Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Information Technology Security Guidance

Identification of Control Elements from Security Controls

ITSG-41 Annex 4

March 2013

Canada

Foreword

The *ITSG-41 Annex 4 - Identification of Control Elements from Security Controls* 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 Client Services Representative at CSEC.

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

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

Effective Date

This publication takes effect on 2013-03-14.

Originally signed by

Toni Moffa

Deputy Chief, IT Security

Revision History

Document No.	Title	Release Date
ITSG-41 Annex 4	Identification of Control Elements from Security Controls	2013-03-14

Table of Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

CSEC	Communications Security Establishment Canada
IT	Information Technology
ITSG	Information Technology Security Guidance
PA	Protected A
PB	Protected B
SDLC	System Development Life Cycle
WLAN	Wireless Local Area Network
ISSIP	Information System Security Implementation Process

1. Introduction

1.1 Purpose

This document describes the process used to identify technology-related and procedural-related control elements from the appropriate security controls selected during the *ITSG-33 IT Security Risk Management: A Lifecycle Approach - Overview* (**ITSG-33**) [1] requirements analysis phase to:

1) Address the *Wireless Local Area Network* (**WLAN**) services deployment's business needs for security; and

2) Comply with the departmentally mandated security controls applicable to the WLAN services deployment.

Examples of how this process is executed is provided using the Protected A/Low Integrity/Low Availability and Protected B/Medium Integrity/Medium Availability security control profiles defined in the ITSG-33 (Annex 4 - Profile 2 (Protected A/Low Integrity/Low Availability) and Annex 4 - Profile 1 (Protected B/Medium Integrity/Medium Availability)).

1.2 Target Audience

This document is intended for information system/security practitioners and those who are responsible for *Information Technology* (**IT**) security risk management activities associated with the design and implementation of WLANs.

1.3 Publication Taxonomy

This document is part of a series of documents that together form the ITSG-41 publication suite. The other documents in the series are listed below:

- *ITSG-41 - Security Requirements for Wireless Local Area Networks* [2]
- *ITSG-41 Annex 1 - Government Hot Spot High-Level Design Guidance* [3]
- *ITSG-41 Annex 2 - Wireless User to Wired Network Connection High-Level Design Guidance* [4]
- *ITSG-41 Annex 3 - Wired Network to Wired Network via Wireless Bridge High-Level Design Guidance* [5]

1 Numbers formatted like "[9]" refer to references listed under the ***References*** heading on the last page of this document.

2. Control Elements

Control Elements are identified from security controls selected from the ITSG-33 (Annex 3 – Security Control Catalogue). The ITSG-33 (Annex 2 - Information System Security Risk Management Activities) also describes security activities to be performed during an IT project's *System Development Life Cycle* (**SDLC**) (illustrated in *Figure 1 - ITSG-33 System Development Life Cycle*) for designing and implementing security in information systems.

Security activities during a requirements analysis phase are performed to select an approved set of security controls to:

1) Address the WLAN services deployment's business needs for security; and
2) Comply with the departmentally mandated security controls applicable to the WLAN services deployment.

