Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Information Technology Security Guidance

IT Security Risk Management: A Lifecycle Approach

Suggested organizational security control profile for departments and agencies requiring protection of business activities of security category

Secret / Medium Integrity / Medium Availability

ITSG-33 – Annex 4 – Profile 3

November 2012

Canada

Foreword

Annex 4 – Profile 3 (*Secret / Medium Integrity / Medium Availability*) to *IT Security Risk Management: A Lifecycle Approach (ITSG-33)* is an unclassified publication issued under the authority of the Chief, Communications Security Establishment Canada (CSEC).

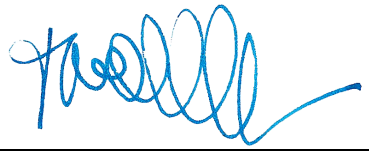
Suggestions for amendments should be forwarded through departmental communications security channels to your Information Technology (IT) Security Client Services Representative at CSEC.

Requests for additional copies or changes in distribution should be directed to your IT Security Client Services Representative at CSEC.

For further information, please contact CSEC's IT Security Client Services area by e-mail at itsclientservices@cse-cst.gc.ca, or call (613) 991-7654.

Effective Date

This publication takes effect on 1 November 2012.



Toni Moffa

Deputy Chief, IT Security

Summary

This Annex is part of a series of documents published by the Communications Security Establishment Canada (CSEC) under Information Technology Security Guidance Publication 33 (ITSG-33), *IT Security Risk Management: A Lifecycle Approach*.

This Annex suggests a selection of security controls and control enhancements, together referred to as a *security control profile*. Departmental security authorities can use this profile as a reference to create departmental-specific security control profiles suitable for protecting the confidentiality, integrity, and availability of departmental information technology (IT) assets against threats that could cause injury to business activities of category Secret / Medium Integrity / Medium Availability. This security control profile has been developed using ITSG-33 Annex 3, *Security Control Catalogue* [Reference 1].

The suggested security controls in this profile constitute a starting point and need to be tailored to the business context, technical context, and threat and risk context of each department's business activities and the information systems supporting them. The selection of security controls was based on industry and governmental security best practices, and under certain threat assumptions, derived from CSEC's analysis of the threat environment faced by information systems in the documented business context.

This profile has been created as a tool to assist security practitioners in their efforts to protect information systems in compliance with applicable Government of Canada (GC) legislation and Treasury Board of Canada Secretariat (TBS) policies, directives, and standards.

It is the responsibility of departmental security authorities, when developing their departmental security control profiles, to ensure compliance to all security requirements of GC regulations and TBS policy instruments applicable to their business activities, and any other obligations they may have contracted.

Revision History

Document No.	Title	Release Date
ITSG-33 Annex 4 – Profile 3	IT Security Risk Management: A Lifecycle Approach - Secret / Medium Integrity / Medium Availability Profile	1 November 2012

Table of Contents

List of Tables

List of Abbreviations and Acronyms

COTS	Commercial off the Shelf
CSEC	Communications Security Establishment Canada
DSO	Departmental Security Officer
GC	Government of Canada
ISSIP	Information System Security Implementation Process
IT	Information Technology
ITSG	Information Technology Security Guidance
PDARR	Prevention Detection Analysis Response Recovery
SAL	Security Assurance Level
TBS	Treasury Board of Canada Secretariat

1 Introduction

1.1 Purpose

This Annex is part of a series of documents published by the Communications Security Establishment Canada (CSEC) under Information Technology Security Guidance Publication 33 (ITSG-33), *IT Security Risk Management: A Lifecycle Approach*.

This Annex suggests a selection of security controls and control enhancements, together referred to as a *security control profile*. Departmental security authorities can use this profile as a reference to create departmental-specific security control profiles suitable for protecting the confidentiality, integrity, and availability of departmental information technology (IT) assets against threats that could cause injury to business activities of category Secret / Medium Integrity / Medium Availability. The security control profile presented in this document has been developed using ITSG-33 Annex 3, *Security Control Catalogue* [Reference 1].

Departmental security control profiles help ensure that the IT security function of a departmental security program performs appropriate IT security risk management activities, and that it provides adequate support to IT projects.

1.2 Scope and Applicability

The suggested security controls in this profile constitute a starting point and need to be tailored to the business context, technical context, and threat and risk context of each department[1]'s business activities and the information systems supporting them (as described in Section 2). The selection of security controls was based on industry and governmental security best practices, and under certain threat assumptions, derived from CSEC's analysis of the threat environment faced by information systems in the documented business context.

This profile does not provide details about the implementation or utilization of these security controls in a department or its information systems. ITSG-33 Annex 1 – *Departmental IT Security Risk Management Activities* [Reference 2] and Annex 2 – *Information System Security Risk Management Activities* [Reference 3] provide more detail guidance on these topics. Refer to CSEC's web site for a current list of additional guidance publications (www.cse-cst.gc.ca).

1.3 Audience

This Annex is intended for:

- Departmental security officers (DSOs), IT security coordinators, and security practitioners supporting departmental IT security risk management activities; and

[1] For the purposes of this publication, the term *department* is used to mean Government of Canada (GC) departments, agencies, and other organizations subject to the *Policy on Government Security*.

- Participants in the definition, design, development, installation, and operations of information systems, more specifically authorizers, project managers, security architects, security practitioners, security assessors, and members of IT operations groups.

1.4 Publication Taxonomy

This Annex is part of a suite of documents on IT security risk management in the GC. The other documents in the series are as follows:

- ITSG-33, Overview – *IT Security Risk Management: A Lifecycle Approach*
- ITSG-33, Annex 1 – *Departmental IT Security Risk Management Activities*
- ITSG-33, Annex 2 – *Information System Security Risk Management Activities*
- ITSG-33, Annex 3 – *Security Control Catalogue*
- ITSG-33, Annex 5 – *Glossary*

1.5 Definitions

should	This word indicates a goal or preferred alternative. There may exist valid reasons in particular circumstances to ignore a particular item or statement, but the full implications must be understood and carefully weighed before choosing a different course.
must	This word means that the statement is a mandatory requirement.

For other definitions of key terms used in this publication, refer to Annex 5 of ITSG-33 [Reference 4].

2 Context and Assumptions

This section characterizes the business context, the technical and threat context, and the security approaches for which this security control profile is suitable. When selecting this profile as a starting point, departmental security authorities (supported by security practitioners) need to tailor it to create departmental-specific security control profiles appropriate to their department and business activities.

2.1 Business Context

This security control profile is suitable for departments using information systems to support GC business activities of medium sensitivity and criticality involving Secret information. Examples of such business activities include, but are not limited to, plan new federal budget, manage diplomatic correspondence, analyze intelligence information, conduct National Defence command and control operations, conduct a criminal investigation on organized crime.

Departments that are candidates for using this security control profile will perform business activities with a maximum security category marking of (Secret / Medium Integrity / Medium Availability), as defined in ITSG-33, Annex 1, Section 6 [Reference 2]. Business activities with such a marking have the following general characteristics:

- Confidentiality – They handle Secret information. A compromise of the confidentiality of this Secret information is reasonably expected to cause a high level of injury to national interests;
- Integrity – A compromise of the integrity of supporting IT assets[2] is reasonably expected to cause a medium level of injury to national or non-national interests;
- Availability – A compromise of the availability of supporting IT assets is reasonably expected to cause a medium level of injury to national or non-national interests; and
- Acceptable residual risks[3] – The business activities require the support of an information system operating with residual risks at a maximum level of low for the security objectives of confidentiality, integrity and availability.

Table 1 characterizes in greater detail suitable business contexts using confidentiality, integrity, and availability objectives and examples of consequences of compromise, business processes, and related information.

[2] An *IT asset* is a generic term used to represent business applications, electronic representations of information (data), and the hardware, software, and system data that information systems are composed of.

[3] The acceptable residual risks are expressed as a business owner (or authorizer) requirement. In normal circumstances, IT projects should be able to deliver an information system that operates with residual risks no higher than what was defined as acceptable, if they adequately implement and operate the security controls specified in this profile, given a similar business, threat, and technology contexts. Acceptable residual risks are sometimes known as target residual risks, or simply acceptable risks.

2.1.1 Compliance with GC Legislation and TBS Policy Instruments

This profile has been created as a tool to assist security practitioners in their efforts to protect information systems in compliance with applicable GC legislation and Treasury Board of Canada Secretariat (TBS) policies, directives, and standards.

It is the responsibility of departmental security authorities, when developing their departmental security control profiles, to ensure compliance to all security requirements of GC regulations and TBS policy instruments applicable to their business activities, and any other obligations they may have contracted.

Table 1: Characterization of Applicable Business Contexts

Characteristics	Descriptions and Examples
Confidentiality Objective	The business activities involve the processing, transmission, and storage of Secret information that needs to be adequately protected from compromise.
Integrity and Availability Objective	The expected injury from threat compromise of IT asset integrity and availability is assessed as medium. IT assets therefore need to be adequately protected from integrity and availability compromise.
Acceptable Residual Risks	The business activities require the support of an information system operating with residual risks at a maximum level of low for the security objectives of confidentiality, integrity and availability.
Examples of Injuries	Compromise of supporting information systems could reasonably be expected to cause: • Civil disorder or unrest such as a riot or the sabotage of a critical infrastructure • Physical pain, injury, trauma, hardship, illness, or disability to individuals, loss of life • Stress, distress, psychological trauma, or mental illness • Financial loss to individuals that affects their quality of life or compromises their financial security • Financial loss to Canadian companies that reduces their competitiveness or compromises the viability • Harm to the Canadian economy that reduces Canada's performance or internal competitiveness in a key business sector • Harm to Canada's reputation (e.g., embarrassment) , damage to federal-provincial relations • Impediment to the development of major government policies • Impediments to effective law enforcement • Loss of continuity of government
Examples of Business Processes	• Senior management processes whose disruption could impede effective decision making • Consular and passport processes whose disruption could hinder assistance to Canadians abroad • Creation and sharing of diplomatic analysis and reports • Creation and sharing of critical infrastructure risk analysis and reports • Automated support to national emergency responses, including information sharing • Creation, processing, and storing of information concerning national defence
Examples of Information Assets	• Sensitive diplomatic information • Critical infrastructure risk analysis • Information concerning national safety and security • Information concerning national defence

2.2 Technical Context

This security control profile is suitable for departments operating in well-controlled IT environments. In general terms, the departmental information systems targeted by this profile can be broadly categorized based on their objective to provide for the creation, processing, storage, and sharing of Secret information.

It is assumed that these information systems will ***not*** be connected directly to the Internet. These information systems may be connected to other GC departments' information systems of equivalent security posture through appropriate high-robustness cross-domain solutions and Type 1-encrypted communication links. Any transfer of information between the Secret information systems and unclassified information systems is assumed to be well controlled through the use of appropriate secure transfer mechanisms. *This profile must be tailored to add the required security controls related to cross-domain functionality.* These safeguards create a high-robustness enclave boundary (see Section 2.4).

This profile may not be suitable for an operational military context, or when implementing a highly distributed network without extensive tailoring.

2.3 Threat Context

This security control profile has been developed to protect departmental business activities from IT-related threats that are relevant to both the business context and the technical context.

In addition to the objective of protecting business activities, this profile seeks the protection of the information systems themselves. This approach is necessary as threats may be directed at GC IT assets for no other reasons than to compromise technical components and benefit form their resources, irrespective of the type of business activities being supported by these IT assets.

Threat information has been analyzed from multiple sources, including TBS and departmental threat and incident reports, in addition to CSEC's own analysis. As a result, this security control profile, when properly implemented (see Section 3), mitigates the risks from exposure to deliberate threat agents of categories from Td1 to Td4 (internal to the enclave boundary) and up to Td7 (external to the boundary, when using appropriate perimeter controls, Type 1 devices, and cross-domain solutions), and accidental threats and natural hazards of categories Ta1 to Ta3 as shown in Table 2 and Table 3, respectively. Note that as threat agent capabilities evolve over time, this security control profile will be updated to ensure that the selection of security controls is appropriately adjusted to mitigate new capabilities.

Before selecting and tailoring this profile, departments must ensure that the threat context is applicable to their environment. If not, substantial tailoring might be necessary, or if the threat context is very different, a different security control profile should be selected if available. If no suitable security control profile is available, departments will have to create their own profile by considering the suite of security controls documented in ITSG-33 Annex 3, *Security Control Catalogue* [Reference 1]. Refer to ITSG-33 Annex 1 [Reference 2] for more details on the creation of security control profiles.

