ETSI TR 103 305-4 V1.1.1 (2016-08)

CYBER;
Critical Security Controls for Effective Cyber Defence;
Part 4: Facilitation Mechanisms

Reference
DTR/CYBER-0012-4

Keywords
Cyber Security, Cyber-defence, information assurance

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 4 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.6].

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document is an evolving repository for diverse facilitation mechanism guidelines for Critical Security Control implementations. These mechanisms initially include privacy impact assessment, mapping to well-known cybersecurity frameworks, Cyber Hygiene programs, and management governance.

Introduction

The Critical Security Controls ("the Controls") exist within a larger cyber security ecosystem that relies on the Controls as critically important defensive measures. There are a variety of facilitation mechanisms that facilitate and encourage their use. This document provides a placeholder for such mechanisms, and initially includes four of them: Privacy Impact Assessment, Mapping to Well-Known Cyber Security Frameworks, Cyber Hygiene Programs, Management Governance.

1 Scope

The present document is an evolving repository for diverse facilitation mechanism guidelines for Critical Security Control implementations. These mechanisms initially include privacy impact assessment, mapping to well-known cyber security frameworks, Cyber Hygiene programs, and management governance.

The present document is also technically equivalent and compatible with the 6.0 version of the CIS Companion Guides and Controls appendices C, D, E and F which can be found at the website https://www.cisecurity.org/critical-controls/ [i.1], [i.2].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] The Center for Internet Cybersecurity: "Toward A Privacy Impact Assessment (PIA) Companion to the CIS Critical SecurityControls" version 6, October 15, 2015.

NOTE: Available at https://www.cisecurity.org/critical-controls.cfm.

[i.2] The Center for Internet Cybersecurity: "Critical Security Controls for Effective Cyber Defense Version 6.0" October 15, 2015.

NOTE: Available at https://www.cisecurity.org/critical-controls.cfm.

[i.3] U.S. Department of Homeland Security: "Fair Information Practice Principles (FIPPS)". See also, NIST, "National strategy for trusted identities in cyberspace, Fair Information Practice Principles (FIPPs)".

NOTE: Available at http://www.dhs.gov/publication/fair-information-practice-principles-fipps and http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

[i.4] Information and Privacy Commissioner of Ontario: "Introduction to PbD".

NOTE: Available at https://www.privacybydesign.ca.

[i.5] CIS National Campaign for Cyber Hygiene.

NOTE: Available at https://www.cisecurity.org/cyber-pledge/.

[i.6] ETSI TR 103 305-1: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Critical Security Control (CSC): specified capabilities that reflect the combined knowledge of actual attacks and effective defences of experts that are maintained by the Center for Internet Cybersecurity and found at the website https://www.cisecurity.org/critical-controls/

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Access Control (NIST)
AE	Anomalies and Events (NIST)
AM	Asset Management (NIST)
AN	Analysis (NIST)
ASD	Australian Signals Directorate
AT	Awareness and Training (NIST)
CDM	Continuous Diagnostic and Mitigation
CIS	Center for Internet Security
CM	Continuous Monitoring (NIST)
CSC	Critical Security Control or Capability
CSF	Cybersecurity Framework (NIST)
DHS	Department of Homeland Security
DP	Detection Processes (NIST)
DS	Data Security (NIST)
FIP	Fair Information Practice principles
IM	Improvements
IP	Information Protection
IT	Information Technology
MI	Mitigation (NIST)
NIST	National Institute of Standards and Technology
NIST	National Institute of Standards and Technology
PIA	Privacy Impact Assessment
PII	Personally identifiable information
PT	Principle of Transparency; Protective Technology (NIST)
RA	Risk Assessment
RP	Recovery Planning
SORN	Statement of Records Notice

4 Critical Security Controls: Privacy Impact Assessment

4.0 Description

An effective posture of enterprise cybersecurity need not, and, indeed, should not compromise individual privacy. Many laws, regulations, guidelines, and recommendations exist to safeguard privacy, and enterprises will, in many cases, adapt their existing policies on privacy as they apply the Controls.

