ISO/TC 292 Security and resilience

Date: 2017-06-12

ISO/XXX

ISO/TC 292/WG 6

Secretariat: Standards Australia

Protective security – Architecture, framework and guidelines

Architecture, cadre et lignes directrices de sécurité en matière de sécurité

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Foreword

The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/TC 292, Security and resilience.

ISO XXXX consists of the following parts. [Add information as necessary.]

Introduction

All organisations implement measures, or controls, to manage the security-related risks that exist in their environment.

This international standard helps entities by providing a means of strategically aligning the highly diverse range of protective security measures within an overarching framework that will enable risk-based prioritisation, development and amendment of protective security policy, procedures and practices in a way that is strategically aligned at the enterprise level.

The term architecture is commonly defined along the following lines: the blueprint that provides a common understanding of the organisation and is used to align strategic objectives and operational demands[1]. In line with this, enterprise architecture (EA) has become a well-defined practice for conducting organisational enterprise analysis, design, planning, and implementation, using a holistic approach at all times, for the successful development and execution of strategy.

1. Scope

This international standard details the enterprise architecture, management framework and guidelines necessary to implement a fully integrated, principles-based approach to mitigating and managing protective security risk.

The standard will be helpful to any organisation in implementing and defining a structure for the range of protective security measures (security governance, information security, personnel security and physical security) in a way that is strategically aligned and cost effective.

2. Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 31000:2009, Risk management – Principles and guidelines

ISO Guide 73, Risk management — Vocabulary

ISO 28001:2007, Security management systems for the supply chain

The ISO/IEC 27000 series – the ISMS Family of Standards

AS4811:2006 – in terms of personnel security elements, particularly regarding background screening (in the absence of an International Standard).

Other protective security frameworks should also be informatively referenced, including the Australian Government Protective Security Framework and similar frameworks implemented by the governments of Canada, France, Holland, Singapore, New Zealand, Norway, UAE, United Kingdom and United States, and models utilised by such international organisations as NATO and IATA.

[1] E.S Elliott, F.Fons, A. Randell – 'Business Architecture and Agile Methodologies – A Business Architecture Guild Whitepaper'. Business Architecture Guild, February 2015.

3. Terms and definitions

For the purposes of this document, the terms and definitions given in ISO Guide 73 and the following apply.

NOTE All terms and definitions contained in ISO Guide 73 are available on the ISO Online Browsing Platform: www.iso.org/obp.

3.1

Security

…

NOTE 1 xxx

[SOURCE: ISO Guide 73: …]

3.2

Protective security

Processes and activities that protect people, information and assets from malicious acts (3.1)

3.3

Protective security framework

Like the enterprise architecture outlined in this standard, a protective security framework is designed to bring together all elements of protective security into a single policy and procedural domain to assist entities in formulating and implementing measures for the management of protective security-related risks.[2]

3.4

Architecture

The blueprint that provides a common understanding of the organisation and is used to align strategic objectives and operational demands

3.5

Governance

…

3.6

Personal security

…

3.7

Information security

…

3.8

Physical security

…

3.9

Tier (1,2, 3)

[2] Many jurisdictions have implemented such frameworks: the Australian Government Protective Security Policy Framework (which significantly informs the design of the architecture detailed in this standard), Her Majesty's Government Security Policy Framework and the New Zealand Government Protective Security Requirements. Many other jurisdictions are developing similar approaches to protective security.

...

3.10
Security culture
...

3.11
Risk
...

3.12
Security risk
...

3.13
Information lifecycle
...

3.14
Security vetting
...

3.15
Aftercare
...

3.16
DDDR
Deter, detect, delay/deny, respond/recover

3.17
Defence-in-depth
...

4. Principles

This section outlines the attributes of an enterprise protective security architecture, in particular the nature of the three tiers and the core elements of protective security.