Table 2: Applicable Deliberate Threat Categories

Threat Category	Threat Agent Description	Examples of Increasing Threat Agent Capabilities
Internal to the high-robustness enclave boundary:		
Td1	Non-malicious adversary (e.g., non-malicious unauthorized browsing, modification, or destruction of information due to the lack of training, concern, or attentiveness.)	Basic end user capabilities to access information systems and contents
Td2	Passive, casual adversary with minimal resources who is willing to take little risk (e.g., listening, *script kiddie*).	• Execution of a publicly available vulnerability scanner • Execution of scripts to attack servers • Attempts to randomly delete system files • Modification of configuration files settings
Td3	Adversary with minimal resources who is willing to take significant risk (e.g., unsophisticated hackers).	• Use of publicly available hacker tools to run various exploits • Insiders installing trojans and key loggers on unprotected systems • Use of simple phishing attacks to compromise targets with malware • Execution of programs to crash computers and applications
Td4	Sophisticated adversary with moderate resources who is willing to take little risk (e.g., organized crime, sophisticated hackers, international corporations).	• Sophisticated use of publicly available hacker tools, including 0-day exploits • Ability to create own attack tools in software • Basic social engineering attacks • Ability to assemble hardware using commercial off the shelf (COTS) components to facilitate attacks • Phishing attacks to gain access to credit card or personal data
External to the high-robustness enclave boundary, all previous threat levels in addition to:		
Td5	Sophisticated adversary with moderate resources who is willing to take significant risk (e.g., organized crime, international terrorists).	• Bribery of insiders to get information • Modification of or fraudulent commercial products to support financial gain (e.g., tampered or bogus ATM cash machines) • Physical destruction of infrastructure • Side-channel attacks (e.g., smart cards)
Td6	Extremely sophisticated adversary with abundant resources who is willing to take little risk (e.g., well-funded national laboratory, nation-state, international corporation).	• TEMPEST attacks • Supply chain attacks, such as tampering of or fraudulent commercial products to support espionage (e.g., bogus network routers) • Hard to detect implant technologies in hardware or software • Exploitation of non-public vulnerabilities

Threat Category	Threat Agent Description	Examples of Increasing Threat Agent Capabilities
Td7	Extremely sophisticated adversary with abundant resources who is willing to take extreme risk (e.g., nation-states in time of crisis).	• Bribery, blackmail, or intimidation of insiders to compromise system security • Penetration of secure facilities to enable attacks

Table 3: Applicable Accidental Threats and Natural Hazard Categories

Threat Category	Magnitude of Events
Ta1	Minor accidental events (e.g., trip over a power cord, enter wrong information)
Ta2	• Moderate accidental events (e.g., render a server inoperable, database corruption, release information to wrong individual or organization) • Minor hardware or software failures (e.g., hard disk failure) • Minor mechanical failures (e.g., power failure within a section of a facility) • Minor natural hazards (e.g., localized flooding, earthquake compromising part of a facility)
Ta3	• Serious inadvertent or accidental events (e.g., cut facility telecommunications or power cables, fire in the facility, large scale compromise of information) • Moderate mechanical failures (e.g., long term facility power failure) • Moderate natural hazards (e.g., localized flooding or earthquake compromising a facility)

2.4 Security Approaches

In addition to the business, technical, and threat contexts documented in previous sections, the selection of security controls documented in Section 4 was also influenced by the choice of security engineering best-practices applied to the implementation of dependable information systems. This profile is meant to address the IT security needs of high sensitivity and medium criticality GC business activities, such as plan new federal budget, manage diplomatic correspondence, analyze intelligence information, conduct National Defence command and control operations, and conduct a criminal investigation on organized crime. The protection of these various business activities call for security approaches where these main security engineering best-practices are applied, at a minimum:

- Strong boundary protection, where high-assurance communications links (e.g., Type1 crypto) and cross-domain solutions are utilized to create a classified enclave and connections to unsecured external network are prohibited;
- Strong personnel and physical security, where personnel screening to Level 2 (Secret) and above, and Security Zones are utilized;
- A defence-in-depth approach, where technical, operational (including personnel and physical), and management security controls are used in a mutually supportive manner to mitigate risks (e.g., technical access controls used to protect sensitive databases, and additional physical security prevents unauthorized personnel to physically access the databases' servers);
- A least-privilege approach, where users are provided only the minimum access necessary to perform their duties (e.g., day-to-day tasks are performed using limited user accounts only, *not* administrative accounts);
- A prevent-protect-detect-analyze-respond-recover (PDARR) approach, to ensure that successful attacks can be detected and contained, IT assets can be restored to a secure and authentic state, and lessons learned are documented and used to improve the security posture of information systems; and
- A layered defence approach, to ensure the various layers of an information system, such as applications, databases, platforms, middleware, and communications are adequately protected. This approach reduces the risk of a weakness in one part of the information system could be exploited to circumvent safeguards in other parts (e.g., compromised USB storage device at the platform-layer bypasses network-layer boundary protection).

This set of security approaches uses strict boundary protection and strong physical and personnel security as main protection measures, which potentially affords the use of less robust internal security controls, in turn reducing cost and complexity. In particular, this set of security approaches specifies a system-high operating mode. In system-high mode all users are cleared to the highest level of information processed on the information system (Secret), although not all users have a need-to-know or a requirement to access all of the information.

Nevertheless, this profile also suggests a balanced set of security controls to reduce the risks of compromised internal elements of an information system being used to easily compromise additional elements. This profile also suggests security controls to detect, respond, and recover gracefully from

security incidents, as these are bound to happen. Many of these controls are operational controls that a mature IT operations group should have in place not only for security reasons, but also for the efficient and cost-effective day-to-day management of information systems.

This set of security approach requires robust boundary protection, personnel and physical security to ensure risks are mitigated adequately. As such, these critical security controls need to be assessed regularly to ensure they meet their security objectives. This approach allows the internal part of the information systems (inside the boundary) to be secured using a set of security controls similar to the (Protected B, Medium Integrity, Medium Availability) security control profile.

It is important to ensure that this set of security approaches is appropriate to a departmental technical environment before selecting this profile. If not appropriate, then extensive tailoring may be required. It is worth emphasizing that this security profile is not suitable for multi-level information systems.

2.4.1 Relationship of Security Controls to Confidentiality, Integrity, and Availability Objectives

The selection of security controls in this profile aims to ensure the appropriate mitigation of threats that could compromise the confidentiality, integrity, or availability of IT assets supporting departmental business activities. This profile does not document the exact mapping between a security control and the specific objectives that it aims to fulfill. While some security controls map more clearly to a specific objective (e.g., CP-7 Alternate Processing Site maps to an availability objective), most security controls support more than one security objective. For example, most controls in the Access Control family support directly or indirectly all three objectives of confidentiality, integrity, and availability of IT assets. An adequate implementation of access control will mitigate a compromise where a threat agent:

- Exfiltrates sensitive documents (confidentiality objective);
- Modifies maliciously documents or database records (integrity and usually availability objectives);
- Tampers with the proper behaviour of a business application (integrity and possibly availability objective);
- Deletes database records (availability objective); and
- Corrupts a business application to make it inoperative (availability objective).

The tailoring of this security control profile to satisfy departmental or business needs must take into account the complex and subtle relationships between afforded security control protection and the three security objectives that they usually aim to fulfill.

3 Adequate Implementation Guidance

3.1 Security Assurance

Security controls need to be implemented in a manner commensurate with the potential for threat and injury. This profile was developed under certain assumptions as described in Section 2. Consequently, the boundary protection, and personnel and physical security controls should be implemented with a high level of effort and due diligence. The remaining security controls should be implemented with a medium level of effort and due diligence, as described in this section, in order to ensure that the information system supporting the business activities operates with residual risks at a maximum level of low.

In order to meet the security control requirements documented in this profile, departments need to define the level of effort that they will invest in developing, documenting, and assessing the implementation of the security controls.

Annex 1 of ITSG-33 [Reference 1] describes activities suggested to put in place, or to update, the security controls in this profile that relate to the management of IT security risks and those that are not deployed as part of information systems. ITSG-33 does not provide guidance on the level of effort expected for implementation of those common security controls (e.g., incident management, risk assessments, personnel screening program, physical security program). TBS provides guidance on the establishment of mature management practices and produces assessment tools to measure the current maturity level of those practices.

Annex 2 of ITSG-33 [Reference 3] describes a suggested information system security implementation process useful to cost-effectively design, develop, test, install, and operate dependable information systems that satisfy business needs for security. Information systems implement most of the technical security controls of this profile. Annex 2 of ITSG-33 [Reference 3] provides guidance to IT project managers, security practitioners, security assessors, and authorizers on the expected level of effort for the security engineering and security assessment tasks to ensure that the IT security implemented in information systems meets the objectives of this profile.

In the case of security controls implemented in information systems, the appropriate level of effort for security engineering and security assessment tasks are defined as security assurance requirements. These requirements are directed at the tasks that security control designers, developers and implementers need to perform to increase confidence that the security engineering work and documentation produced is adequate, and that security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security objectives defined for the information systems. A Security Assurance Level of 2 (SAL2) as defined in ITSG-33, Annex 2, Section 8 [Reference 3], is suggested for use by IT projects for the implementation of the majority of the security controls in this profile.

For critical security controls, in particular those on the boundary of an information system, and those facing greater threat agent capabilities, an adequate implementation will ensure that a greater level of effort has been applied to the design, development, testing, installation, and operations of these security controls. A Security Assurance Level of 3 (SAL3) as defined in ITSG-33, Annex 2, Section 8 [Reference

3] is suggested for use by IT projects for the implementation of the critical security controls in this profile. Note that this may mean the integration of high-assurance devices, such as Type 1 crypto. In that case, the devices themselves have already been implemented and certified. The integration effort and rigor is placed in the correct installation, configuration, operation, and operational testing of the devices.

Additionally, as described in ITSG-33, Annex 2, Section 7.3.2.1 [Reference 3], any supplier involved in the design, development, or operation of an information system processing Secret information should hold, as a minimum, a Secret facility clearance.

The criticality of a security control is dependent on the specific design of the information systems and need to be determined by IT projects' security practitioners. At a minimum, the critical security controls must include boundary protection, and personnel and physical security.

ITSG-33 Annex 2 [Reference 3] provides more detailed guidance to IT projects on security assurance requirements and the development, documentation, and assessment activities required to satisfy those requirements.

In addition, it is recommended that selected commercial IT products, which perform security functionality, need to be evaluated in order to ensure they perform functionally as required and are sufficiently resilient to identified threats. To facilitate this assurance process and ensure that IT products are evaluated against appropriate security requirements, the following are recommended:

1. For IT products implementing security controls internal to the security boundary, CSEC makes available for departments to use at their discretion, a pool of commercially available products that have been evaluated by CSEC in partnership with certain commercial Laboratories[4]. If Departments choose to leverage this pool of CSEC assured IT products, then procurement vehicles should specify that the selected IT security products be verified by the Common Criteria program against an appropriate security target or CC protection profile[5] (either defined organizationally in security standards, or determined by the IT project's security practitioners to satisfy the requirements of Sections 2 and 3). If the IT product contains a cryptographic module, then it should also be verified by the Cryptographic Module Validation Program[6] (CMVP) against FIPS 140-2.
2. IT products implementing communication encryption at the boundary of the enclave must be implemented using products evaluated and approved by CSEC (e.g., Type 1 products). In addition, the organization must follow CSEC doctrine when using these products.
3. The selection, design and configuration of IT products implementing cross-domain functionality at the boundary of the enclave should be made in collaboration with CSEC.

3.2 Implementation priority guidance

Not all organizations have the necessary budget to simultaneously implement all of the security controls and enhancements that are required. In reality, organizations may be required to implement the security controls and enhancements as time and budget permit. In order to aid organizations in deciding which security controls and enhancements to implement initially, CSEC has categorized security controls and

[4] Refer to http://www.cse-cst.gc.ca/its-sti/services/cc/cp-pc-eng.html for more information.
[5] Refer to http://www.cse-cst.gc.ca/its-sti/services/cc/pp-ppc-eng.html for more information.
[6] Refer to http://csrc.nist.gov/groups/STM/cmvp/index.html for more information.

enhancements into three priority levels, as documented in Table 4 of Section 4. It should be noted that this effort is targeted at new information systems so that the emphasis is on prevention rather than detection or response. Obviously, priorities would be different for existing systems. This implementation priority ensures mitigation of the most common threats while planning for the implementation of the remaining security controls. Note that in order to appropriately secure an information system, and achieve low residual risks, all of the security controls and enhancements specified in the security control profile need to be implemented.

3.3 Format

Table 4 of Section 4 provides the suggested set of security controls and control enhancements for this profile. For each security control, a control ID is provided along with:

- The name of the security control;
- A listing of suggested enhancements;
- Suggested groups responsible (R) to implement or to support (S) the implementation of the control requirements (IT security Function, IT operations group, IT projects, Physical Security Group, Personnel Security Group and Learning Center);
- General tailoring and implementation guidance notes;
- Suggested implementation priority;
- Values for the placeholder parameters documented as part of each security control in the profile; and
- Additional notes regarding the security controls and control enhancements in the context of this profile.

The complete description of the security control, enhancements and placeholder parameters is available in Annex 3 of ITSG-33 (*Security Control Catalogue*) [Reference 1].

Note: To make it easier for security practitioners to create their own departmental security control profile, a spreadsheet document that contains the selection of controls provided in Section 4 is available.