At a minimum, use of the Controls should conform to the general principles embodied in the *Fair Information Practice principles* (FIPs) [i.3] and in *Privacy by Design* [i.4]. All enterprises that apply the Controls should undertake - and make available to stakeholders - privacy impact assessments of relevant systems to ensure that appropriate protections are in place as the Controls are implemented. Every enterprise should also regularly review these assessments as material changes to its cybersecurity posture are adopted. The aim is to assess and mitigate the major potential privacy risks associated with implementing specific Controls as well as evaluate the overall impact of the Controls on individual privacy.

To assist enterprises in efforts to conduct a privacy impact assessment when implementing the Controls and to contribute to the establishment of a more general reference standard for privacy and the Controls, the CIS convenes technical and privacy experts to review each Control and offer recommendations for best practice. The following framework guides this efforts and provides an outline for a Privacy Impact Assessment.

4.1 Privacy Impact Assessment of the Critical Security Controls

4.1.1 Overview

Outline the purpose of each Control and provide justification for any actual or potential intersection with privacy-sensitive information:

- Where possible, identify how technologies, procedures, and data flows are used to implement the Control. Provide a brief description of how the Control generally collects and stores information. Identify the type of data collected by the Control and the kinds of information that can be derived from this data. In discussing how the Control might collect and use PII, include a typical transaction that details the life cycle of that PII from collection to disposal.

- Describe the measures necessary to protect privacy data and mitigate any risks of unauthorized access or inadvertent disclosure of the data. The aim here is not to list every possible risk to privacy, but rather, to provide a holistic view of the risks to privacy that could arise from implementation of the Control.

- Describe any potential ad-hoc or routine information sharing that will result from the implementation of the Control both within the enterprise and with external sharing partners. Also describe how such external sharing is compatible with the original collection of the information, and what agreements would need to be in place to support this sharing.

4.1.2 Authorities

Identify the legal authorities or enterprise policies that would permit or, conversely, limit or prohibit the collection or use of information by the Control:

- List the statutory and regulatory authorities that would govern operation of the Control, including the authorities to collect the information identified above. Explain how the statutory and regulatory authorities permit or would limit collection and use of the information or govern geographic storage requirements. If the Control would conceivably collect Personally Identifiable Information (PII), also identify the specific statutory authority that would permit such collection.

- Would the responsible office of an enterprise be able to rely on authorities of another parent organization, subsidiary, partner or agency?

- Might the information collected by the Control be received from a foreign user, organization or government? If so, do any international agreement, contract, privacy policy or memorandum of understanding exist to support or otherwise govern this collection?

4.1.3 Characterizing Control-Related Information

Identify the type of data the Control collects, uses, disseminates, or maintains:

- For each Control, identify both the categories of technology sources, logs, or individuals from whom information would be collected, and, for each category, list any potential PII, that might be gathered, used, or stored to support the Control:
  - Relevant information here includes (but is not limited to): name; date of birth; mailing address; telephone numbers; social security number; e-mail address; mother's maiden name; medical records locators; bank account numbers; health plan beneficiaries; any other account numbers; certificates or other license numbers; vehicle identifiers, including license plates; marriage records; civil or criminal history information; medical records; device identifiers and serial numbers; education records; biometric identifiers; photographic facial images; or any other unique identifying number or characteristic.
- If the output of the Control, or system on which it operates, creates new information from data collected (for example, a scoring, analysis, or report), might this new information have privacy implications? If so, perform the same above analysis on the newly created information.
- If the Control uses information from commercial sources or publicly available data to enrich other data collected, explain how this information might be used:
  - Commercial data includes information from data aggregators (such as threat feeds, or malware databases), or from social networking sources where the information was originally collected by a private organization.
  - Publicly available data includes information obtained from the internet, news feeds, or from state or local public records, such as court records where the records are received directly from the state or local agency, rather than from a commercial data aggregator.
  - Identify scenarios with this enriched data might derive data that could have privacy implications. If so, perform the same above analysis on the newly created information.
- Identify and discuss the privacy risks for Control information and explain how they are mitigated. Specific risks may be inherent in the sources or methods of collection.
- Consider the following Fair Information Practice principles (FIPs):
  - *Principle of Purpose Specification:* Explain how the collection of PII by the Control links to the cybersecurity needs of the enterprise.
  - *Principle of Minimization:* Is the PII data directly relevant and necessary to accomplish the specific purposes of the Control?
  - *Principle of Individual Participation:* Does the Control, to the extent possible and practical, collect PII directly from individuals?