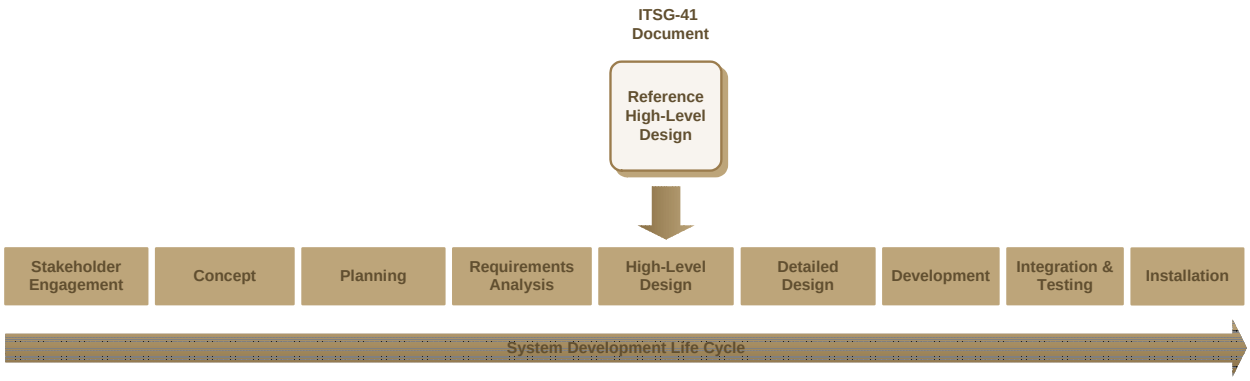

Figure 1 - ITSG-33 Information System Security Implementation Process

The approved set of security controls for the for the WLAN services deployment will include security controls from the management, technical and operational classes as illustrated in *Figure 2 - Security Controls and Control Elements* (**Figure 2**):

1) *Management Class* includes security controls that are not implemented within an information system and focus on the management of IT security;
2) *Technical Class* includes security controls that are typically implemented within an information system using hardware, software, or firmware components; and
3) *Operational Class* includes information system security controls that are typically implemented and executed by people (i.e., adherence to policies or execution of procedures).

Technology-related control elements are determined by first identifying all the management, technical or operations security controls and then grouping them into operating environment and information system security controls. Then the information system security controls are disseminated into technology-related and procedural-related control elements as illustrated in Figure 2:

1) Information system security controls can be either procedural-related and/or technology-related and the responsibility for their implementation falls under the information system owner. They are implemented within the information system using hardware or software components and include any manual procedures associated with the security functionality of those components (e.g., auditing and logging); and

2) Operating environment security controls are predominately management or operational in nature and are implemented through programs, policies or procedures at the departmental level. In some cases they may be implemented through physical infrastructure or through technical means (e.g., physical security) but not within an information system.

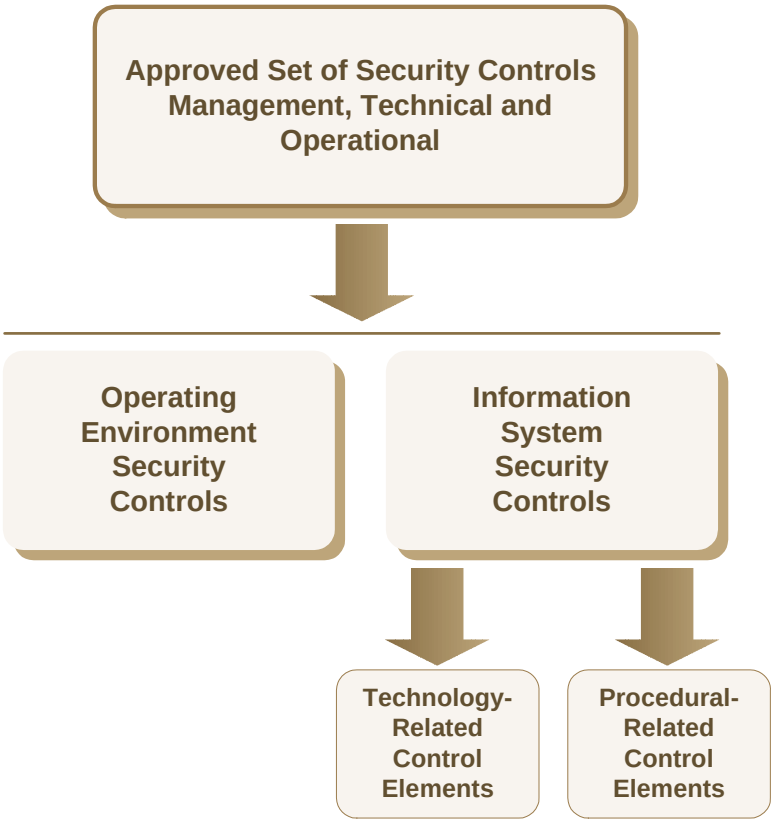

Figure 2 - Security Controls and Control Elements

Each security control definition consists of:

1) A "control" section which specifies one or more concise statements of the specific security capability needed to protect an aspect of an information system. Each statement in the control section is assigned a separate alphabetic designator (i.e., (A), (B), etc.) and must be complied with in order to implement the security control; and

2) An optional "control enhancements" section which specifies through one or more concise statements, additional security capabilities used to increase the strength of a security control. Each control enhancement is assigned a separate numeric designator (i.e., (1), (2), etc.).

Each concise statement within a "control" or "control enhancement" section defines a separate "control element". Information system security controls need to be disseminated into technology-related and procedural-related control elements to determine how the individual elements that comprise each security control will be addressed within the information system.

Technology-related control elements are identified from information system security controls and are to be implemented using technology (e.g., firewall). Procedural-related control elements are identified from information system security controls and are implemented using policies or manual procedures (e.g., human review of firewall logs).

2.1 Technology-Related Control Element Selection

This section describes the detailed steps illustrated in *Figure 3 - Control Elements Identification* required to select the technology-related control elements from an approved set of security controls determined during the *Information System Security Implementation Process* (**ISSIP**) requirements analysis phase.

Step 1: Once the approved set of security controls are defined, *Table 1 - Operating Environment and Information System Security Controls* (**Table 1**) is used to identify which are operating environment and which are information system security controls; and

Step 2: *Table 2 - Technology-Related Control Elements* (**Table 2**) and *Table 3 - Procedural-Related Control Elements* (**Table 3**) are used to identify the technology-related control elements and procedural-related control elements from the information system security controls identified in *Step 1*.