4 Suggested Security Controls and Control Enhancements

Table 4: Suggested Security Controls and Control Enhancements

Family	Control ID	Enhancement	Name	Suggested Assignment						General tailoring and implementation guidance notes	Suggested Priority	Suggested for this Profile	Suggested Placeholder Values	Profile-specific notes
				ITS Func.	IT Ops	IT Project	Phy Sec	Per Sec	Learning					
AC	1		ACCESS CONTROL POLICY AND PROCEDURES	R					S		P1	X	(A) (B) frequency [at a frequency no longer than annually]	
AC	2		ACCOUNT MANAGEMENT	S	R			S		Account review does not need to be a full reconciliation. An incremental (or differential) review from previous review may be sufficient. It is recommended these reviews be performed when physical access list reviews are performed (see PE-2). This security control/enhancement can be addressed by the organization using a combination of automated and procedural controls. The minimization of administrative privileges is an account management best-practice.	P1	X	(J) frequency [at a frequency no longer than monthly]	
AC	2	(1)	ACCOUNT MANAGEMENT		R	S				This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion of this security control/enhancement is strongly encouraged in most cases.	P2	X		
AC	2	(2)	ACCOUNT MANAGEMENT	S	S	R					P2	X	(2) time period [organization-defined]	

AC	2	(3)	ACCOUNT MANAGEMENT	S	S	R				This security control/enhancement requires careful balance between usability and security. Care needs to be taken to ensure that the appropriate balance between the two seemingly conflicting requirements is achieved. Disabling an account is understood to be the equivalent of locking an account. The account can easily be reactivated (unlocked) by an authorized administrator.	P2	X	(3) time period [not to exceed 30 days]	
AC	2	(4)	ACCOUNT MANAGEMENT	S	S	R					P2	X		
AC	2	(5)	ACCOUNT MANAGEMENT	S	R	S			S	Users should be required to log out at the end of the business day in order to enable the organization to apply the appropriate patches to the operating system. Organizations are typically unable to patch the operating system when a user has an active session.	P2	X	(5a) time period [end of business day]	
AC	2	(6)	ACCOUNT MANAGEMENT	S	S	R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AC	2	(7)	ACCOUNT MANAGEMENT	S	R					This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components, and is considered to be best practice. Consequently, inclusion of this security control/enhancement is strongly encouraged in most cases. The minimization of administrative privileges is an account management best-practice.	P2	X		
AC	3		ACCESS ENFORCEMENT	S	S	R					P1	X		
AC	3	(1)	ACCESS ENFORCEMENT								None defined	Not Selected		

AC	3	(2)	ACCESS ENFORCEMENT	S	S	R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis. Dual authorization mechanisms are applicable to specialized systems such as a key management system.	None defined	Not Selected		
AC	3	(3)	ACCESS ENFORCEMENT	S	S	R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		

AC	3	(4)	ACCESS ENFORCEMENT		S	R				This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion of this security control/enhancement is strongly encouraged in most cases.	P2	X		Control enhancement (4) clarifies the Access Enforcement security control by detailing the policy that should be used for access enforcement to Secret information. That is, while the system may be authorized to process Secret, not all information will necessarily be Secret. Therefore, DAC will be used to establish and enforce access controls over Secret information to "need to know." Examples of DAC include Windows groups (at the file object level) and document management systems that allow document access permissions to be modified by the owner.
AC	3	(5)	ACCESS ENFORCEMENT	S	S	R				This security control/enhancement specifies a very specialized and/or advanced capability, typically found in Type 1 devices or guards, that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AC	3	(6)	ACCESS ENFORCEMENT	S	R	S				This security control/enhancement is considered a compensating control that should be applied if the capability cannot be addressed using an alternate security control/enhancement.	None defined	Not Selected		

AC	4		INFORMATION FLOW ENFORCEMENT	S	S	R				Examples of devices that can perform information flow enforcement include firewalls, gateways and virtual private networks. Example technologies of implement this control are the Sender Policy Framework (SPF), that can be used to help protect organizations from spoofed email attacks, web content filtering devices that help protect organizations from malicious web traffic and deny users' access to unauthorized web sites, and Data Loss Prevention products.	P1	X		
AC	4	(1)	INFORMATION FLOW ENFORCEMENT			R				This security control/enhancement specifies a very specialized and/or advanced capability, typically found in CDS, guards or XML firewalls, that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AC	4	(2)	INFORMATION FLOW ENFORCEMENT			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AC	4	(3)	INFORMATION FLOW ENFORCEMENT			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AC	4	(4)	INFORMATION FLOW ENFORCEMENT			R					P1	X		
AC	4	(5)	INFORMATION FLOW ENFORCEMENT	S		R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		

AC	4	(6)	INFORMATION FLOW ENFORCEMENT			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AC	4	(7)	INFORMATION FLOW ENFORCEMENT	S		R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AC	4	(8)	INFORMATION FLOW ENFORCEMENT	S		R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AC	4	(9)	INFORMATION FLOW ENFORCEMENT	S	R	S				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AC	4	(10)	INFORMATION FLOW ENFORCEMENT	S		R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AC	4	(11)	INFORMATION FLOW ENFORCEMENT	S		R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AC	4	(12)	INFORMATION FLOW ENFORCEMENT			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	P1	X		

AC	4	(13)	INFORMATION FLOW ENFORCEMENT			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	P1	X		
AC	4	(14)	INFORMATION FLOW ENFORCEMENT	S		R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	P1	X		
AC	4	(15)	INFORMATION FLOW ENFORCEMENT	S		R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	P1	X		
AC	4	(16)	INFORMATION FLOW ENFORCEMENT	S		R					None defined	Not Selected		
AC	4	(17)	INFORMATION FLOW ENFORCEMENT			R					None defined	Not Selected		
AC	5		SEPARATION OF DUTIES	S	R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
AC	6		LEAST PRIVILEGE	S	R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
AC	6	(1)	LEAST PRIVILEGE	R						This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		

AC	6	(2)	LEAST PRIVILEGE	S	R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
AC	6	(3)	LEAST PRIVILEGE	S	R	S				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis. An example of this would be local administration of a Certification Authority.	None defined	Not Selected		
AC	6	(4)	LEAST PRIVILEGE			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AC	6	(5)	LEAST PRIVILEGE	S	R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
AC	6	(6)	LEAST PRIVILEGE	S	R					This security control/enhancement is not suggested for inclusion in a departmental profile. However, it is recommended that organizations give the security control/enhancement due consideration. There may be a requirement for outside personnel to have privileged access to systems in order to perform maintenance. In all cases, these people should be supervised and their actions carefully audited.	None defined	Not Selected		

AC	7		UNSUCCESSFUL LOGIN ATTEMPTS	S	S	R				This security control/enhancement requires careful balance between usability and security. Care needs to be taken to ensure that the appropriate balance between the two seemingly conflicting requirements is achieved. If possible, an increasing time-out period should be used to deter determined attackers. For example, a original time-out of 5 minutes can become 10 minutes after the next 3 unsuccessful attempts, then 20 minutes, then 40 minutes, etc.	P1	X	(A) number [of a maximum of 5] (A) time period [period of at least 5 minutes] (B) automatic response [locks the account/node for an organization defined time period]	
AC	7	(1)	UNSUCCESSFUL LOGIN ATTEMPTS		S	R				This security control/enhancement requires careful balance between usability and security. Care needs to be taken to ensure that the appropriate balance between the two seemingly conflicting requirements is achieved.	None defined	Not Selected		
AC	7	(2)	UNSUCCESSFUL LOGIN ATTEMPTS	S		R				This security control/enhancement requires careful balance between usability and security. Care needs to be taken to ensure that the appropriate balance between the two seemingly conflicting requirements is achieved.	None defined	Not Selected	number [of a maximum of 10]	
AC	8		SYSTEM USE NOTIFICATION	S	S	R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
AC	9		PREVIOUS LOGON (ACCESS) NOTIFICATION			R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. This security control/enhancement should be implemented where possible and practical. Some COTS operating systems may not support this capability.	P2	X		

AC	9	(1)	PREVIOUS LOGON (ACCESS) NOTIFICATION			R				Control enhancements (1) and (2) may provide an excessive amount of information to the users at logon which may result in a reduction of its utility as a security mechanisms. Unsuccessful logon attempts should be detected and actioned by the audit function within the organization. Furthermore, control enhancements (1) and (2) are not readily provided by many COTS products and as a result may be difficult to implement. However, the enhancements are more easily implementable in custom-built software, and web-based applications. Therefore, control enhancements (1) and (2) are recommended for privileged users, but not generally for all organizational users.	P2	X		
AC	9	(2)	PREVIOUS LOGON (ACCESS) NOTIFICATION	S		R				Control enhancements (1) and (2) may provide an excessive amount of information to the users at logon which may result in a reduction of its utility as a security mechanisms. Unsuccessful logon attempts should be detected and actioned by the audit function within the organization. Furthermore, control enhancements (1) and (2) are not readily provided by many COTS products and as a result may be difficult to implement. However, the enhancements are more easily implementable in custom-built software, and web-based applications. Therefore, control enhancements (1) and (2) are recommended for privileged users, but not generally for all organizational users.	P2	X		

AC	9	(3)	PREVIOUS LOGON (ACCESS) NOTIFICATION	S		R				Control enhancement (3) is beneficial in that successful changes to security-related functions will not be detected by audit. By notifying the user of these changes, the user would be able to initiate a security incident if he/she wasn't responsible for the change.	P2	X		
AC	10		CONCURRENT SESSION CONTROL	S		R					P2	X	(A) concurrent [a number not greater than 3]	
AC	11		SESSION LOCK	S		R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X	(A) time period [after a period no longer than 30 minutes]	
AC	11	(1)	SESSION LOCK			R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
AC	12		SESSION TERMINATION								None defined	Not Selected		
AC	13		SUPERVISION AND REVIEW — ACCESS CONTROL								None defined	Not Selected		
AC	14		PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	R	S	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
AC	14	(1)	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	S		R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
AC	15		AUTOMATED MARKING								None defined	Not Selected		

AC	16		SECURITY ATTRIBUTES	S		R				In terms of security attributes, this guidance refers specifically to a security label that reflects the sensitivity of the resource, including its classification and any additional restrictions (e.g., caveats, warning terms, compartments) (ex: UNCLASSIFIED, PROTECTED A, PROTECTED B//CEO, etc).	P2	X		In the context of this profile, the objective of this control is to achieve consistent labeling of Secret material to the maximum extent supported by available, automated mechanisms (e.g. email system enforcing classification labels). Since not all information on the system will be sensitive, labeling will help prevent the accidental distribution of Secret information by providing filter mechanisms with a differentiator.
AC	16	(1)	SECURITY ATTRIBUTES			R					None defined	Not Selected		
AC	16	(2)	SECURITY ATTRIBUTES			R				Control enhancement (2) and (4) allow authors and other authorized entities to assign security labels to resources.	P2	X		
AC	16	(3)	SECURITY ATTRIBUTES			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis. However, if you are using security labels for access control then the security labels should be cryptographically bound to the data.	None defined	Not Selected		
AC	16	(4)	SECURITY ATTRIBUTES			R				Control enhancement (2) and (4) allow authors and other authorized entities to assign security labels to resources.	P2	X		

AC	16	(5)	SECURITY ATTRIBUTES	S		R				Control enhancement (5) displays the security label in a human readable form. The resulting security marking will encourage proper handling of these resources by users. These enhancements may be implemented by procedural means (e.g. manual insertion of a classification header in a word processing document), or, preferably, managed efficiently by the information system (e.g. enterprise content management (ECM) system) using metadata field.	P2	X		
AC	17		REMOTE ACCESS	S	R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. See IA-2 for authentication requirements related to this control.	P1	X		
AC	17	(1)	REMOTE ACCESS		R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
AC	17	(2)	REMOTE ACCESS		R	S				This security control/enhancement is considered to be best practice. This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
AC	17	(3)	REMOTE ACCESS		R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
AC	17	(4)	REMOTE ACCESS	S	R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		

AC	17	(5)	REMOTE ACCESS	S	R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X	(5) frequency [continuously]	
AC	17	(6)	REMOTE ACCESS	R					S	This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. Control enhancement (6) specifies that information about remote access mechanisms be protected. It is anticipated that this control enhancement could be addressed through a line item in the user training program.	P2	X		
AC	17	(7)	REMOTE ACCESS	S	R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
AC	17	(8)	REMOTE ACCESS	S	R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
AC	17	(100)	REMOTE ACCESS		R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
AC	18		WIRELESS ACCESS	S	R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
AC	18	(1)	WIRELESS ACCESS			R					P2	X		
AC	18	(2)	WIRELESS ACCESS		R	S					P2	X	(2) frequency [continuously]	
AC	18	(3)	WIRELESS ACCESS		R	S					P2	X		