4.1.4 Uses of Control-Related Information

Describe the Control's use of PII or privacy protected data. Describe how and why the Control uses this data:

- List likely uses of the information collected or maintained, both internal and external to the enterprise. Explain how and why different data elements will be used. If Social Security numbers are collected for any reason, for example, describe why such collection is necessary and how such information would be used. Describe types of procedures and protections to be in place to ensure that information is handled appropriately, and policies that need to be in place to provide user notification.
- Does the Control make use of technology to conduct electronic searches, queries, or analyses in a database to discover or locate a predictive pattern or an anomaly? If so, describe what results would be achieved and if there would be possibility of privacy implications.

- Some Controls require the processing of large amounts of information in response to user inquiry or programmed functions. The Controls may help identify data that were previously not identifiable and may generate the need for additional research by analysts or other employees. Some Controls are designed to perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis.

- Discuss the results generated by the uses described above, including link analysis, scoring, or other analyses. These results may be generated electronically by the information system, or manually through review by an analyst. Would these results potentially have privacy implications?

- Are there other offices or departments within or connected to the enterprise that would receive any data generated? Would there be privacy implications to their use or collection of this data?

- Consider the following FIPs:

  - *Principle of Transparency:* Is the PIA and related policies clear about the uses of information generated by the Control?

  - *Principle of Use Limitation*: Is the use of information contained in the system relevant to the mission of the Control?

4.1.5 Security

Complete a security plan for the information system(s) supporting the Control:

- Is there appropriate guidance when implementing the Control to ensure that appropriate physical, personnel, IT, and other safeguards are in place to protect privacy protected data flowing to and generated from the Control?

- Consider the following Fair Information Practice principle:

  - *Principle of Security*: Is the security appropriate and proportionate to the protected data?

4.1.6 Notice

Identify if any notice to individuals should be put in place regarding implementation of the Control, PII collected, the right to consent to uses of information, and the right to decline to provide information (if practicable):

- Define how the enterprise might require notice to individuals prior to the collection of information.

- Enterprises often provide written or oral notice to employees, customers, shareholders, and other stakeholders before they collect information from individuals. In the U.S. government, that notice may include a posted privacy policy, a Privacy Act statement, a Privacy Impact Assessment, or a Statement of Records Notice (SORN) published in the *U.S. Federal Register*. For private companies, collecting information from consumers, publicly available privacy policies are used. Describe what notice might be relevant to individuals whose information might be collected by the Control.

- If notice might not, or cannot be provided, define if one is required or how it can be mitigated. For certain law enforcement operations, notice may not be appropriate - enterprises would then explain how providing direct notice to the individual at the time of collection would undermine a law enforcement mission.

- Discuss how the notice provided corresponds to the purpose of the Control and the declared uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how implementation of the Control mitigates the risks associated with potentially insufficient notice and opportunity to decline or consent.

- Consider the following FIPs:

  - *Principle of Transparency*: Will this Control allow sufficient notice to be provided to individuals?

  - *Principle of Use Limitation:* Is the information used only for the purpose for which notice was provided either directly to individuals or through a public notice? What procedures can be put in place to ensure that information is used only for the purpose articulated in the notice?

- *Principle of Individual Participation*: Will the enterprise be required to provide notice to individuals regarding redress, including access and correction, including other purposes of notice such as types of information and controls over security, retention, disposal, etc.?

4.1.7 Data Retention

Will there be a requirement to develop a records retention policy, subject to approval by the appropriate enterprise authorities (e.g. management, Board), to govern information gathered and generated by the Control?

- Consider the following FIPs below to assist in providing a response:
  - *Principle of Minimization:* Does the Control have the capacity to use only the information necessary for declared purposes? Would the Control be able to manage PII retained only for as long as necessary and relevant to fulfil the specified purposes?
  - *Principle of Data Quality and Integrity:* Does the PIA describe policies and procedures required by an organization for how PII is purged once it is determined to be no longer relevant and necessary?