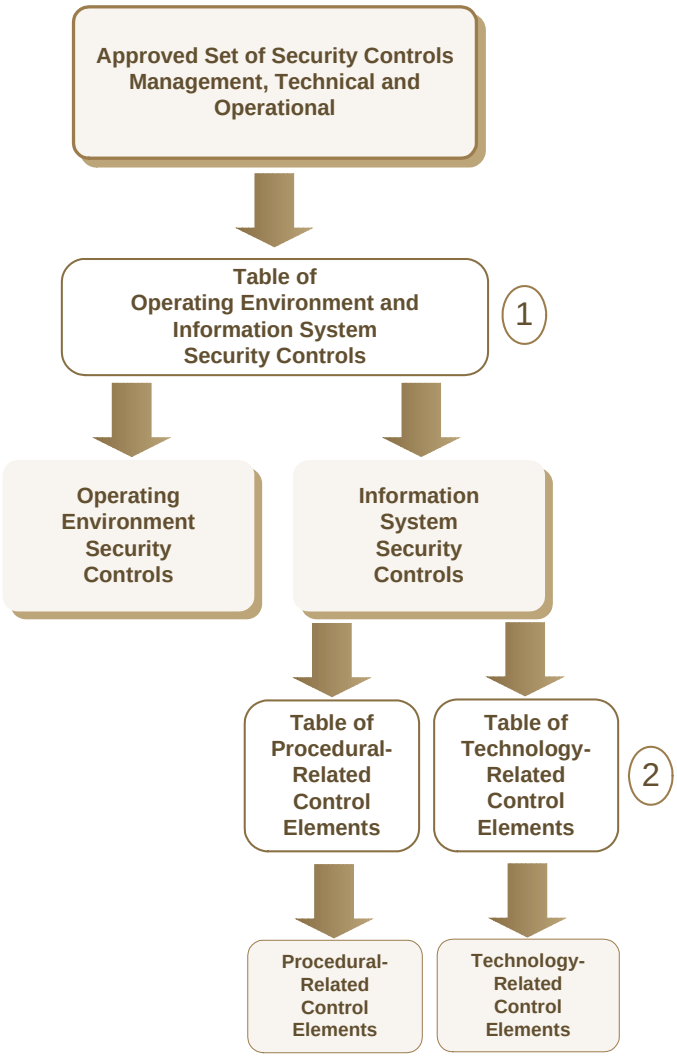

Figure 3 - Control Elements Identification

Table 1 - Operating Environment and Information System Security Controls

Security Control Type	Security Control Number
Operating Environment	AT-1, AT-2, AT-3, AT-4, AT-5, AU-13, CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CM-2, CM-3, CM-4, CM-9, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, IR-8, MA-2, MA-3, MA-5, MA-6, MP-2, MP-3, MP-5, PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-7, PE-8, PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, PE-17, PE-18, PE-19, PL-1, PL-2, PL-4, PL-5, PL-6, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, RA-1, RA-2, RA-3, RA-5, SA-1, SA-2, SA-3, SA-4, SA-5, SA-6, SA-7, SA-8, SA-9, SA-10, SA-11, SA-12, SA-13, SA-14, SI-5, SI-12
Information System	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-9. AC-10, AC-11, AC-14, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11, AU-12, AU-14, CM-1, CM-5, CM-6, CM-7, CM-8, CP-1, CP-9, CP-10, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, MA-1, MA-4, MP-1, MP-4, MP-6, SC-1, SC-2, SC-3, SC-4, SC-5, SC-6, SC-7, SC-8, SC-9, SC-10, SC-11, SC-12, SC-13, SC-14, SC-15, SC-16, SC-17, SC-18, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-26, SC-27, SC-28, SC-29, SC-30, SC-31, SC-32, SC-33, SC-34, SC-100, SC-101, SI-1, SI-2, SI-3, SI-4, SI-6, SI-7, SI-8, SI-9, SI-10, SI-11, SI-13

Table 2 - Technology-Related Control Elements

Security Control Type	Security Control Number
AC-2 Account Management	AC-2-1, AC-2-2, AC-2-3, AC-2-4, AC-2-5, AC-2-6, AC-2-7
AC-3 Access Enforcement	AC-3-A, AC-3-2, AC-3-3, AC-3-4, AC-3-5, AC-3-6
AC-4 Information Flow Enforcement	AC-4-A, AC-4-1, AC-4-2, AC-4-3, AC-4-4, AC-4-5, AC-4-6, AC-4-7, AC-4-8, AC-4-9, AC-4-10, AC-4-11, AC-4-12, AC-4-13, AC-4-14, AC-4-15, AC-4-17
AC-5 Separation of Duties	AC-5-C
AC-6 Least Privilege	AC-6-4
AC-7 Unsuccessful Login Attempts	AC-7-A, AC-7-B, AC-7-1, AC-7-2
AC-8 System Use Notification	AC-8-A, AC-8-B, AC-8-C
AC-9 Previous Logon (Access) Notification	AC-9-A, AC-9-1, AC-9-2, AC-9-3
AC-10 Concurrent Session Control	AC-10-A
AC-11 Session Lock	AC-11-A, AC-11-B, AC-11-1
AC-16 Security Attributes	AC-16-A, AC-16-1, AC-16-2, AC-16-3, AC-16-4, AC-16-5
AC-17 Remote Access	AC-17-C, AC-17-D, AC-17-E, AC-17-1, AC-17-2, AC-17-3, AC-17-5, C-17-7, AC-17-8, AC-17-100
AC-18 Wireless Access	AC-18-B, AC-18-C, AC-18-D, AC-18-1, AC-18-2, AC-18-4, AC-18-5
AC-19 Access Control for Mobile Devices	AC-19-B, AC-19-C, AC-19-D, AC-19-E
AC-21 User-Based Collaboration and Information Sharing	AC-21-B, AC-21-1
AU-3 Content of Audit Records	AU-3-A, AU-3-1, AU-3-2
AU-4 Audit Storage Capacity	AU-4-A
AU-5 Response to Audit Processing Failures	AU-5-A, AU-5-B, AU-5-1, AU-5-2, AU-5-3, AU-5-4
AU-6 Audit Review, Analysis, and Reporting	AU-6-3, AU-6-4, AU-6-5
AU-7 Audit Reduction and Report Generation	AU-7-A, AU-7-1
AU-8 Time Stamps	AU-8-A, AU-8-1
AU-9 Protection of Audit Information	AU-9-A, AU-9-1, AU-9-2, AU-9-3, AU-9-4
AU-10 Non-Repudiation	AU-10-A, AU-10-1, AU-10-2, AU-10-3, AU-10-4, AU-10-5