AC	18	(4)	WIRELESS ACCESS		R	S					P2	X		
AC	18	(5)	WIRELESS ACCESS	S	R	S					P1	X		
AC	19		ACCESS CONTROL FOR MOBILE DEVICES	S	R	S					P1	X		
AC	19	(1)	ACCESS CONTROL FOR MOBILE DEVICES	S	R	S			S		P2	X		
AC	19	(2)	ACCESS CONTROL FOR MOBILE DEVICES	R					S	Likewise, organization-owned removable media should not be used in personally owned information systems.	P2	X		
AC	19	(3)	ACCESS CONTROL FOR MOBILE DEVICES	R					S		P2	X		
AC	19	(4)	ACCESS CONTROL FOR MOBILE DEVICES	S	R	S	S		S		P1	X		
AC	19	(100)	ACCESS CONTROL FOR MOBILE DEVICES	R					S		P2	X		
AC	20		USE OF EXTERNAL INFORMATION SYSTEMS	R						This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
AC	20	(1)	USE OF EXTERNAL INFORMATION SYSTEMS	R							P2	X		
AC	20	(2)	USE OF EXTERNAL INFORMATION SYSTEMS	R					S		P2	X		
AC	21		USER-BASED COLLABORATION AND INFORMATION SHARING	S	R	S				Security control (AC-21) aims to ensure that collaboration and information sharing by authorized users with sharing partners is performed in manner consistent with organizational policies.	P2	X		
AC	21	(1)	USER-BASED COLLABORATION AND INFORMATION SHARING		R	S					P2	X		

AC	21	(100)	USER-BASED COLLABORATION AND INFORMATION SHARING	R						P2	X		
AC	22		PUBLICLY ACCESSIBLE CONTENT	R					S	This security control/enhancement is applicable to the organization as opposed to a specific information system.	P1	Not Selected		
AT	1		SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	R					S		P1	X	(A) (B) frequency [at a frequency no longer than annually]	
AT	2		SECURITY AWARENESS	S					R		P1	X	(A) frequency [at a frequency no longer than annually]	
AT	2	(1)	SECURITY AWARENESS	S	S				R	This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AT	3		SECURITY TRAINING	S					R	This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
AT	3	(1)	SECURITY TRAINING	S					R		None defined	Not Selected		
AT	3	(2)	SECURITY TRAINING				R		S		None defined	Not Selected		
AT	4		SECURITY TRAINING RECORDS	R					S		P2	X		
AT	5		CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	R	S				S		None defined	Not Selected		
AU	1		AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	R					S		P1	X	(A) (B) frequency [at a frequency no longer than annually]	

AU	2		AUDITABLE EVENTS	R	S					The information system audits the following privileged user/process events at a minimum: (a) Successful and unsuccessful attempts to access, modify, or delete security objects (Security objects include audit data, system configuration files and file or users' formal access permissions.) (b) Successful and unsuccessful logon attempts (c) Privileged activities or other system level access (see notes for AU-2 (4)) (d) Starting and ending time for user access to the system (e) Concurrent logons from different workstations (f) All program initiations (see notes for AU-2 (4)) In addition, the information system audits the following unprivileged user/process events at a minimum: (a) Successful and unsuccessful attempts to access, modify, or delete security objects (b) Successful and unsuccessful logon attempts (c) Starting and ending time for user access to the system (d) Concurrent logons from different workstations	P1	X	(A) events [Authorizer defined list of auditable events (see column General tailoring and implementation guidance notes)]	
AU	2	(1)	AUDITABLE EVENTS								None defined	Not Selected		
AU	2	(2)	AUDITABLE EVENTS								None defined	Not Selected		
AU	2	(3)	AUDITABLE EVENTS	R	S						P2	X	(3) frequency [at a frequency no longer than annually]	
AU	2	(4)	AUDITABLE EVENTS	R	S					It may not be realistic to audit all privileged functions. Consequently, an organization should audit privileged functions of interest.	P2	X		

AU	3		CONTENT OF AUDIT RECORDS	S		R					P1	X		
AU	3	(1)	CONTENT OF AUDIT RECORDS	S		R				Additional guidance for enhancement (1): Audit events should always be capable of being associated with an individual identity. Associating audit events with a group or role is insufficient.	P2	X		
AU	3	(2)	CONTENT OF AUDIT RECORDS	S	R	S				This security control/enhancement cannot be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, implementation of this security control/enhancement may be somewhat problematic.	None defined	Not Selected		
AU	4		AUDIT STORAGE CAPACITY		R						P1	X		
AU	5		RESPONSE TO AUDIT PROCESSING FAILURES	S	S	R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X	(B) Action [overwrite]	
AU	5	(1)	RESPONSE TO AUDIT PROCESSING FAILURES	S		R					P2	X	(1) Percentage [75%]	
AU	5	(2)	RESPONSE TO AUDIT PROCESSING FAILURES	S		R					None defined	Not Selected		
AU	5	(3)	RESPONSE TO AUDIT PROCESSING FAILURES			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AU	5	(4)	RESPONSE TO AUDIT PROCESSING FAILURES		S	R					None defined	Not Selected		

AU	6		AUDIT REVIEW, ANALYSIS, AND REPORTING	R						In order for audit to be effective, audit logs need to be collected from the various systems, amalgamated centrally and analyzed regularly by an automated tool. This approach ensures that audit logs are scrutinized and that coordinated attacks can be identified. Although an automated capability is preferable, this security control can be met using manual processes.	P1	X		
AU	6	(1)	AUDIT REVIEW, ANALYSIS, AND REPORTING			R					P2	X		
AU	6	(2)	AUDIT REVIEW, ANALYSIS, AND REPORTING								None defined	Not Selected		
AU	6	(3)	AUDIT REVIEW, ANALYSIS, AND REPORTING	R							P2	X		
AU	6	(4)	AUDIT REVIEW, ANALYSIS, AND REPORTING	R	S	S				While control enhancement (4) specifically mentions the use of a SIM (Security Information Management) product, the use of simpler solutions, such as a syslog server and perl scripts capable of parsing the logs may also suffice, depending on the complexity of the information system (e.g. number of servers and network devices to monitor).	P2	X		
AU	6	(5)	AUDIT REVIEW, ANALYSIS, AND REPORTING	R	S	S				This security control/enhancement cannot be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, implementation of this security control/enhancement may be somewhat problematic.	None defined	Not Selected		
AU	6	(6)	AUDIT REVIEW, ANALYSIS, AND REPORTING	R	S		S			This security control/enhancement cannot be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, implementation of this security control/enhancement may be somewhat problematic.	None defined	Not Selected		

AU	6	(7)	AUDIT REVIEW, ANALYSIS, AND REPORTING	R							P2	X		
AU	6	(8)	AUDIT REVIEW, ANALYSIS, AND REPORTING								None defined	Not Selected		
AU	6	(9)	AUDIT REVIEW, ANALYSIS, AND REPORTING	R							None defined	Not Selected		
AU	7		AUDIT REDUCTION AND REPORT GENERATION			R					P2	X		
AU	7	(1)	AUDIT REDUCTION AND REPORT GENERATION			R					P2	X		
AU	8		TIME STAMPS			R					P1	X		
AU	8	(1)	TIME STAMPS			R					P2	X	(1) frequency [a period no longer than daily] (1) time [an Authorizer defined time source]	
AU	9		PROTECTION OF AUDIT INFORMATION			R					P2	X		
AU	9	(1)	PROTECTION OF AUDIT INFORMATION			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AU	9	(2)	PROTECTION OF AUDIT INFORMATION			R					P2	X		
AU	9	(3)	PROTECTION OF AUDIT INFORMATION			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		

AU	9	(4)	PROTECTION OF AUDIT INFORMATION	S	R	S					P2	X		
AU	10		NON-REPUDIATION			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
AU	10	(1)	NON-REPUDIATION			R					None defined	Not Selected		
AU	10	(2)	NON-REPUDIATION			R					None defined	Not Selected		
AU	10	(3)	NON-REPUDIATION			R					None defined	Not Selected		
AU	10	(4)	NON-REPUDIATION			R					None defined	Not Selected		
AU	10	(5)	NON-REPUDIATION			R					None defined	Not Selected		
AU	11		AUDIT RECORD RETENTION	R						Applicable legal requirements may determine the required retention period.	P2	X		
AU	12		AUDIT GENERATION			R				In order to facilitate audit review and analysis, audit records should be time correlated and provided in a common format. Time correlation can be achieved by synchronizing the clocks of the systems generating the audit events.	P1	X	(A) components [Authorizer defined components]	
AU	12	(1)	AUDIT GENERATION			R					P2	X		
AU	12	(2)	AUDIT GENERATION			R				Although control enhancement (2) specifies the use of a standardized format, this should be changed to read common format. As long as the audit events are sent in a common format understandable by the organization it does not matter whether or not the format adheres to a published standard.	P2	X		
AU	13		MONITORING FOR INFORMATION DISCLOSURE	R							None defined	Not Selected		
AU	14		SESSION AUDIT			R					None defined	Not Selected		

AU	14	(1)	SESSION AUDIT			R					None defined	Not Selected		
CA	1		SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES	R					S		P1	X	(A) (B) frequency [at a frequency no longer than annually]	
CA	2		SECURITY ASSESSMENTS	R							P3	X	(B) frequency [Authorizer-determined frequency]	
CA	2	(1)	SECURITY ASSESSMENTS	R							P1	X		
CA	2	(2)	SECURITY ASSESSMENTS	R							P3	X		
CA	3		INFORMATION SYSTEM CONNECTIONS	R	S	S					P1	X		
CA	3	(1)	INFORMATION SYSTEM CONNECTIONS	R							None defined	Not Selected		
CA	3	(2)	INFORMATION SYSTEM CONNECTIONS	R							P1	X		
CA	4		SECURITY CERTIFICATION								None defined	Not Selected		
CA	5		PLAN OF ACTION AND MILESTONES	R							P3	X	(B) frequency [Authorizer-determined frequency]	
CA	5	(1)	PLAN OF ACTION AND MILESTONES	S	R	S				This security control/enhancement specifies the use of an automated mechanism. While there are obvious benefits to the use of such mechanisms, in most cases the use of manual mechanisms will suffice.	None defined	Not Selected		
CA	6		SECURITY AUTHORIZATION	R							P1	X	(C) frequency [Authorizer-determined frequency]	
CA	7		CONTINUOUS MONITORING	R							P2	X		

CA	7	(1)	CONTINUOUS MONITORING	R							P1	X		
CA	7	(2)	CONTINUOUS MONITORING	R							P2	X		
CM	1		CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	R					S		P1	X	(A) (B) frequency [at a frequency no longer than annually]	
CM	2		BASELINE CONFIGURATION	S	R					A baseline configuration should include all current patches for the operating system and applications installed. The baseline should also deactivate all unused ports, services and software and use an hardened configuration (e.g., guest accounts deactivated, access control to all system files and directories applied, default passwords changed)	P1	X		
CM	2	(1)	BASELINE CONFIGURATION	S	R						P2	X		
CM	2	(2)	BASELINE CONFIGURATION	S	R	S				This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
CM	2	(3)	BASELINE CONFIGURATION		R						None defined	Not Selected		
CM	2	(4)	BASELINE CONFIGURATION	R	S						None defined	Not Selected		
CM	2	(5)	BASELINE CONFIGURATION	R	S					This security control enhancement may be implemented by application whitelisting COTS products.	P1	X		
CM	2	(6)	BASELINE CONFIGURATION	S	R						P2	X		
CM	3		CONFIGURATION CHANGE CONTROL	S	R						P1	X	(F) [Configuration Control Board]	
CM	3	(1)	CONFIGURATION CHANGE CONTROL	S	R	S				This security control/enhancement specifies the use of an automated mechanism. While there are obvious benefits to the use of such mechanisms, in most cases the use of manual mechanisms will suffice.	None defined	Not Selected		

CM	3	(2)	CONFIGURATION CHANGE CONTROL		R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
CM	3	(3)	CONFIGURATION CHANGE CONTROL		R	S				This security control/enhancement should be addressed where applicable and if practical to do so. Control enhancement (3) is required to effectively manage deployments with at least some user base (e.g. standard desktop configuration) or with multiple instances of the same server (e.g. server farm). Only in cases where each user system and/or server is unique does it preclude the use of control enhancement (3). An example of this is an update server part of an operating system.	P2	X		
CM	3	(4)	CONFIGURATION CHANGE CONTROL	R						This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
CM	4		SECURITY IMPACT ANALYSIS	S	R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P3	X		
CM	4	(1)	SECURITY IMPACT ANALYSIS	S	R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P3	X		
CM	4	(2)	SECURITY IMPACT ANALYSIS	S	R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P3	X		
CM	5		ACCESS RESTRICTIONS FOR CHANGE	S	R	S	S				P1	X		

CM	5	(1)	ACCESS RESTRICTIONS FOR CHANGE		R	S					P2	X		
CM	5	(2)	ACCESS RESTRICTIONS FOR CHANGE	S	R						P2	X	(2) [at least every 6 months]	
CM	5	(3)	ACCESS RESTRICTIONS FOR CHANGE	S	S	R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
CM	5	(4)	ACCESS RESTRICTIONS FOR CHANGE	S	R					This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected	(4) [Authorizer provided list]	
CM	5	(5)	ACCESS RESTRICTIONS FOR CHANGE	S	R	S					P2	X		
CM	5	(6)	ACCESS RESTRICTIONS FOR CHANGE	R	S	S					P2	X		
CM	5	(7)	ACCESS RESTRICTIONS FOR CHANGE	S		R				Control enhancement (7) can be implemented using readily available tools (e.g., system integrity software) on critical systems. These tools can not only monitor unauthorized changes in files, but also security-critical entries in the operating system registry.	P2	X		
CM	6		CONFIGURATION SETTINGS		R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. Such best practices include disabling unrequired operating system functionality, application security configuration hardening, and randomizing local administrator passwords.	P1	X	(A) [an Authorizer-approved checklist]	
CM	6	(1)	CONFIGURATION SETTINGS		R	S				Control enhancement (1) can be implemented using readily available tools (e.g., Group Policy).	P2	X		