5. Function

This section outlines how the architecture works and its key principles are operationalised, with sections on:

5.1 Leadership

5.2 Principles-based protective security risk management

5.3 Enterprise security culture

5.4 Governance

5.5 Communications

5.6 Education

5.7 Continuous improvement

5.8 Resourcing and supporting protective security

6. Architecture design

This international standard is designed to enable implementation of an architecture model that defines a 3-tier protective security architecture that links core principles with outcomes and ultimately with guidelines on implementing the means of delivering the outcomes as follows:

Tier 1

The guiding philosophy and principles that drive strategy, objectives, resourcing and review at the enterprise leadership and governance level.

Tier 2

The outcomes that will support these principles, and the management, planning and review mechanisms needed to deliver them.

Tier 3

The primary protective security controls and the arrangements necessary to implement them.

'Tier 4' consists of technical standards and entity-specific procedures that will deliver the Tier 3 controls, such as details of security design, security practice and security operations are detailed.

6.1 Tier 1 - the *principles* of protective security

The leadership and governance level defines protective security principles, strategy, objectives, resourcing and review at enterprise level. It sets the principles that define protective security and how it is delivered. These Tier 1 principles might include, but not necessarily be limited to, the following:

- The critical importance of a positive security culture in which all staff members have a sense of shared ownership of security outcomes and are both authorized and competent to act in the security interests of the enterprise; where all staff are harnessed in security outcomes.
- The importance of protective security in the enterprise-level decision making.
- The application of an enterprise protective security architecture as a key milestone in the development and maintenance of organisational resilience.
- Unambiguous inclusion of the notion that effective protective security outcomes (protecting their people, information and assets according to security risk) are integral to the ultimate success of any entity.
- The importance of continuous improvement enabling enterprises to learn from incidents and responses.

6.2 Tier 2 - The *outcomes* that will deliver against the Tier 1 *principles*

This section details the outcomes that support or deliver against the Tier 1 principles, and the basis upon which protective security measures prioritised, planned and implemented. Such an outcome might, in the Governance domain be: Security risks are managed appropriately with necessarily effective accountabilities, appropriate processes, planning and assurance, and reporting. Outcomes may be defined under the following (and possibly other) categories:

- Governance
- Information security (including transactional security)
- Personnel security
- Physical security.

6.2.1 Security governance arrangements

This section details attributes of protective security governance, including ethical principles considerations, structures, accountabilities, key enterprise responsibilities (for example maintain enterprise security risk management and planning), accountabilities and reporting structures, as well as core attributes of planning, implementation, monitoring and review.

6.2.2 Information security

This section defines the key attributes of the measures necessary to protect confidential / sensitive information, including, but not necessarily limited to evaluation, protection, accessibility and management. This includes tangible information (evaluation of sensitivity, classification, handling and storage, disposal and destruction etc.), data at rest (refer 27000 series) and data in transit (cryptographic arrangements, technical standards covering cabling etc.) and the physical transfer of tangible information assets.

This section also provides a framework in which protective security issues, threats and risks arising from the rapid uptake of technology, and its consequential governance demands, can be accommodated within the architecture. Society's now-critical reliance, across the financial, social and political domain, on the Internet, the 'Internet of things', artificial intelligence and robots, for example, presents unprecedented protective security risks that need to be incorporated within any effective enterprise architecture. Other technological changes with growing protective security implications include, but are not limited to, nanotechnology, genetic modification, robotics and cryptocurrencies, and the capacity to give effective and appropriate consideration to each in protective security decision making needs to be included in the architecture.

Further issues that will be covered include, but not necessarily be limited to guidance on:

- Defining and developing an integrated model for management of all information assets
- Handling privacy information
- Protection of intellectual property
- Transactional security
- Legal and regulatory compliance
- The Information life cycle.

6.2.3 Personnel security

This section defines the key attributes of the measures necessary to deliver assurance for enterprises that their employees and contractors are suitable to access sensitive information, that they have integrity and are honest at recruitment and throughout their employment, and that entity security is maintained post-separation.