Security Control Type	Security Control Number
AU-12 Audit Generation	AU-12-A, AU-12-B, AU-12-C, AU-12-1, AU-12-2
AU-14 Session Audit	AU-14-A, AU-14-B, AU-14-1
CM-5 Access Restrictions for Change	CM-5-A, CM-5-1, CM-5-3, CM-5-6, CM-5-7
CM-6 Configuration Settings	CM-6-B, CM-6-1, CM-6-2, CM-6-3
CM-7 Least Functionality	CM-7-A, CM-7-2
CM-8 Information System Component Inventory	CM-8-2, CM-8-3
CP-9 Information System Backup	CP-9-A, CP-9-B, CP-9-C, CP-9-6
CP-10 Information System Recovery and Reconstitution	CP-10-2, CP-10-5
IA-2 Identification and Authentication (Organizational Users)	IA-2-A, IA-2-1, IA-2-2, IA-2-3, IA-2-4, IA-2-5, IA-2-6, IA-2-7, IA-2-8, IA-2-9, IA-2-100
IA-3 Device Identification and Authentication	IA-3-A, IA-3-1, IA-3-2
IA-4 Identifier Management	IA-4-5
IA-5 Authenticator Management	IA-5-1, IA-5-2
IA-6 Authenticator Feedback	IA-6-A
IA-7 Cryptographic Module Authentication	IA-7-A
IA-8 Identification and Authentication (Non-Organizational Users)	IA-8-A
MA-4 Non-Local Maintenance	MA-4-C, MA-4-4, MA-4-6, MA-4-7
SC-2 Application Partitioning	SC-2-A, SC-2-1
SC-3 Security Function Isolation	SC-3-A, SC-3-1, SC-3-2, SC-3-3, SC-3-4, SC-3-5
SC-4 Information in Shared Resources	SC-4-A, SC-4-1
SC-5 Denial of Service Protection	SC-5-A, SC-5-1, SC-5-2
SC-6 Resource Priority	SC-6-A
SC-7 Boundary Protection	SC-7-A, SC-7-B, SC-7-1, SC-7-2, SC-7-3, SC-7-4, SC-7-5, SC-7-6, SC-7-7, SC-7-8, SC-7-9, SC-7-10, SC-7-11, SC-7-12, SC-7-13, SC-7-15, SC-7-16, SC-7-17, SC-7-18
SC-8 Transmission Integrity	SC-8-A, SC-8-1, SC-8-2