CM	6	(2)	CONFIGURATION SETTINGS		R	S				Control enhancement (2) can be addressed using the same tools as for CM-5 (7).	P2	X		
CM	6	(3)	CONFIGURATION SETTINGS	R	S					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. While control enhancement (3) may be slightly more difficult to implement, it ensures that the organization learns and adapts from previous incidents.	P2	X		
CM	6	(4)	CONFIGURATION SETTINGS			R				This security control/enhancement does not necessitate the use of an automated capability. It can be satisfied through the use of a manual process.	P2	X		
CM	7		LEAST FUNCTIONALITY	S	R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
CM	7	(1)	LEAST FUNCTIONALITY	S	R						P2	X	(1) frequency [at a frequency no longer than annually]	
CM	7	(2)	LEAST FUNCTIONALITY			R					None defined	Not Selected		
CM	7	(3)	LEAST FUNCTIONALITY	R	S	S					P2	X		
CM	8		INFORMATION SYSTEM COMPONENT INVENTORY		R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
CM	8	(1)	INFORMATION SYSTEM COMPONENT INVENTORY		R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		

CM	8	(2)	INFORMATION SYSTEM COMPONENT INVENTORY		R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. Control enhancement (2) is key. Organizations need to maintain an accurate inventory of information system components for both patching and licensing purposes. Automated tools exist to scan the network to identify devices. Note that some network scanning tools used for inventory purposes might trigger alerts on intrusion detection systems. It may thus be necessary to coordinate intrusion detection and network inventory activities to minimize false positives and negatives.	P2	X		
CM	8	(3)	INFORMATION SYSTEM COMPONENT INVENTORY	S	R	S				This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
CM	8	(4)	INFORMATION SYSTEM COMPONENT INVENTORY		R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
CM	8	(5)	INFORMATION SYSTEM COMPONENT INVENTORY		R					Control enhancement (5) ensures that unauthorized components are detected and, just as importantly, that authorized components don't go missing.	P2	X		
CM	8	(6)	INFORMATION SYSTEM COMPONENT INVENTORY		R						P2	X		
CM	9		CONFIGURATION MANAGEMENT PLAN		R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		

CM	9	(1)	CONFIGURATION MANAGEMENT PLAN		R						None defined	Not Selected		
CP	1		CONTINGENCY PLANNING POLICY AND PROCEDURES	R	S		S		S	This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X	(A) (B) frequency [at a frequency no longer than annually]	
CP	2		CONTINGENCY PLAN	R	S	S	S			This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P3	X	(D) [at a frequency no longer than annually]	
CP	2	(1)	CONTINGENCY PLAN	R	S		S			This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P3	X		
CP	2	(2)	CONTINGENCY PLAN	R	S					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P3	X		
CP	2	(3)	CONTINGENCY PLAN	R	S					Control enhancements (3) and (4) stipulate that a time period for the resumption of essential and all missions and business functions should be provided in the contingency plan.	P3	X	(3) [within 24 hours]	
CP	2	(4)	CONTINGENCY PLAN	R	S					Control enhancements (3) and (4) stipulate that a time period for the resumption of essential and all missions and business functions should be provided in the contingency plan.	P3	X		
CP	2	(5)	CONTINGENCY PLAN	R	S					Control enhancements (5) and (6) ensure that the contingency plan adequately addresses essential missions and business functions.	P3	X		
CP	2	(6)	CONTINGENCY PLAN	R	S					Control enhancements (5) and (6) ensure that the contingency plan adequately addresses essential missions and business functions.	P3	X		

CP	3		CONTINGENCY TRAINING						R	This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P3	X		
CP	3	(1)	CONTINGENCY TRAINING						R	(1) The inclusion of simulated events need not be automated or overly complicated. It basically involves including a scenario in order to increase the realism and effectiveness of the contingency training.	P3	X		
CP	3	(2)	CONTINGENCY TRAINING						R	This security control/enhancement specifies the use of an automated mechanism. While there are obvious benefits to the use of such mechanisms, in most cases the use of manual mechanisms will suffice.	None defined	Not Selected		
CP	4		CONTINGENCY PLAN TESTING AND EXERCISES	R	S						P3	X	(A) frequency [at a frequency no longer than annually]	
CP	4	(1)	CONTINGENCY PLAN TESTING AND EXERCISES	R	S		S			This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. Control enhancement (1) specifies that the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans. It does not specify that all of the related plans be included as part of the contingency plan testing. Consequently, contingency plan testing should ensure the validity of information where it intersects with related plans.	P3	X		

CP	4	(2)	CONTINGENCY PLAN TESTING AND EXERCISES	R	S		S			This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. Control enhancement (2) ensures that personnel are familiar with the alternate processing site and that the site meets the requirements as specified in the contingency plan.	P3	X		
CP	4	(3)	CONTINGENCY PLAN TESTING AND EXERCISES		R	S				This security control/enhancement specifies the use of an automated mechanism. While there are obvious benefits to the use of such mechanisms, in most cases the use of manual mechanisms will suffice.	None defined	Not Selected		
CP	4	(4)	CONTINGENCY PLAN TESTING AND EXERCISES	S	R		S				None defined	Not Selected		
CP	5		CONTINGENCY PLAN UPDATE								None defined	Not Selected		
CP	6		ALTERNATE STORAGE SITE	R	S						P3	X		
CP	6	(1)	ALTERNATE STORAGE SITE	R							P3	X		
CP	6	(2)	ALTERNATE STORAGE SITE		R					Control enhancement (2) ensures that the alternate storage site meets the requirements as specified in the contingency plan.	P3	X		
CP	6	(3)	ALTERNATE STORAGE SITE	R	S						P3	X		
CP	7		ALTERNATE PROCESSING SITE	R	S		S				P3	X	(A) [not to exceed 24 hours]	
CP	7	(1)	ALTERNATE PROCESSING SITE	R							P3	X		
CP	7	(2)	ALTERNATE PROCESSING SITE	R	S						P3	X		
CP	7	(3)	ALTERNATE PROCESSING SITE	R							P3	X		
CP	7	(4)	ALTERNATE PROCESSING SITE		R					Control enhancement (4) ensures that the alternate processing site meets the requirements as specified in the contingency plan.	P3	X		

CP	7	(5)	ALTERNATE PROCESSING SITE	R	S		S				P3	X		
CP	8		TELECOMMUNICATIONS SERVICES	R	S						P3	X	(A) [not to exceed 24 hours]	
CP	8	(1)	TELECOMMUNICATIONS SERVICES	R	S						P3	X		
CP	8	(2)	TELECOMMUNICATIONS SERVICES	R	S						P3	X		
CP	8	(3)	TELECOMMUNICATIONS SERVICES	R	S					Control enhancement (3) ensures that any alternate telecommunications services are sufficiently separated from primary telecommunications services so as not to be susceptible to the same hazard.	P3	X		
CP	8	(4)	TELECOMMUNICATIONS SERVICES	R	S						None defined	Not Selected		
CP	9		INFORMATION SYSTEM BACKUP		R					Incremental daily backups and full weekly backups can be performed.	P1	X	(A) frequency [at a frequency no longer than daily]	
CP	9	(1)	INFORMATION SYSTEM BACKUP		R						P2	X	(1) [at least monthly]	
CP	9	(2)	INFORMATION SYSTEM BACKUP		R						P2	X		
CP	9	(3)	INFORMATION SYSTEM BACKUP		R						P2	X		
CP	9	(4)	INFORMATION SYSTEM BACKUP								None defined	Not Selected		
CP	9	(5)	INFORMATION SYSTEM BACKUP		R						P2	X		
CP	9	(6)	INFORMATION SYSTEM BACKUP		R						None defined	Not Selected		
CP	10		INFORMATION SYSTEM RECOVERY AND RECONSTITUTION		R					Rather than re-building systems from scratch this control enhancement ensures that organizations re-build systems from either a secure image or baseline. This approach will improve the effectiveness of the recovery process.	P3	X		
CP	10	(1)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION								None defined	Not Selected		

CP	10	(2)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION		S	R				This security control/enhancement should be addressed where applicable and if practical to do so.	P3	X		
CP	10	(3)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	R	S	S					None defined	Not Selected		
CP	10	(4)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION		R					This security control/enhancement should be addressed where applicable and if practical to do so. Rather than re-building systems from scratch this control enhancement ensures that organizations re-build systems from a secure image, baseline or virtualized snapshots. This approach will improve the effectiveness of the recovery process.	P3	X		
CP	10	(5)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION		R						None defined	Not Selected		
CP	10	(6)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION		R						P3	X		
IA	1		IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	R					S		P1	X	(A) (B) frequency [at a frequency no longer than annually]	
IA	2		IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	S	R	S				The implementation of this security control/enhancement should be determined based on a Threat and Risk Assessment (TRA). Multifactor authentication can be addresed using a software-based certificate in conjunction with a username and password. Network access is not the same as remote access.	P1	X		

IA	2	(1)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)			R					P1	X		
IA	2	(2)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)			R					None defined	Not Selected		
IA	2	(3)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)			R				This security control/enhancement is considered a compensating control that should be applied if the capability cannot be addressed using an alternate security control/enhancement. All management should be done in a controlled zone. This security control/enhancement could be used to strengthen the audit capability if a TRA has identified an insider threat.	None defined	Not Selected		
IA	2	(4)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)			R					None defined	Not Selected		
IA	2	(5)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	S		R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
IA	2	(6)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)			R					None defined	Not Selected		
IA	2	(7)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)			R					None defined	Not Selected		

IA	2	(8)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	S		R				This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. The vast majority of authentication mechanisms presently available from vendors are replay-resistant. Consequently, an organization should make every effort to use one of these.	P2	X	replay [Authorizer-defined replay mechanisms]	
IA	2	(9)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	S		R				This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
IA	2	(100)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)			R				Depending on robustness requirements, multifactor authentication can be addressed using a software-based certificate in conjunction with a username and password or hardware cryptographic tokens. For additional guidance please refer to ITSG-31 User Authentication Guidance for IT Systems.	P2	X		
IA	3		DEVICE IDENTIFICATION AND AUTHENTICATION	S		R				This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
IA	3	(1)	DEVICE IDENTIFICATION AND AUTHENTICATION			R				This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
IA	3	(2)	DEVICE IDENTIFICATION AND AUTHENTICATION			R					None defined	Not Selected		

IA	3	(3)	DEVICE IDENTIFICATION AND AUTHENTICATION		R					This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
IA	4		IDENTIFIER MANAGEMENT	S	R	S					P1	X		
IA	4	(1)	IDENTIFIER MANAGEMENT	R							P2	X		
IA	4	(2)	IDENTIFIER MANAGEMENT	R						This could have been accomplished previously as part of the security or indoctrination process. For privileged accounts this is highly recommended.	P2	X		
IA	4	(3)	IDENTIFIER MANAGEMENT	R						This could have been accomplished previously as part of the security or indoctrination process. The organization either requires multiple forms of certification of individual identification or requires a single form of certification of individual identification (e.g., employee ID) that represents multiple forms.	P2	X		
IA	4	(4)	IDENTIFIER MANAGEMENT	S	R	S					P2	X		
IA	4	(5)	IDENTIFIER MANAGEMENT			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
IA	5		AUTHENTICATOR MANAGEMENT	S	R	S					P1	X	(G) [not to exceed 180 days]	
IA	5	(1)	AUTHENTICATOR MANAGEMENT	S		R					P1	X	(1) [case sensitive, 8 character, at least one upper case, lower case, number, and special character]	

IA	5	(2)	AUTHENTICATOR MANAGEMENT			R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
IA	5	(3)	AUTHENTICATOR MANAGEMENT	R							P2	X	(3) [user ID and password]	
IA	5	(4)	AUTHENTICATOR MANAGEMENT	S	R	S					None defined	Not Selected		
IA	5	(5)	AUTHENTICATOR MANAGEMENT	R							None defined	Not Selected		
IA	5	(6)	AUTHENTICATOR MANAGEMENT		R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
IA	5	(7)	AUTHENTICATOR MANAGEMENT		S	R					P2	X		
IA	5	(8)	AUTHENTICATOR MANAGEMENT	S	R						P2	X		
IA	6		AUTHENTICATOR FEEDBACK			R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
IA	7		CRYPTOGRAPHIC MODULE AUTHENTICATION			R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. For additional guidance please refer to ITSG-31 User Authentication Guidance for IT Systems.	P2	X		
IA	8		IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)			R					P2	X		
IR	1		INCIDENT RESPONSE POLICY AND PROCEDURES	R	S				S		P1	X	(A) (B) frequency [at a frequency no longer than annually]	

