoring	A developmental relationship between a more experienced mentor and a less experienced person. The less experienced person is guided and protected by a more prominent person. *Source: Wikipedia (online encyclopedia) (modified)*

N	
Natural disasters	The impact of a natural hazard that negatively affects society or environment e.g. Tsunami, earthquake. *Source: Based on Wikipedia (online encyclopedia) definition*
O	
Off-shoring	The relocation of business processes from one country to another. *Source: Wikipedia (online encyclopedia)*
Outsourcing (purchasing)	Subcontracting a process, such as product design or manufacturing, to a third-party company. *Source: Wikipedia (online encyclopedia)*
P	
Pandemic	An epidemic of infectious disease that spreads through human populations across a large region; for instance a continent, or even worldwide. *Source: Wikipedia (online encyclopedia)*
Places of mass gathering	Places where a large number of people gather together e.g. public spaces and events. *No reference source*
R	
Radio frequency ID	Radio-frequency identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. *Source: Wikipedia (online encyclopedia)*
Radiological agent	Radioactive substance. *Source: Based on The Free Dictionary by Farlex*

Resilience	The ability to avoid, minimize, withstand, and recover from the effects of adversity, whether natural or manmade, under all circumstances of use. In business terms, resilience is the ability of an organization, resource, or structure to sustain the impact of a business interruption and recover and resume its operations to continue to provide minimum services. *Source: Wikipedia (online encyclopedia)*
Risk Management	Risk management is a structured approach to managing uncertainty related to a threat, a sequence of human activities including: risk assessment, strategies development to manage it, and mitigation of risk using managerial resources. *Source: Wikipedia (online encyclopedia)*
S	
Solution	An act, plan or other means, used or proposed, to solve a problem. *Source: Wikipedia (online encyclopedia)*
Spam	An unsolicited electronic message sent in bulk, usually by email or newsgroups. *Source Wiktionary (Online Dictionary)*
Spyware	Programs that surreptitiously monitor and report the actions of a computer user. *Source Wiktionary (Online Dictionary)*
Standard	A technical standard is an established norm or requirement. It is usually a formal document that establishes uniform engineering or technical criteria, methods, processes and practices. *Source: Wikipedia (online encyclopedia)*
Supply chain	A supply chain or logistics network is the system of organizations, people, technology, activities, information and resources involved in moving a product or service from supplier to customer. *Source: Wikipedia (online encyclopedia)*

Systems audit	An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. *Source: Wikipedia (online encyclopedia)*
Systems security - Supervisory Control And Data Acquisition (SCADA)	SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation. *Source: Webopedia Computer Dictionary*
T	
Thermal imaging	Infrared-based system used for screening large groups of people for elevated body temperature. *Based on Encarta Dictionary definition (modified)*

Critical Infrastructure and Support Systems Standardisation Survey

1. Introduction

Welcome to the The Critical Infrastructure and Support Systems Standardisation Project Survey. Your participation in this survey is greatly appreciated by all concerned with this important initiative.

This survey will assist in the development of a proposed framework of standards to address the need to protect critical infrastructure and support systems across the Asia-Pacific Region during times of emergencies.

The survey will also identify and prioritise the standards required by the owners and operators of critical infrastructure and any gaps that may exist. An all hazards approach is being taken to threats. This approach includes security threats that are intentional or man-made (such as criminal acts or terrorism), as well as accidents, natural disasters and pandemics.

SSL encryption has been applied to this survey to protect the security of information.

There are optional comment boxes throughout the survey for the entry of additional information. Comments should be entered in English. It will not be possible to translate entries in other languages.

Note:
This is a multi-page survey that must be completed in one session. If the survey form is closed prior to completion it will not be possible to return at a later time and enter more information. Navigation to subsequent and previous pages in the survey is via the buttons at the bottom of each page. Estimated time for completion is 15 minutes.

We suggest that before commencing this survey you download the and print the instructions, background papers and support materials via the links provided below. You will need a PDF reader such as Adobe Reader to view and print these documents.

Survey Glossary
Survey Instructions
Project Plan
Background Paper

Critical Infrastructure and Support Systems Standardisation Survey

2. Contact details and background information

Note:
Only your last name, first name and email address are required information in Q1.below.
The other fields in this question are optional.

* 1. Please provide the following information.