Security Control Type	Security Control Number
SC-9 Transmission Confidentiality	SC-9-A, SC-9-1, SC-9-2, SC-9-100
SC-10 Network Disconnect	SC-10-A
SC-11 Trusted Path	SC-11-A
SC-12 Cryptographic Key Establishment and Management	SC-12-A, SC-12-2, SC-12-3, SC-12-4, SC12-5
SC-13 Use of Cryptography	SC-13-A, SC-13-1, SC-13-2, SC-13-3, SC-13-4, SC-13-100, SC-13-101, SC-13-102, SC-13-103, SC-13-104
SC-14 Public Access Protections	SC-14-A
SC-15 Collaborative Computing Devices	SC-15-A, SC-15-B, SC-15-1, SC-15-2
SC-16 Transmission of Security Attributes	SC-16-A, SC-16-1
SC-18 Mobile Code	SC-18-C, SC-18-1, SC-18-3, SC-18-4
SC-20 Secure Name/Address Resolution Service (Authoritative Source)	SC-20-A, SC-20-1
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)	SC-21-A, SC-21-1
SC-22 Architecture and Provisioning for Name/Address Resolution Service	SC-22-A
SC-23 Session Authenticity	SC-23-A, SC-23-1, SC-23-2, SC-23-3, SC-23-4
SC-24 Fail in Known State	SC-24-A
SC-25 Thin Nodes	SC-25-A
SC-26 Honeypots	SC-26-A, SC-26-1
SC-27 Operating System-Independent Applications	SC-27-A
SC-28 Protection of Information at Rest	SC-28-A, SC-28-1
SC-29 Heterogeneity	SC-29-A
SC-30 Virtualization Techniques	SC-30-A, SC-30-1, SC-30-2
SC-32 Information System Partitioning	SC-32-A
SC-33 Transmission Preparation Integrity	SC-33-A

Security Control Type	Security Control Number
SC-34 Non-Modifiable Executable Programs	SC-34-A, SC-34-B, SC-34-1
SC-100 Source Authentication	SC-100-A, SC-100-1, SC-100-2, SC-100-3
SC-101 Unclassified Telecommunications Systems in Secure Facilities	SC-101-A, SC-101-B, SC-101-C, SC-101-D
SI-2 Flaw Remediation	SI-2-1, SI-2-2, SI-2-4
SI-3 Malicious Code Protection	SI-3-A, SI-3-C, SI-3-1, SI-3-2, SI-3-3, SI-3-4
SI-4 Information System Monitoring	SI-4-A, SI-4-C, SI-4-1, SI-4-2, SI-4-3, SI-4-4, SI-4-5, SI-4-6, SI-4-7, SI-4-8, SI-4-10, SI-4-11, SI-4-12, SI-4-13, SI-4-14, SI-4-15
SI-6 Security Functionality Verification	SI-6-A, SI-6-1 SI-6-2
SI-7 Software and Information Integrity	SI-7-A, SI-7-2, SI-7-3
SI-8 Spam Protection	SI-8-A, SI-8-1, SI-8-2
SI-9 Information Input Restrictions	SI-9-A
SI-10 Information Input Validation	SI-10-A
SI-11 Error Handling	SI-11-A, SI-11-B, SI-11-C

Table 3 - Procedural-Related Control Elements

Security Control Type	Security Control Number
AC-2 Account Management	AC-2-1, AC-2-2, AC-2-3, AC-2-4, AC-2-5, AC-2-6, AC-2-7
AC-3 Access Enforcement	AC-3-A, AC-3-2, AC-3-3, AC-3-4, AC-3-5, AC-3-6
AC-4 Information Flow Enforcement	AC-4-A, AC-4-1, AC-4-2, AC-4-3, AC-4-4, AC-4-5, AC-4-6, AC-4-7, AC-4-8, AC-4-9, AC-4-10, AC-4-11, AC-4-12, AC-4-13, AC-4-14, AC-4-15, AC-4-17
AC-5 Separation of Duties	AC-5-C
AC-6 Least Privilege	AC-6-4
AC-7 Unsuccessful Login Attempts	AC-7-A, AC-7-B, AC-7-1, AC-7-2
AC-8 System Use Notification	AC-8-A, AC-8-B, AC-8-C
AC-9 Previous Logon (Access) Notification	AC-9-A, AC-9-1, AC-9-2, AC-9-3
AC-10 Concurrent Session Control	AC-10-A
AC-11 Session Lock	AC-11-A, AC-11-B, AC-11-1
AC-16 Security Attributes	AC-16-A, AC-16-1, AC-16-2, AC-16-3, AC-16-4, AC-16-5
AC-17 Remote Access	AC-17-C, AC-17-D, AC-17-E, AC-17-1, AC-17-2, AC-17-3, AC-17-5, C-17-7, AC-17-8, AC-17-100
AC-18 Wireless Access	AC-18-B, AC-18-C, AC-18-D, AC-18-1, AC-18-2, AC-18-4, AC-18-5
AC-19 Access Control for Mobile Devices	AC-19-B, AC-19-C, AC-19-D, AC-19-E
AC-21 User-Based Collaboration and Information Sharing	AC-21-B, AC-21-1
AU-3 Content of Audit Records	AU-3-A, AU-3-1, AU-3-2
AU-4 Audit Storage Capacity	AU-4-A
AU-5 Response to Audit Processing Failures	AU-5-A, AU-5-B, AU-5-1, AU-5-2, AU-5-3, AU-5-4
AU-6 Audit Review, Analysis, and Reporting	AU-6-3, AU-6-4, AU-6-5
AU-7 Audit Reduction and Report Generation	AU-7-A, AU-7-1
AU-8 Time Stamps	AU-8-A, AU-8-1
AU-9 Protection of Audit Information	AU-9-A, AU-9-1, AU-9-2, AU-9-3, AU-9-4