IR	2		INCIDENT RESPONSE TRAINING						R		P2	X	(B) frequency [at a frequency no longer than annually]	
IR	2	(1)	INCIDENT RESPONSE TRAINING						R		P2	X		
IR	2	(2)	INCIDENT RESPONSE TRAINING						R		None defined	Not Selected		
IR	3		INCIDENT RESPONSE TESTING AND EXERCISES	R					S		P3	X	(A) frequency [at a frequency no longer than annually]	
IR	3	(1)	INCIDENT RESPONSE TESTING AND EXERCISES						R		None defined	Not Selected		
IR	4		INCIDENT HANDLING	R	S						P2	X		
IR	4	(1)	INCIDENT HANDLING	S	R	S				This security control/enhancement specifies the use of an automated mechanism. While there are obvious benefits to the use of such mechanisms, in most cases the use of manual mechanisms will suffice.	None defined	Not Selected		
IR	4	(2)	INCIDENT HANDLING		R	S					None defined	Not Selected		
IR	4	(3)	INCIDENT HANDLING	R	S						P2	X		
IR	4	(4)	INCIDENT HANDLING	R	S					Control enhancement (4) ensures that incident information and individual incident responses are stored centrally in order that they can be leveraged by the entire organization. This control enhancement can be implemented as simply as using a shared network folder for the storage of incident response information.	P2	X		
IR	4	(5)	INCIDENT HANDLING	S	R	S					None defined	Not Selected		
IR	5		INCIDENT MONITORING	R							P2	X		

IR	5	(1)	INCIDENT MONITORING	S	R	S					None defined	Not Selected		
IR	6		INCIDENT REPORTING	R	S						P2	X		
IR	6	(1)	INCIDENT REPORTING	S	R	S					None defined	Not Selected		
IR	6	(2)	INCIDENT REPORTING	R							P3	X		
IR	7		INCIDENT RESPONSE ASSISTANCE	R							P3	X		
IR	7	(1)	INCIDENT RESPONSE ASSISTANCE	S	R	S					None defined	Not Selected		
IR	7	(2)	INCIDENT RESPONSE ASSISTANCE	R							None defined	Not Selected		
IR	8		INCIDENT RESPONSE PLAN	R							P3	X	(C) frequency [at a frequency no longer than annually]	
MA	1		SYSTEM MAINTENANCE POLICY AND PROCEDURES	R	S				S		P1	X	(A) (B) frequency [at a frequency no longer than annually]	
MA	2		CONTROLLED MAINTENANCE		R						P3	X		
MA	2	(1)	CONTROLLED MAINTENANCE		R						P3	X		
MA	2	(2)	CONTROLLED MAINTENANCE		R	S					None defined	Not Selected		
MA	3		MAINTENANCE TOOLS		R						P3	X		
MA	3	(1)	MAINTENANCE TOOLS		R						P3	X		
MA	3	(2)	MAINTENANCE TOOLS		R						P3	X		
MA	3	(3)	MAINTENANCE TOOLS		R						P1	X		
MA	3	(4)	MAINTENANCE TOOLS		R	S					None defined	Not Selected		
MA	4		NON-LOCAL MAINTENANCE		R						P3	X		

MA	4	(1)	NON-LOCAL MAINTENANCE	S	R						P3	X		
MA	4	(2)	NON-LOCAL MAINTENANCE	S	S	R					P3	X		
MA	4	(3)	NON-LOCAL MAINTENANCE		R						P3	X		
MA	4	(4)	NON-LOCAL MAINTENANCE		R						P3	X		
MA	4	(5)	NON-LOCAL MAINTENANCE	S	R						P3	X		
MA	4	(6)	NON-LOCAL MAINTENANCE		R						P3	X		
MA	4	(7)	NON-LOCAL MAINTENANCE		R	S					None defined	Not Selected		
MA	5		MAINTENANCE PERSONNEL		R						P2	X		
MA	5	(1)	MAINTENANCE PERSONNEL		R						P2	X		
MA	5	(2)	MAINTENANCE PERSONNEL	S	R			S			P1	X		
MA	5	(3)	MAINTENANCE PERSONNEL	S	R			S			None defined	Not Selected		
MA	5	(4)	MAINTENANCE PERSONNEL	S	R			S			None defined	Not Selected		
MA	6		TIMELY MAINTENANCE		R						P3	X		
MP	1		MEDIA PROTECTION POLICY AND PROCEDURES	R					S		P1	X	(A) (B) frequency [at a frequency no longer than annually]	
MP	2		MEDIA ACCESS	R	S						P1	X		
MP	2	(1)	MEDIA ACCESS		R						P2	X		
MP	2	(2)	MEDIA ACCESS		R	S					P2	X		
MP	3		MEDIA MARKING	R	S				S		P1	X		
MP	4		MEDIA STORAGE		R						P1	X		

MP	4	(1)	MEDIA STORAGE		R	S					P2	X		Secret information stored on portable digital media must be encrypted using CSEC-approved solutions.
MP	5		MEDIA TRANSPORT	R	S		S				P1	X		
MP	5	(1)	MEDIA TRANSPORT								None defined	Not Selected		
MP	5	(2)	MEDIA TRANSPORT		R						P2	X		
MP	5	(3)	MEDIA TRANSPORT		R						P1	X		
MP	5	(4)	MEDIA TRANSPORT		R	S					P2	X		
MP	6		MEDIA SANITIZATION		R						P2	X		
MP	6	(1)	MEDIA SANITIZATION		R						P2	X		
MP	6	(2)	MEDIA SANITIZATION		R						P2	X	(2) frequency [at a frequency no longer than annually]	
MP	6	(3)	MEDIA SANITIZATION		R						P2	X		
MP	6	(4)	MEDIA SANITIZATION		R						P2	X		
MP	6	(5)	MEDIA SANITIZATION		R						P2	X		
MP	6	(6)	MEDIA SANITIZATION		R						P2	X		
PE	1		PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	R			S		S		P1	X	(A) (B) frequency [at a frequency no longer than annually]	
PE	2		PHYSICAL ACCESS AUTHORIZATIONS	S			R	S		The reviews can be performed simultaneously with account reviews (see AC-2).	P1	X	(C) frequency [monthly]	
PE	2	(1)	PHYSICAL ACCESS AUTHORIZATIONS	R			S				P2	X		

PE	2	(2)	PHYSICAL ACCESS AUTHORIZATIONS		S		R				None defined	Not Selected		
PE	2	(3)	PHYSICAL ACCESS AUTHORIZATIONS	R			S	S			P1	X		
PE	2	(100)	PHYSICAL ACCESS AUTHORIZATIONS	R			S	S			P1	X		
PE	3		PHYSICAL ACCESS CONTROL				R				P1	X	(F) Inventories of physical devices [annually] (G) Changes combinations and keys [only when keys are lost, combinations are compromised or individuals are transferred or terminated]	According the TBS Operational Standard on Physical Security, a physical Security Zone is required where secret information is processed or stored. This zone is an area to which access is limited to authorized personnel and to authorized and properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored continuously, i.e., 24 hours a day and 7 days a week.
PE	3	(1)	PHYSICAL ACCESS CONTROL				R				P2	X		
PE	3	(2)	PHYSICAL ACCESS CONTROL				R				P2	X		
PE	3	(3)	PHYSICAL ACCESS CONTROL				R				P2	X		
PE	3	(4)	PHYSICAL ACCESS CONTROL				R				P2	X	(4) [tbd, e.g. lockable data centre racks]	
PE	3	(5)	PHYSICAL ACCESS CONTROL				R				None defined	Not Selected		
PE	3	(6)	PHYSICAL ACCESS CONTROL				R				P3	Not Selected		
PE	4		ACCESS CONTROL FOR TRANSMISSION MEDIUM				R				P1	X		

PE	5		ACCESS CONTROL FOR OUTPUT DEVICES				R				P2	X		
PE	6		MONITORING PHYSICAL ACCESS		S		R				P1	X	(B) frequency [at a frequency no longer than monthly]	
PE	6	(1)	MONITORING PHYSICAL ACCESS				R				P2	X		
PE	6	(2)	MONITORING PHYSICAL ACCESS				R				P1	X		
PE	7		VISITOR CONTROL				R				P1	X		
PE	7	(1)	VISITOR CONTROL				R				P2	X		
PE	7	(2)	VISITOR CONTROL				R				None defined	Not Selected		
PE	8		ACCESS RECORDS				R				P1	X	(B) frequency [at least monthly]	
PE	8	(1)	ACCESS RECORDS			S	R			This security control/enhancement specifies the use of an automated mechanism. While there are obvious benefits to the use of such mechanisms, in most cases the use of manual mechanisms will suffice.	P2	Not Selected		
PE	8	(2)	ACCESS RECORDS				R				P2	X		
PE	9		POWER EQUIPMENT AND POWER CABLING			S	R				P3	X		
PE	9	(1)	POWER EQUIPMENT AND POWER CABLING			S	R				None defined	Not Selected		
PE	9	(2)	POWER EQUIPMENT AND POWER CABLING			S	R				None defined	Not Selected		
PE	10		EMERGENCY SHUTOFF			S	R				P3	X		
PE	10	(1)	EMERGENCY SHUTOFF								None defined	Not Selected		
PE	11		EMERGENCY POWER			S	R				P3	X		

PE	11	(1)	EMERGENCY POWER			S	R				None defined	Not Selected		
PE	11	(2)	EMERGENCY POWER			S	R				None defined	Not Selected		
PE	12		EMERGENCY LIGHTING			S	R				P2	X		
PE	12	(1)	EMERGENCY LIGHTING			S	R				P2	X		
PE	13		FIRE PROTECTION			S	R				P2	X		
PE	13	(1)	FIRE PROTECTION			S	R				P2	X		
PE	13	(2)	FIRE PROTECTION			S	R				P2	X		
PE	13	(3)	FIRE PROTECTION			S	R				P2	X		
PE	13	(4)	FIRE PROTECTION				R				P2	X		
PE	14		TEMPERATURE AND HUMIDITY CONTROLS				R				P3	X		
PE	14	(1)	TEMPERATURE AND HUMIDITY CONTROLS			S	R				P3	X		
PE	14	(2)	TEMPERATURE AND HUMIDITY CONTROLS			S	R				P3	X		
PE	15		WATER DAMAGE PROTECTION			S	R				P3	X		
PE	15	(1)	WATER DAMAGE PROTECTION			S	R				None defined	Not Selected		
PE	16		DELIVERY AND REMOVAL				R				P1	X		
PE	17		ALTERNATE WORK SITE				R				P3	X	(A) [Authorizer defined controls]	
PE	18		LOCATION OF INFORMATION SYSTEM COMPONENTS	S			R				P1	X		
PE	18	(1)	LOCATION OF INFORMATION SYSTEM COMPONENTS	S		S	R				P1	X		

PE	19		INFORMATION LEAKAGE			S	R				P2	X		
PE	19	(1)	INFORMATION LEAKAGE			S	R				P2	X		
PL	1		SECURITY PLANNING POLICY AND PROCEDURES	R					S		P1	X	(A) (B) frequency [at a frequency no longer than annually]	
PL	2		SYSTEM SECURITY PLAN	S		R				By completing the ISSIP activities, IT projects will produce the information elements that are normally found in a system security plan. Although ISSIP promotes the minimization of standalone security documentation through the integration of ISSIP outputs into standard project deliverables, it does not proscribe the use of system security plans. Where departments have established the requirement for system security plans in their departmental security control profile or domain security control profiles, IT projects can easily prepare one for their information system by assembling the prescribed information elements from the various ISSIP activities.	P1	X	(B) frequency [at a frequency no longer than annually, or whenever a significant system change occurs]	
PL	2	(1)	SYSTEM SECURITY PLAN	S		R					P2	X		
PL	2	(2)	SYSTEM SECURITY PLAN	S		R					P2	X		
PL	3		SYSTEM SECURITY PLAN UPDATE								None defined	Not Selected		
PL	4		RULES OF BEHAVIOUR	R				S	S		P1	X		
PL	4	(1)	RULES OF BEHAVIOUR	R					S		P2	X		
PL	5		PRIVACY IMPACT ASSESSMENT	R		S					P1	X		
PL	6		SECURITY-RELATED ACTIVITY PLANNING	R	S	S					P2	X		
PS	1		PERSONNEL SECURITY POLICY AND PROCEDURES	S				R	S		P1	X	(A) (B) frequency [at least annually]	

PS	2		POSITION CATEGORIZATION	S				R			P2	X		
PS	3		PERSONNEL SCREENING	S				R			P1	X		According to the TBS Personnel Security Standard, personnel must be screened to Level 2 security clearance when the duties or tasks of a position or contract necessitate access to classified (Secret) information and assets. An individual granted a security clearance may access, on a need-to-know basis, classified information and assets up to and including the level of security clearance granted.
PS	3	(1)	PERSONNEL SCREENING	S	S			R			P1	X		
PS	3	(2)	PERSONNEL SCREENING	S	S			R			P1	X		
PS	4		PERSONNEL TERMINATION		S			R			P1	X		
PS	5		PERSONNEL TRANSFER	S				R			P1	X		
PS	6		ACCESS AGREEMENTS		S			R			P1	X		
PS	6	(1)	ACCESS AGREEMENTS	R	S			S			P2	X		
PS	6	(2)	ACCESS AGREEMENTS	R	S			S			P1	X		
PS	7		THIRD-PARTY PERSONNEL SECURITY					R			P1	X		
PS	8		PERSONNEL SANCTIONS					R			P2	X		