Last Name:

First Name(s):

Company/Organisation:

Email Address:

Phone Number:

* 2. Country

* 3. Gender

○ Male ○ Female

* 4. Respondent sector(s)

○ Energy (e.g. gas, electricity, petroleum fuels)

○ Utilities (e.g. water, water waste management)

○ Communications (e.g. telecommunications, IT, postal services)

○ Transport

○ Health

○ Food Supply

○ Finance

○ Government Services

○ National Icons (e.g. buildings, cultural, sport and tourism)

○ Essential Manufacturing

○ Other (please specify) 50 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

* 5. Respondent role within organisation

○ CEO

○ Executive

○ Manager

○ Policy Advisor

○ Standards Developer

○ Technical Specialist

○ Vendor or Consultant

○ Other (please specify) (50 character limit)

6. Briefly describe the role of your organisation in your sector (500 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

3. Security objectives, barriers and solutions

In the following question please choose the major security issue in your sector from the list below (one choice only).
Then suggest solution(s) for the issue in the box.
If your issue is not listed, enter it with a solution under Q 7. Additional Comments at the bottom of this page.

1. Security Issues and solutions

○ Funding

○ Resources

○ Time

○ Personnel (workforce)

○ Information / data

○ Communication

○ Consultation

○ Training

○ Planning

○ Executive buy-in / commitment

○ Industry specific standards

Solutions (250 character limit)

* 2. Would the solutions to addressing these issues involve adopting standards?

○ Yes ○ No

* 3. How well do you understand the systems that are in place to protect your organisation when there is a significant disruption to normal services?

○ Very well ○ Well ○ Neutral ○ Not well ○ Unsure

* 4. How well do you understand the impact on your organisation's customers and suppliers if there is a significant disruption to normal services?

○ Very well ○ Well ○ Neutral ○ Not well ○ Unsure

* 5. Would your organisation help to fund the development of standards that are considered critical to the security of your sector?

○ Yes ○ Possibly ○ Not Sure ○ Unlikely ○ No

* 6. Would your organisation participate in the development of standards that are considered critical to the security of your sector?

○ Yes ○ Possibly ○ Not Sure ○ Unlikely ○ No

Critical Infrastructure and Support Systems Standardisation Survey

7. Additional Comments
(500 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

4. Common approaches supporting security processes

*** 1. How important do you believe common and agreed approaches, standards, methods, protocols and procedures are to improved security?**

○ Very Important ○ Important ○ Neutral ○ Unimportant ○ Very Unimportant ○ Unsure

*** 2. Within your organisation or sector what are the major sources of guidance when developing security products, installations, processes or systems?**

□ International standards

□ National standards

□ Legislation

□ Government guidelines

□ Regional guidelines

□ Internally developed operating procedures

□ Industry contacts (e.g. systems obtained from industry partners)

□ Other (please specify) (150 character limit)

*** 3. In your experience what has been the outcome of using these major sources of guidance?**

○ Substantial improvements

○ Some improvements

○ Neutral

○ Minimal improvements

○ No improvements

○ Unsure

4. Additional Comments (500 character limit)

5. Assessing priorities for broad categories of security standards and other s...

*** 1. Please rate the level of importance for the following broad categories of security standards and other sources of guidance.**
Consider the level of urgency when rating the importance level.

	Very Important	Important	Neutral	Unimportant	Very Unimportant	Unsure
Governance, strategy and policy	○	○	○	○	○	○
Risk Management	○	○	○	○	○	○
Information Security	○	○	○	○	○	○
Personnel Security	○	○	○	○	○	○
Physical Security	○	○	○	○	○	○

2. Are there any other broad categories of security standards and other sources of guidance that you believe should have been included in this section? If so, please identify these below and rate the level of importance.
(500 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

6. Governance, Strategy & Policy

Assessing priorities for specific security standards and other sources of guidance

*** 1. Please indicate the level of importance you attach to specific security standards and other sources of guidance in this category.**
Consider the level of urgency when you are choosing the level of importance.