6.2.4 Physical security

This section defines the key attributes of the measures necessary to deliver and maintenance of a safe and secure environment for sensitive information, people (staff, contractors etc.) and tangible (ISO 55000) and intangible assets.

6.3 Tier 3 – the *primary controls* necessary to deliver the Tier 2 *outcomes*

This section details the primary treatments and controls necessary to deliver the Tier 2 outcomes; primarily to guide entities in ensuring that security risk is assessed and managed according to agreed parameters, that there is appropriate appreciation of interdependencies and that the

entity has a framework in which to coordinate, plan and implement the range of protective security measures in relation to its people, information and assets.

6.3.1 Governance

This section defines the core treatments and controls in relation to the governance outcomes defined in Tier 2. Guidance on the implementation and management of protective security arrangements is also provided. Core treatments might include key attributes of, and guidance on:

- Enterprise security culture
- Enterprise security management structure and accountabilities
- Entity governance security policy, as part of overall enterprise security planning
- Effective security risk assessment, planning and management
- Application of such approaches as 'defence-in-depth' and 'deter, detect, delay/deny, respond/recover (DDDR)'
- Security management and technical competencies
- Awareness and training
- Security investigations
- Business continuity
- Governance arrangements in relation to 3rd party service providers and contractors
- Conformance with relevant regulatory arrangements
- Reporting, review and audit.

6.3.2 Information Security

This section defines the core treatments and controls in relation to the information security outcomes defined at Tier 2. Core treatments might include key attributes of, and guidance on:

- Entity information security policy, as part of overall enterprise security planning, capturing the entire information management lifecycle
- Evaluating the importance of, and classifying, information
- Access to classified information
- Information sharing processes between entities
- 3rd party access
- Implementation of effective cyber security controls and ICT systems
- Conformance with relevant regulatory arrangements, such as privacy.

6.3.3 Personnel Security

This section defines the core treatments and controls in relation to the personnel security outcomes defined at Tier 2. These may include security vetting (ensuring the right people are allowed into the enterprise), ongoing suitability (ensuring that the suitability of people to have access to sensitive information is assessed and monitored through time), and the arrangements by which people leave the organisation without compromising its security. Core treatments might include key attributes of, and guidance on:

- Entity personnel security policy, as part of overall enterprise security planning
- Defining and implementing eligibility criteria for access to classified information and assets
- Security vetting and clearance arrangements
- Monitoring of suitability of staff to access classified information and assets
- Evaluation of positions within the entity that require access to classified information
- Information security arrangements in relation to staff separations
- Conformance with relevant regulatory arrangements, such as privacy, natural justice and human rights.

6.3.4 Physical Security

This section defines the core treatments and controls in relation to the physical security outcomes defined at Tier 2, focussing on the physical (including electronic) measures designed to protect the entity's people and valuable information and assets. Core treatments might include key attributes of, and guidance on:

- Entity physical security policy, as part of overall enterprise security planning
- Policies and processes enabling entities to ensure that protective security considerations are reflected in physical design, construction and fit out

- Conformance with relevant regulatory provisions, such as work health and safety and emergency management legislation
- Maintaining sufficient physical protections of classified information and assets, including ICT systems.

6.4 Reference to Tier 4

Tier 4 (detailed guidelines) falls outside of the scope of this international standard, and relates to specific standards, policy and better practice guidance. Tier 4 would include, for example, detailed guidance for effective vetting and ongoing post-employment monitoring, or 'aftercare' as this is known in some jurisdictions. Importantly, the necessity of clearly delineating the attributes and nature of Tiers 1, 2 and 3 is necessary in delivering strategically aligned Tier 4 guidance – international standards that detail the operational measures and activities that are strategically aligned at the tactical and operational level.

7. Implementation

These sections details guidance on the generic nature of governance arrangements the key elements of work needed to implement coordinated and strategically aligned protective security across the information security, personnel security and physical security domains.

8. Preparing and implementing protective security plans

9. Continuous Improvement

10. Planning, monitoring, review and reporting

11. Reporting

Bibliography