4.1.8 Information Sharing

Describe the scope of the information sharing within and external to the enterprise that could be required to support the Control. External sharing encompasses sharing with other businesses, vendors, private sector groups, or federal, state, local, tribal, and territorial government, as well as with governments or official agencies of other countries:

- For state or local government agencies, or private sector organizations list the general types that might be applicable for the Control, rather than the specific names.
- Describe any agreements that might be required for an organization to conduct information sharing as part of normal enterprise operations.
- Discuss the privacy risks associated with the sharing of information outside of the enterprise. How can those risks be mitigated?
- Discuss how the sharing of information is compatible with the stated purpose and use of the original collection for the Control.

4.1.9 Redress

Enterprises should have in place procedures for individuals to seek redress if they believe their PII may have been improperly or inadvertently disclosed or misused through implementation of the Controls. These procedures may include allowing them to file complaints about what data is collected or how it is used:

- Consider the following issue that falls under the FIP principle of *Individual Participation*:
  - Can a mechanism be applied by which an individual can prevent PII obtained for one purpose from being used for other purposes without the individual's knowledge?

4.1.10 Auditing and Accountability

Describe what technical and policy based safeguards and security measures might be needed to support the Control. Include an examination of technical and policy safeguards, such as information sharing protocols, special access restrictions, and other controls:

- Discuss whether the Control allows for self-audits, permits third party audits, or allows real time or forensic reviews by appropriate oversight agencies.
- Do the IT systems supporting the Control have automated tools to indicate when information is possibly being misused?

- Describe what requirements for privacy training should be provided to users either generally or specifically relevant to the Control, including information handling procedures and sensitivity of information. Discuss how individuals who have access to PII collected or generated by the Control should be trained to appropriately handle that information.

- Discuss the types of processes and procedures necessary to review and approve information sharing agreements, new uses of Control information, and new access to Control information by other parties.

5 Critical Security Controls: Mapping to Well-Known Cyber Security Frameworks

Since its release in February 2014, the NIST *Framework for Improving Critical Infrastructure Cybersecurity* has become well-known as a major part of national conversations about cybersecurity for critical infrastructure (and beyond). It represents an important step towards large-scale and specific improvements in national security. The Critical Security Controls are called out in the NIST Framework as one of the "Informative References" that can be used to drive specific implementation.

The NIST Framework is true to the dictionary definition of its name - "a set of principles, ideas, etc. that you use when you are forming your decisions and judgments" - and it provides a way to organize, conduct, and drive the conversation about security goals and improvements, for individual enterprises and across communities of enterprises. However, it does not include any specific risk management process, or specify any priority of action. Those "decisions and judgments" are left to the adopter to manage for their specific situation and context.

For the vast majority of enterprises, the best approach to solving these problems is to tackle them as a community - not enterprise-by-enterprise. Below is an example of the working aids maintained to help communities leverage the Framework. This chart shows the mapping from the Critical Security Controls (Version 6.0) into the most relevant NIST CSF (Version 1.0) Core Functions and Categories.

Table 1: CSC controls mapping to NIST Cybersecurity Framework (CSF) Core

	Cybersecurity Framework (CSF) Core				
Critical Security Controls (V6.0)	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
CSC 1: Inventory of Authorized and Unauthorized Devices	AM				
CSC 2: Inventory of Authorized and Unauthorized Software	AM				
CSC 3: Secure Configuration of End user devices		IP			
CSC 4: Continuous Vulnerability Assessment and Remediation	RA		CM	MI	
CSC 5: Controlled Use of Administrative Privileges		AC			
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs			AE	AN	
CSC 7: Email and Web Browser Protections		PT			
CSC 8: Malware Defense		PT	CM		
CSC 9: Limitation and Control of Network Ports, Protocols, and Service		IP			
CSC 10: Data Recovery Capability					RP
CSC 11: Secure Configuration of Network Devices		IP			
CSC 12: Boundary Defense			DP		
CSC 13: Data Protection		DS			
CSC 14: Controlled Access Based on Need to Know		AC			
CSC 15: Wireless Access Control		AC			
CSC 16: Account Monitoring and Control		AC	CM		
CSC 17: Security Skills Assessment and Appropriate Training		AT			
CSC 18: Application Software Security		IP			