	Very Important	Important	Neutral	Unimportant	Very Unimportant	Unsure
Corporate governance	○	○	○	○	○	○
Compliance management (including legal compliance and reporting to relevant authorities)	○	○	○	○	○	○
Reporting incidents and issues management	○	○	○	○	○	○
Systems review, audit and assessment	○	○	○	○	○	○
Security management	○	○	○	○	○	○
Communications, public affairs and media management	○	○	○	○	○	○
Security policy (including security requirements in contracts)	○	○	○	○	○	○
Systems for the categorisation of organisational assets	○	○	○	○	○	○
Crisis management	○	○	○	○	○	○
Understanding networks and inter-dependencies	○	○	○	○	○	○
Continuous improvement mechanisms	○	○	○	○	○	○
Outsourcing (purchasing) or off-shoring security systems and operations	○	○	○	○	○	○
Effective leadership	○	○	○	○	○	○
Executive buy-in / commitment	○	○	○	○	○	○
Building effective partnerships	○	○	○	○	○	○
Building a resilient culture	○	○	○	○	○	○

2. Are there any other specific security standards and other sources of guidance that you believe should have been included in this category? If so, please identify these below and rate the level of importance.
(500 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

7. Risk Management

Assessing priorities for specific security standards and other sources of guidance

Note:
The term 'emergency' includes natural disasters (such as hurricanes, floods, Tsunamis, earthquakes, pandemics) and man-made or intentional acts (such as terrorism and crime).

*** 1. Please indicate the level of importance you attach to specific security standards and other sources of guidance in this category.**
Consider the level of urgency when you are choosing the level of importance.

	Very Important	Important	Neutral	Unimportant	Very Unimportant	Unsure
Risk Management	○	○	○	○	○	○
Emergency management	○	○	○	○	○	○
Business continuity management	○	○	○	○	○	○
Business Resilience	○	○	○	○	○	○
Financial recovery provisions	○	○	○	○	○	○
Intelligence and information services	○	○	○	○	○	○
Command, control and communications	○	○	○	○	○	○
First responders	○	○	○	○	○	○
Supply chain and transport	○	○	○	○	○	○
Evacuation plans	○	○	○	○	○	○
Chemical agent detection systems	○	○	○	○	○	○
Radiological agent detection systems	○	○	○	○	○	○
Biological agent detection systems	○	○	○	○	○	○

2. Are there any other specific security standards and other sources of guidance that you believe should have been included in this category? If so, please identify these below and rate the level of importance.
(500 character limit)

8. Information Security

Assessing priorities for specific security standards and other sources of guidance

*** 1. Please indicate the level of importance you attach to specific security standards and other sources of guidance in this category.**
Consider the level of urgency when you are choosing the level of importance.

	Very Important	Important	Neutral	Unimportant	Very Unimportant	Unsure
General IT security management	○	○	○	○	○	○
General IT security management reporting	○	○	○	○	○	○
Communications security	○	○	○	○	○	○
Systems access control	○	○	○	○	○	○
Systems security - Supervisory Control and Data Acquisition (SCADA)	○	○	○	○	○	○
Network security	○	○	○	○	○	○
Hardware security (including certification)	○	○	○	○	○	○
Software security (including certification)	○	○	○	○	○	○
Information security (storage and categorisation of sensitive information)	○	○	○	○	○	○
Information asset classification and control	○	○	○	○	○	○
Data sharing security	○	○	○	○	○	○
Industrial automation security	○	○	○	○	○	○
Interoperability of security data	○	○	○	○	○	○
Cryptography	○	○	○	○	○	○
Digital certificates	○	○	○	○	○	○
Forensics and evidence collection	○	○	○	○	○	○
Penetration testing	○	○	○	○	○	○
Control of viruses and Trojans	○	○	○	○	○	○
Control of spam and spyware	○	○	○	○	○	○
Email attacks (e.g. scams and theft of online banking details)	○	○	○	○	○	○
Scenario simulation applications	○	○	○	○	○	○

2. Are there any other specific security standards and other sources of guidance that you believe should have been included in this category? If so, please identify these below and rate the level of importance.
(500 character limit)

9. Personnel Security

Assessing priorities for specific security standards and other sources of guidance

*** 1. Please indicate the level of importance you attach to specific security standards and other sources of guidance in this category.**
Consider the level of urgency when you are choosing the level of importance.