RA	1		RISK ASSESSMENT POLICY AND PROCEDURES	R	S				S		P1	X	(A) (B) frequency [at a frequency no longer than annually]	
RA	2		SECURITY CATEGORIZATION	R							P1	X		
RA	3		RISK ASSESSMENT	R							P1	X	(C) frequency [at a frequency no longer than annually]	
RA	4		RISK ASSESSMENT UPDATE								None defined	Not Selected		
RA	5		VULNERABILITY SCANNING		R	S					P2	X	(A) frequency [at least every 30 days] (D) response time [within 1 week]	
RA	5	(1)	VULNERABILITY SCANNING		R	S					P2	X		
RA	5	(2)	VULNERABILITY SCANNING		R	S					P2	X	(2) frequency [immediately prior to each vulnerability scan]	
RA	5	(3)	VULNERABILITY SCANNING		R	S					P2	X		
RA	5	(4)	VULNERABILITY SCANNING		R	S					None defined	Not Selected		
RA	5	(5)	VULNERABILITY SCANNING		R	S					None defined	Not Selected		
RA	5	(6)	VULNERABILITY SCANNING		R	S					None defined	Not Selected		
RA	5	(7)	VULNERABILITY SCANNING		R	S					None defined	Not Selected		
RA	5	(8)	VULNERABILITY SCANNING		R						None defined	Not Selected		
RA	5	(9)	VULNERABILITY SCANNING		R	S					P2	X		
SA	1		SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	R					S		P1	X	(A) (B) frequency [at a frequency no longer than annually]	

SA	2		ALLOCATION OF RESOURCES			R					P3	X		
SA	3		LIFE CYCLE SUPPORT	S		R					P3	X		
SA	4		ACQUISITIONS	S		R					P3	X		
SA	4	(1)	ACQUISITIONS	S		R					P3	X		
SA	4	(2)	ACQUISITIONS	S		R					P1	X		
SA	4	(3)	ACQUISITIONS	S		R					None defined	Not Selected		
SA	4	(4)	ACQUISITIONS	S	R	S					None defined	Not Selected		
SA	4	(5)	ACQUISITIONS	S		R				In the context of ITSG-33 Annex 4 profiles, secure refers to the practice of disabling extraneous services, ports and accounts where possible. The intent behind this security enhancement is that organizations can deploy information system components in a secure manner with relatively little additional effort. The concern is that if information system components are not delivered in a secure, documented configuration then additional burden will fall on the organization deploying the components.	P3	X		
SA	4	(6)	ACQUISITIONS	S		R					P1	X		
SA	4	(7)	ACQUISITIONS	S		R					P1	X		
SA	5		INFORMATION SYSTEM DOCUMENTATION	S	S	R					P3	X		
SA	5	(1)	INFORMATION SYSTEM DOCUMENTATION	S	S	R					P3	X		
SA	5	(2)	INFORMATION SYSTEM DOCUMENTATION	S	S	R					P3	X		
SA	5	(3)	INFORMATION SYSTEM DOCUMENTATION	S	S	R					P3	X		

SA	5	(4)	INFORMATION SYSTEM DOCUMENTATION	S	S	R					None defined	Not Selected		
SA	5	(5)	INFORMATION SYSTEM DOCUMENTATION	S	S	R					None defined	Not Selected		
SA	6		SOFTWARE USAGE RESTRICTIONS	R	S						P3	X		
SA	6	(1)	SOFTWARE USAGE RESTRICTIONS	R	S	S					None defined	Not Selected		
SA	7		USER-INSTALLED SOFTWARE	S	R						P1	X		
SA	8		SECURITY ENGINEERING PRINCIPLES	S	S	R					P3	X		
SA	8	(100)	SECURITY ENGINEERING PRINCIPLES	S		R					None defined	Not Selected		
SA	9		EXTERNAL INFORMATION SYSTEM SERVICES	R							P1	X		
SA	9	(1)	EXTERNAL INFORMATION SYSTEM SERVICES	R							P2	X		
SA	10		DEVELOPER CONFIGURATION MANAGEMENT	S		R					P3	X		
SA	10	(1)	DEVELOPER CONFIGURATION MANAGEMENT	S		R					P3	X		
SA	10	(2)	DEVELOPER CONFIGURATION MANAGEMENT	S		R					P3	X		
SA	11		DEVELOPER SECURITY TESTING	S		R					P3	X		
SA	11	(1)	DEVELOPER SECURITY TESTING	S		R					P2	X		
SA	11	(2)	DEVELOPER SECURITY TESTING	S		R					P3	X		
SA	11	(3)	DEVELOPER SECURITY TESTING	S		R					None defined	Not Selected		
SA	12		SUPPLY CHAIN PROTECTION	R	S	S					P3	X		

SA	12	(1)	SUPPLY CHAIN PROTECTION	S		R					None defined	Not Selected		
SA	12	(2)	SUPPLY CHAIN PROTECTION	S		R					P3	X		
SA	12	(3)	SUPPLY CHAIN PROTECTION	S		R					None defined	Not Selected		
SA	12	(4)	SUPPLY CHAIN PROTECTION	S		R					None defined	Not Selected		
SA	12	(5)	SUPPLY CHAIN PROTECTION	S	S	R					None defined	Not Selected		
SA	12	(6)	SUPPLY CHAIN PROTECTION	S		R					None defined	Not Selected		
SA	12	(7)	SUPPLY CHAIN PROTECTION	S		R					None defined	Not Selected		
SA	13		TRUSTWORTHINESS	S		R					None defined	Not Selected		
SA	14		CRITICAL INFORMATION SYSTEM COMPONENTS	S		R					None defined	Not Selected		
SA	14	(1)	CRITICAL INFORMATION SYSTEM COMPONENTS	S		R					None defined	Not Selected		
SC	1		SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	R					S	This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X	(A) (B) frequency [at a frequency no longer than annually]	
SC	2		APPLICATION PARTITIONING			R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
SC	2	(1)	APPLICATION PARTITIONING			R					P2	X		

SC	3		SECURITY FUNCTION ISOLATION			R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. However, this security control/enhancement cannot be met using readily available COTS components. Consequently, compliance with this security control/enhancement may be problematic. Note that this security control/enhancement applies at the platform level.	None defined	Not Selected		
SC	3	(1)	SECURITY FUNCTION ISOLATION			R					None defined	Not Selected		
SC	3	(2)	SECURITY FUNCTION ISOLATION			R					None defined	Not Selected		
SC	3	(3)	SECURITY FUNCTION ISOLATION			R					None defined	Not Selected		
SC	3	(4)	SECURITY FUNCTION ISOLATION			R					None defined	Not Selected		
SC	3	(5)	SECURITY FUNCTION ISOLATION			R					None defined	Not Selected		
SC	4		INFORMATION IN SHARED RESOURCES			R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. However, this security control/enhancement cannot be met using readily available COTS components. Consequently, implementation of this security control/enhancement may be problematic.	None defined	Not Selected		
SC	4	(1)	INFORMATION IN SHARED RESOURCES			R					None defined	Not Selected		

SC	5		DENIAL OF SERVICE PROTECTION			R					P1	X	(A) list [Organizationally defined list]	
SC	5	(1)	DENIAL OF SERVICE PROTECTION			R					None defined	Not Selected		
SC	5	(2)	DENIAL OF SERVICE PROTECTION			R					P2	X		
SC	6		RESOURCE PRIORITY			R				This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	None defined	Not Selected		
SC	7		BOUNDARY PROTECTION		R	S				A Web Content Filtering proxy is a common device to monitor and control web traffic. Network-based intrusion detection or prevention system is another common device to monitor and control network traffic.	P1	X		
SC	7	(1)	BOUNDARY PROTECTION	S	R	S					P1	X		
SC	7	(2)	BOUNDARY PROTECTION			R					P1	X		
SC	7	(3)	BOUNDARY PROTECTION	S	R	S					P1	X		
SC	7	(4)	BOUNDARY PROTECTION	S	R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X	(4)(e) frequency [at a frequency no longer than annually]	
SC	7	(5)	BOUNDARY PROTECTION			R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
SC	7	(6)	BOUNDARY PROTECTION		S	R					P2	X		
SC	7	(7)	BOUNDARY PROTECTION			R					P2	X		

SC	7	(8)	BOUNDARY PROTECTION	S		R					P2	X	(8) list [list of communications traffic] (8) list [list of external networks]	
SC	7	(9)	BOUNDARY PROTECTION		S	R					P1	X		
SC	7	(10)	BOUNDARY PROTECTION		R	S					P2	X		
SC	7	(11)	BOUNDARY PROTECTION			R				This security control/enhancement should be addressed where applicable and if practical to do so.	P2	X		
SC	7	(12)	BOUNDARY PROTECTION			R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
SC	7	(13)	BOUNDARY PROTECTION	S		R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. This security control/enhancement can be met through the use of a dedicated management zone.	P2	X		
SC	7	(14)	BOUNDARY PROTECTION		R	S	S				P1	X		
SC	7	(15)	BOUNDARY PROTECTION			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
SC	7	(16)	BOUNDARY PROTECTION			R					None defined	Not Selected		
SC	7	(17)	BOUNDARY PROTECTION			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		

SC	7	(18)	BOUNDARY PROTECTION			R				Control enhancement (18) basically says the same thing as control enhancement (6).	P2	X		
SC	8		TRANSMISSION INTEGRITY			R				TLS encryption between email servers is a example implementation of this control applied for emails exchange.	P1	X		
SC	8	(1)	TRANSMISSION INTEGRITY			R	S			This security control/enhancement should be addressed where applicable and if practical to do so.	P2	X		
SC	8	(2)	TRANSMISSION INTEGRITY			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
SC	9		TRANSMISSION CONFIDENTIALITY			R				TLS encryption between email servers is a example implementation of this control applied for emails exchange.	P1	X		
SC	9	(1)	TRANSMISSION CONFIDENTIALITY	S	S	R					P2	X	(1) list [alternative physical measures]	For internal departmental networks, Secret data does not need to be encrypted, unless warranted by a TRA. Secret data must be encrypted using the appropriate Type 1 encryption during transmission over a public (e.g. Internet) or otherwise unsecured network.
SC	9	(2)	TRANSMISSION CONFIDENTIALITY			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
SC	9	(100)	TRANSMISSION CONFIDENTIALITY	S	S	R					None defined	Not Selected		

SC	10		NETWORK DISCONNECT			R				This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. The security control/enhancement refers to user sessions such as Web sessions or client VPN sessions. Firewalls will automatically drop TCP/IP sessions after a certain period of inactivity.	P3	X		
SC	11		TRUSTED PATH	S		R				This security control/enhancement applies to the platform.	None defined	Not Selected		
SC	12		CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT		R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P3	X		
SC	12	(1)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT		R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P3	X		
SC	12	(2)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT		R	S					P1	X		
SC	12	(3)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT		R	S					P1	X		
SC	12	(4)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT		R	S					P1	X		
SC	12	(5)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT		R	S					P1	X		
SC	13		USE OF CRYPTOGRAPHY			R					P3	X		
SC	13	(1)	USE OF CRYPTOGRAPHY	S	S	R					None defined	Not Selected		

SC	13	(2)	USE OF CRYPTOGRAPHY	S	S	R					P1	X		
SC	13	(3)	USE OF CRYPTOGRAPHY	S	S	R				This security control/enhancement is considered a compensating control that should be applied if the capability cannot be addressed using an alternate security control/enhancement. Specifically, if access control is not going to be used for this purpose then cryptography could be used. In this situation, the use of CMVP-validated cryptography is recommended.	None defined	Not Selected		
SC	13	(4)	USE OF CRYPTOGRAPHY	S	S	R					P3	X	[CMVP-validated]	
SC	13	(100)	USE OF CRYPTOGRAPHY	S	S	R					None defined	Not Selected		
SC	13	(101)	USE OF CRYPTOGRAPHY	S	S	R					None defined	Not Selected		
SC	13	(102)	USE OF CRYPTOGRAPHY	S	S	R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
SC	13	(103)	USE OF CRYPTOGRAPHY	S	S	R					None defined	Not Selected		
SC	13	(104)	USE OF CRYPTOGRAPHY	S	S	R					P1	X		
SC	14		PUBLIC ACCESS PROTECTIONS			R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
SC	15		COLLABORATIVE COMPUTING DEVICES	S		R					P3	X	(A) [no exceptions]	
SC	15	(1)	COLLABORATIVE COMPUTING DEVICES			R					None defined	Not Selected		
SC	15	(2)	COLLABORATIVE COMPUTING DEVICES			R				This security control/enhancement should include consideration for other social networking applications such as Facebook and Twitter.	P3	X		