	Cybersecurity Framework (CSF) Core				
Critical Security Controls (V6.0)	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
CSC 19: Incident Response and Management			AE	RP	
CSC 20: Penetration Tests and Red Team Exercises				IM	IM

6 Critical Security Controls: Cyber Hygiene Programs

National Campaigns for Cyber Hygiene have been developed to provide a plain-language, accessible, and low-cost foundation for implementation of the Critical Security Controls. [i.5] Although the Controls already simplify the challenges of cyber defense by creating community priorities and action, many enterprises are starting from a very basic level of security.

Such a Campaign starts with a few basic questions that corporate and government leaders should be able to answer:

- What is connected to their systems and networks? (CSC 1).
- What software is running (or trying to run) on their systems and networks? (CSC 2).
- Are their systems continuously managed using "known good" configurations? (CSC 3).
- Is someone continuously looking for and managing "known bad" software? (CSC 4).
- Do limits and tracking exist for the people who have the administrative privileges to change, bypass, or over-ride security settings? (CSC 5).

These questions, and the actions required to answer them, are represented in "plain language" by the Top 5 Priorities of the Campaign: **"Count, Configure, Control Patch, Repeat"**. Documentation and "toolkits" exist to guide implementation [i.5].

Although the language is simple, each of these questions is associated with a primary Control that provides an action plan. The Campaign is also designed to be in alignment with the first 5 of the Critical Security Controls, the Australian Signals Directorate's (ASD) "Top Four Strategies to Mitigate Targeted Intrusions, and the DHS Continuous Diagnostic and Mitigation (CDM) Program. This provides a strong and defendable basis for the Campaign Priorities, a growth path for maturity beyond these basic actions, and the benefits of a large community of experts, users, and vendors.

7 Critical Security Controls: Management Governance

7.0 General

Cybersecurity governance is a key responsibility senior management in any organization, and it should be an integral part of overall enterprise governance. Because of its dynamic nature, cybersecurity governance should also be aligned with an *operational* cybersecurity framework.

To exercise effective governance, executives should have a clear understanding of what to expect from their information security program. They need to know how to direct the implementation, evaluate their own status with regard to existing security programs, and determine the strategy and objectives of an effective security program.

7.1 How the Critical Security Controls Can Help

7.1.0 Introduction

The Controls are actionable, automated activities that detect and prevent attacks against a network and the most important data. They support enterprise security governance programs by bridging the gap from an executive view of business risk to a technical view of specific actions and operational controls to manage those risks. Key executive concerns about information security risks can be translated into specific programs for security improvement, and also into day-to-day security tasks for front-line personnel. This allows better alignment top-to-bottom of corporate risk management. Also, since the Controls are created and supported by a large independent community of practitioners and vendors, they provide a specific, supported, and open baseline for measurement and negotiation about security improvement - one that is demonstrably in alignment with essentially all formal regulatory, governance and oversight frameworks.

To help improve an organization's ability to manage information risks, some sample steps are listed below to help align organization governance concerns with the implementation of security controls. These examples identify the primary, but not the only, Critical Security Controls to be implemented.

7.1.1 Governance item #1: Identify the most important information assets and the impact on business or mission if they are compromised

Information is the lifeblood of every modern enterprise, and the movement, storage, and control of that information is inextricably bound to the use of Information Technology. Therefore the following Critical Security Controls are the primary means to track and control the system components that manage the flow, presentation and use of information:

- CSC 1: Inventory of Authorized and Unauthorized Devices.
- CSC 2: Inventory of Authorized and Unauthorized and Software.

7.1.2 Governance Item #2: Manage the known cyber vulnerabilities of your information and make sure the necessary security policies are in place to manage the risk

At a minimum, you should be able to identify and manage the large volume of *known* flaws and vulnerabilities found in Information Technology and processes. The following Critical Security Controls are the primary means to establish a baseline of responsible practices that can be measured, managed, and reported:

- CSC 3: Secure Configurations of Hardware and Software.
- CSC 4: Continuous Vulnerability Assessment and Remediation.