	Very Important	Important	Neutral	Unimportant	Very Unimportant	Unsure
Pre employment screening	○	○	○	○	○	○
Employee termination procedure	○	○	○	○	○	○
Security training systems for staff	○	○	○	○	○	○
Dealing with psychological trauma	○	○	○	○	○	○
Identity management	○	○	○	○	○	○
Biometrics	○	○	○	○	○	○
Radio frequency ID	○	○	○	○	○	○
Building and facility access control	○	○	○	○	○	○
Entry searches	○	○	○	○	○	○
Video and closed circuit TV	○	○	○	○	○	○
Guards and patrols	○	○	○	○	○	○
Personnel protective equipment (eg bullet proof vests, respirators etc)	○	○	○	○	○	○
Crowd controllers	○	○	○	○	○	○
Public health security	○	○	○	○	○	○
Thermal imaging (for human temperature screening)	○	○	○	○	○	○

2. Are there any other specific security standards and other sources of guidance that you believe should have been included in this category? If so, please identify these below and rate the level of importance.
(500 character limit)

10. Physical Security

Assessing priorities for specific security standards and other sources of guidance

*** 1. Please indicate the level of importance you attach to specific security standards and other sources of guidance in this category.**
Consider the level of urgency when you are choosing the level of importance.

	Very Important	Important	Neutral	Unimportant	Very Unimportant	Unsure
Perimeter security (e.g. lighting, fencing, bollards, chains, doors, windows, gates)	○	○	○	○	○	○
Construction security (e.g. construction materials, building structure, fire protection)	○	○	○	○	○	○
Crime prevention through environmental design	○	○	○	○	○	○
Security of facility utilities (water, gas, electricity, telecommunications and waste)	○	○	○	○	○	○
Signs, notices and instructions	○	○	○	○	○	○
Alarms, intruder alarms and detection devices	○	○	○	○	○	○
Locksets and security of keys	○	○	○	○	○	○
Safes and strong rooms	○	○	○	○	○	○
Bullet resistant panels	○	○	○	○	○	○
Control room security	○	○	○	○	○	○
Car parks and vehicle security (including vehicle control points)	○	○	○	○	○	○
Transport security	○	○	○	○	○	○
Postal and mail room safety	○	○	○	○	○	○
Food Safety	○	○	○	○	○	○
Packaging and seals	○	○	○	○	○	○
Hotel security	○	○	○	○	○	○
Places of mass gathering (security of public spaces and events)	○	○	○	○	○	○
Projectile barriers and blast resistance	○	○	○	○	○	○
Protecting maritime and off shore assets (including boats and ships)	○	○	○	○	○	○

2. Are there any other specific security standards and other sources of guidance that you believe should have been included in this category? If so, please identify these below and rate the level of importance.
(500 character limit)

Critical Infrastructure and Support Systems Standardisation Survey

11. Methods for improving the implementation of security standards

*** 1. What could be done to make the implementation of security standards more successful?**
Check <u>exactly</u> 3 boxes to indicate your top 3 choices from the list below

□ Training (e.g. induction, workshops, exercises, professional development and mentoring)

□ Computer based training

□ Technical assistance from consultants

□ Consultants and practitioners capability certified

□ User forums and support groups

□ Products and services certified as security compliant

□ Implementation handbooks and guidance material

□ Reference sites and case studies

□ Other (please specify) (50 character limit)

2. Final comments

Enter any final comments you wish to make here.
(1000 character limit)

Standards Australia

Standards Australia is an independent, non-government organisation that is recognised as the peak non-government standards developing body in Australia through a Memorandum of Understanding with the Commonwealth Government.

Standards Australia aims to excel in meeting national needs for contemporary, internationally aligned standards and related services, which enhance the nation's economic efficiency and international competitiveness and fulfil the community's demand for a safe and sustainable environment. Standards Australia represents Australia's interest in the two peak international standards organisations, The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), representing Australian industry's perspective in an international arena.

Standards Australia has a rich history of providing documents to the market based on an inclusive, transparent and consensus based methodology. Standards are written by experts participating in committees; and reflect the needs of industry, producing relevant, workable documents. Standards Australia works and consults with a wide spectrum of interest from the community to publish consensus-based standards that are practical and contemporary in nature. The committee structure has provided Standards Australia with an abundance of knowledge and ties to professional organisations that has spanned decades. Standards Australia has an ongoing and involved relationship with a variety of government agencies through committee involvement.

Standards Australia is at the forefront of security standards, having already established many committees addressing security concerns ranging from logical and physical security to food safety, risk management and business continuity management. Pre-eminent among these committees is the National Centre for Security Standards (NCSS). The NCSS was established in December 2003 to support the Commonwealth government and industry in addressing issues related to the security of critical infrastructure. It is the mission of the NCSS to assist key government agencies and private organisations requesting assistance to accelerate development and adoption of consensus standards critical to national security.