SC	15	(3)	COLLABORATIVE COMPUTING DEVICES	R	S	S					P3	X		
SC	16		TRANSMISSION OF SECURITY ATTRIBUTES			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
SC	16	(1)	TRANSMISSION OF SECURITY ATTRIBUTES			R					None defined	Not Selected		
SC	17		PUBLIC KEY INFRASTRUCTURE CERTIFICATES	S	R	S				This security control ensures that public key certificates are issued from an appropriate GC Certification Authority.	P3	X		
SC	18		MOBILE CODE	R	S	S					P1	X		
SC	18	(1)	MOBILE CODE			R					P2	X		
SC	18	(2)	MOBILE CODE	S		R					P2	X	(2) list [Mobile code requirements]	
SC	18	(3)	MOBILE CODE			R					P2	X		
SC	18	(4)	MOBILE CODE	S		R					P2	X	(4) list [software applications] (4) list [actions]	
SC	19		VOICE OVER INTERNET PROTOCOL	R	S	S					P1	X		
SC	19	(100)	VOICE OVER INTERNET PROTOCOL		R	S					None defined	Not Selected		
SC	19	(101)	VOICE OVER INTERNET PROTOCOL		R	S					None defined	Not Selected		

SC	20		SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis. This security control/enhancement cannot be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, implementation of this security control/enhancement may be somewhat problematic.	None defined	Not Selected		
SC	20	(1)	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)			R					None defined	Not Selected		
SC	21		SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)			R					None defined	Not Selected		
SC	21	(1)	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)			R					None defined	Not Selected		
SC	22		ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE			R					P3	X		
SC	23		SESSION AUTHENTICITY			R					P1	X		

SC	23	(1)	SESSION AUTHENTICITY			R				This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
SC	23	(2)	SESSION AUTHENTICITY			R				This security control/enhancement can be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X		
SC	23	(3)	SESSION AUTHENTICITY			R					P2	X		
SC	23	(4)	SESSION AUTHENTICITY			R					P2	X		
SC	24		FAIL IN KNOWN STATE			R				This security control/enhancement is appropriate for organizationally defined systems (e.g., firewalls).	P1	X		
SC	25		THIN NODES			R					None defined	Not Selected		
SC	26		HONEYPOTS			R					None defined	Not Selected		
SC	26	(1)	HONEYPOTS			R					None defined	Not Selected		
SC	27		OPERATING SYSTEM-INDEPENDENT APPLICATIONS			R					None defined	Not Selected		
SC	28		PROTECTION OF INFORMATION AT REST			R					P1	X		
SC	28	(1)	PROTECTION OF INFORMATION AT REST		R	S	S				None defined	Not Selected		

SC	29		HETEROGENEITY	S	S	R				In this context employing diverse information technologies refers specifically to the practice of deploying security safeguards from different vendors at various locations. The intent of this security control is to ensure that an attack which exploits a security flaw in one product will be mitigated by a second product from a different vendor. The principle being that products from different vendors are unlikely to be susceptible to the same flaw. For example, firewalls from different vendors should be used in adjacent network zones. Or, virus scanners from different vendors should be used on servers (e.g., mail server) and on desktops.	P2	X		
SC	30		VIRTUALIZATION TECHNIQUES		S	R					None defined	Not Selected		
SC	30	(1)	VIRTUALIZATION TECHNIQUES		S	R					None defined	Not Selected		
SC	30	(2)	VIRTUALIZATION TECHNIQUES		S	R					None defined	Not Selected		
SC	31		COVERT CHANNEL ANALYSIS	S	S	R					None defined	Not Selected		
SC	31	(1)	COVERT CHANNEL ANALYSIS	S	S	R					None defined	Not Selected		
SC	32		INFORMATION SYSTEM PARTITIONING	S	S	R					None defined	Not Selected		
SC	33		TRANSMISSION PREPARATION INTEGRITY			R					None defined	Not Selected		
SC	34		NON-MODIFIABLE EXECUTABLE PROGRAMS	S		R					None defined	Not Selected		
SC	34	(1)	NON-MODIFIABLE EXECUTABLE PROGRAMS		S	R					None defined	Not Selected		
SC	34	(2)	NON-MODIFIABLE EXECUTABLE PROGRAMS		S	R					None defined	Not Selected		

SC	100		SOURCE AUTHENTICATION			R				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
SC	100	(1)	SOURCE AUTHENTICATION			R					None defined	Not Selected		
SC	100	(2)	SOURCE AUTHENTICATION			R					None defined	Not Selected		
SC	100	(3)	SOURCE AUTHENTICATION			R					None defined	Not Selected		
SC	101		UNCLASSIFIED TELECOMMUNICATIONS SYSTEMS IN SECURE FACILITIES	R	S	S				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all environments. Consequently, inclusion in a departmental profile is made on a case by case basis.	P1	X		This control should be included in any Secret profile.
SI	1		SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	R					S	This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X	(A) (B) frequency [at a frequency no longer than annually]	
SI	2		FLAW REMEDIATION		R					This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X		
SI	2	(1)	FLAW REMEDIATION		R						None defined	Not Selected		
SI	2	(2)	FLAW REMEDIATION		R	S					None defined	Not Selected		
SI	2	(3)	FLAW REMEDIATION	S	R						None defined	Not Selected		
SI	2	(4)	FLAW REMEDIATION		R	S				This security control/enhancement specifies the use of an automated mechanism. While there are obvious benefits to the use of such mechanisms, in most cases the use of manual mechanisms will suffice.	None defined	Not Selected		

SI	3		MALICIOUS CODE PROTECTION		R	S					P1	X	(C) (a) frequency [at least every 30 days] (C) (b) selection [quarantine malicious code]	
SI	3	(1)	MALICIOUS CODE PROTECTION		R	S				Control enhancements (1) and (2) ensure that malicious code mechanisms are centrally managed and that they are automatically updated so as to be effective.	P2	X		
SI	3	(2)	MALICIOUS CODE PROTECTION		R	S				Control enhancements (1) and (2) ensure that malicious code mechanisms are centrally managed and that they are automatically updated so as to be effective.	P2	X		
SI	3	(3)	MALICIOUS CODE PROTECTION		R	S				Control enhancement (3) ensures that malicious code mechanisms cannot be circumvented by non-privileged users. These control enhancements ensure that malicious code protection is implemented effectively.	P2	X		
SI	3	(4)	MALICIOUS CODE PROTECTION		R	S				Updates to an information system that could detrimentally impact the security posture should be tested. This is especially true for mission critical systems.	P2	X		

SI	3	(5)	MALICIOUS CODE PROTECTION	R	S	S				This security enhancement prohibits the use of unapproved removable media on organization information systems. Specifically, it is intended to prevent users from introducing personal removable media into the information system as personal removable media may contain malicious code. It is also intended to prevent users from taking organization removable media home due to the threat of infecting the removable media. While this security enhancement can be addressed through the development of a removable media usage policy, this could be supplemented, where possible, with technical controls to prevent personal removable media from being introduced into organizational information systems.	P2	X		
SI	3	(6)	MALICIOUS CODE PROTECTION	S	R	S					P2	X		
SI	4		INFORMATION SYSTEM MONITORING	R	S	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P1	X	(A) list [Authorizer defined list of objectives]	
SI	4	(1)	INFORMATION SYSTEM MONITORING	S	R	S				This security control/enhancement cannot be met using readily available Commercial-Off-The-Shelf (COTS) components. Consequently, implementation of this security control/enhancement may be somewhat problematic.	None defined	Not Selected		
SI	4	(2)	INFORMATION SYSTEM MONITORING	S	R	S					P2	X		
SI	4	(3)	INFORMATION SYSTEM MONITORING	S	R	S					None defined	Not Selected		
SI	4	(4)	INFORMATION SYSTEM MONITORING		R	S				Control enhancement (4) ensures that the primary location for monitoring is at the ingress and egress to the organization.	P2	X		

SI	4	(5)	INFORMATION SYSTEM MONITORING		R	S				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases.	P2	X	indicators [Authorizer defined list of compromise indicators]	
SI	4	(6)	INFORMATION SYSTEM MONITORING		R	S					P2	X		
SI	4	(7)	INFORMATION SYSTEM MONITORING	S	R	S				Control enhancements (7) and (12) expand on control enhancement (2).	P2	X	(7) list [list of roles], list [list of termination actions]	
SI	4	(8)	INFORMATION SYSTEM MONITORING		R	S					P2	X		
SI	4	(9)	INFORMATION SYSTEM MONITORING	S	R						P3	X	(9) frequency [at least monthly]	
SI	4	(10)	INFORMATION SYSTEM MONITORING	S	S	R				Control enhancement (10) requires that the organization ensures that traffic be decrypted at appropriate locations in the network to satisfy the monitoring requirement. For example, a border gateway may decrypt https session for malicious content verification. Emails may be decrypted at the end-user host and scanned for malicious content locally.	P2	X		
SI	4	(11)	INFORMATION SYSTEM MONITORING	S	R	S				Control enhancement (11) expands upon control enhancement (4).	P2	X		
SI	4	(12)	INFORMATION SYSTEM MONITORING	S	R	S				Control enhancements (7) and (12) expand on control enhancement (2).	P2	X	(12) list [list of inappropriate or unusual activities that trigger alerts]	
SI	4	(13)	INFORMATION SYSTEM MONITORING	S	R	S					P2	X		
SI	4	(14)	INFORMATION SYSTEM MONITORING	S	R	S					P2	X		
SI	4	(15)	INFORMATION SYSTEM MONITORING	S	R	S					P2	X		

SI	4	(16)	INFORMATION SYSTEM MONITORING	S	R	S				This security control/enhancement specifies a very specialized and/or advanced capability that is not required for all systems. Consequently, inclusion in a departmental profile is made on a case by case basis.	None defined	Not Selected		
SI	4	(17)	INFORMATION SYSTEM MONITORING	R	S	S	S				None defined	Not Selected		
SI	5		SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	R	S						P1	X	(C) list [list of roles]	
SI	5	(1)	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	S	R	S					None defined	Not Selected		
SI	6		SECURITY FUNCTIONALITY VERIFICATION	S	R	S					None defined	Not Selected		
SI	6	(1)	SECURITY FUNCTIONALITY VERIFICATION			R					None defined	Not Selected		
SI	6	(2)	SECURITY FUNCTIONALITY VERIFICATION			R					None defined	Not Selected		
SI	6	(3)	SECURITY FUNCTIONALITY VERIFICATION	R	S	S					None defined	Not Selected		
SI	7		SOFTWARE AND INFORMATION INTEGRITY		R	S					P2	X		
SI	7	(1)	SOFTWARE AND INFORMATION INTEGRITY	S	R	S					P2	X	(1) Frequency [at a frequency no longer than 30 days]	
SI	7	(2)	SOFTWARE AND INFORMATION INTEGRITY	S	R	S					P2	X		
SI	7	(3)	SOFTWARE AND INFORMATION INTEGRITY		R	S					P2	X		

SI	7	(4)	SOFTWARE AND INFORMATION INTEGRITY	S	R	S					P2	X	(4) list [information system components], selection [transportation from vendor to operational site and during operation]	
SI	8		SPAM PROTECTION		R					Spam filters are increasingly relying on the reputation of the email originator. Consequently, these systems need to be continuously updated in order to be effective.	P1	X		
SI	8	(1)	SPAM PROTECTION		R	S					P2	X		
SI	8	(2)	SPAM PROTECTION		R	S					P2	X		
SI	9		INFORMATION INPUT RESTRICTIONS	S		R					P2	X		
SI	10		INFORMATION INPUT VALIDATION			R				This security control/enhancement is considered to be best practice. Consequently, inclusion in a departmental profile is strongly encouraged in most cases. This security control/enhancement should be addressed where applicable and if practical to do so.	P3	X		
SI	11		ERROR HANDLING			R					P3	X	(B) [Authorizer defined sensitive or harmful information]	
SI	12		INFORMATION OUTPUT HANDLING AND RETENTION	R	S	S					P3	X		
SI	13		PREDICTABLE FAILURE PREVENTION		R	S					None defined	Not Selected		
SI	13	(1)	PREDICTABLE FAILURE PREVENTION		R	S					None defined	Not Selected		

SI	13	(2)	PREDICTABLE FAILURE PREVENTION		R	S					None defined	Not Selected		
SI	13	(3)	PREDICTABLE FAILURE PREVENTION		R	S					None defined	Not Selected		
SI	13	(4)	PREDICTABLE FAILURE PREVENTION		R	S					None defined	Not Selected		

5 References

[Reference 1] Communications Security Establishment Canada. *IT Security Risk Management: A Lifecycle Approach – Security Control Catalogue*. Information Technology Security Guidance Publication 33 (ITSG-33), Annex 3. 1 November 2012.

[Reference 2] Communications Security Establishment Canada. *IT Security Risk Management: A Lifecycle Approach – Departmental IT Security Risk Management Activities*. Information Technology Security Guidance Publication 33 (ITSG-33), Annex 1. 1 November 2012.

[Reference 3] Communications Security Establishment Canada. *IT Security Risk Management: A Lifecycle Approach – Information System Security Risk Management Activities*. Information Technology Security Guidance Publication 33 (ITSG-33), Annex 2. 1 November 2012.

[Reference 4] Communications Security Establishment Canada. *IT Security Risk Management: A Lifecycle Approach – Glossary*. Information Technology Security Guidance Publication 33 (ITSG-33), Annex 5. 1 November 2012.