7.1.3 Governance Item #3: Clearly identify the key threats to your information and assess the weaknesses in your defense

Threats to information, systems, and processes evolve constantly. The following Critical Security Controls are the primary means to establish a baseline of responsible practices that can be measured, managed, and reported:

- CSC 8: Malware Defenses.
- CSC 20: Penetration Tests and Red Team Exercises.

7.1.4 Governance Item #4: Confirm and control who has access to the most important information

Ensuring that the right people have access to corporate data and ensuring privileges are managed accurately can reduce the impact of unauthorized access, both from internal threats and external. The following Critical Security Controls are the primary means to establish a baseline of responsible practices to identify needs and manage access:

- CSC 5: Controlled Use of Administrative Privileges.
- CSC 14: Controlled Access Based on the Need to Know.

A fundamental goal of information security is to reduce adverse impacts on the organization to an acceptable level of risk. Therefore, a crucial metric comprises the adverse impacts of information security incidents experienced by the company. An effective security program will show a trend of impact reduction. Quantitative measures can include trend analysis of impacts over time.

7.2 Developing an Overall Governance Strategy

While the Critical Security Controls provide an effective way to plan, prioritize, and implement primarily *technical* controls for cyberdefense, they are best used as part of a holistic information governance program - one that also addresses policies, standards, and guidelines that support technical implementations. For example, conducting an inventory of devices on the network is an important technical best practice, but an organization should also define and publish policies and processes that clearly communicate to employees the purpose of these controls, what is expected of them and the role they play in protecting the organization's interests.

The following topics provide a useful framework for developing your overall governance strategy. Based on experience, these are prioritized based on their impact in building and supporting an effective information assurance program:

- **Executive Sponsorship:** Develop information assurance charters with roles and responsibilities, steering committees, and board of director briefings to establish support and leadership from executives.
- **Information Assurance Program Management:** Define management and resource allocation controls, such as budgeting, and prioritization to govern information assurance programs under executive sponsorship.
- **Information Assurance Policies and Standards Management:** Define and document policies and standards to provide detailed guidance regarding how security controls will be completed to promote consistency in defense.
- **Data Classification:** Identify, prioritize and label data assets, including analog or physical assets.
- **Risk Management:** Identify thoughtful and purposeful defense strategies based on priority decisions on how best to defend valuable data assets.
- **Compliance and Legal Management:** Address compliance requirements based on the regulatory and contractual requirements placed on the organization.
- **Security Awareness and Education:** Establish education plans for all workforce members to ensure that they have the necessary skills to protect information assets as a part of their responsibilities.
- **Audit and Assessment Management:** Conduct audits and assessments to ensure that information assurance efforts are consistent with the standards defined and to assist efforts to manage risk.
- **Personnel and Human Resources Management:** Specify personnel and human resources controls to manage the way people interact with data assets. People, as well as technology controls, are critical for the defense of information assets.
- **Budgets and Resource Management:** Allocate appropriate resources in order to be effective at defense. Information assurance architectures are vital for defense, but without budgets and resources, such plans will never be effective.
- **Physical Security:** Protect the equipment, buildings, and locations where data assets are stored to provide a foundation for the logical security of data assets.

- **Incident Response Management:** Specify the planned management of the response in the face of potentially adverse events. This acts as a component of business continuity and disaster management.
- **Business Continuity and Disaster Recovery Management:** Specify resiliency controls to help mitigate potential losses due to potential disruptions to business operations.
- **Procurement and Vendor Management:** Partner with business associates in defending their data assets. The Controls define how an organization aligns with third parties and vendors to protect their data assets.
- **Change and Configuration Management:** Assess, accept or deny, and log changes to systems, especially configuration changes in a systematic formal manner in order to defend the organization's information assets.

Organizations are encouraged (and many are required) to implement these governance controls in parallel with the technical controls defined elsewhere in this document. Both technical and governance related controls should be considered equally important pillars in the architecture of an organization's defense.

History

Document history		
V1.1.1	August 2016	Publication