Security Control Type	Security Control Number
AU-10 Non-Repudiation	AU-10-A, AU-10-1, AU-10-2, AU-10-3, AU-10-4, AU-10-5
AU-12 Audit Generation	AU-12-A, AU-12-B, AU-12-C, AU-12-1, AU-12-2
AU-14 Session Audit	AU-14-A, AU-14-B, AU-14-1
CM-5 Access Restrictions for Change	CM-5-A, CM-5-1, CM-5-3, CM-5-6, CM-5-7
CM-6 Configuration Settings	CM-6-B, CM-6-1, CM-6-2, CM-6-3
CM-7 Least Functionality	CM-7-A, CM-7-2
CM-8 Information System Component Inventory	CM-8-2, CM-8-3
CP-9 Information System Backup	CP-9-A, CP-9-B, CP-9-C, CP-9-6
CP-10 Information System Recovery and Reconstitution	CP-10-2, CP-10-5
IA-2 Identification and Authentication (Organizational Users)	IA-2-A, IA-2-1, IA-2-2, IA-2-3, IA-2-4, IA-2-5, IA-2-6, IA-2-7, IA-2-8, IA-2-9, IA-2-100
IA-3 Device Identification and Authentication	IA-3-A, IA-3-1, IA-3-2
IA-4 Identifier Management	IA-4-5
IA-5 Authenticator Management	IA-5-1, IA-5-2
IA-6 Authenticator Feedback	IA-6-A
IA-7 Cryptographic Module Authentication	IA-7-A
IA-8 Identification and Authentication (Non-Organizational Users)	IA-8-A
MA-4 Non-Local Maintenance	MA-4-C, MA-4-4, MA-4-6, MA-4-7
SC-2 Application Partitioning	SC-2-A, SC-2-1
SC-3 Security Function Isolation	SC-3-A, SC-3-1, SC-3-2, SC-3-3, SC-3-4, SC-3-5
SC-4 Information in Shared Resources	SC-4-A, SC-4-1
SC-5 Denial of Service Protection	SC-5-A, SC-5-1, SC-5-2
SC-6 Resource Priority	SC-6-A
SC-7 Boundary Protection	SC-7-A, SC-7-B, SC-7-1, SC-7-2, SC-7-3, SC-7-4, SC-7-5, SC-7-6, SC-7-7, SC-7-8, SC-7-9, SC-7-10, SC-7-11, SC-7-12, SC-7-13, SC-7-15, SC-7-16, SC-7-17, SC-7-18

Security Control Type	Security Control Number
SC-8 Transmission Integrity	SC-8-A, SC-8-1, SC-8-2
SC-9 Transmission Confidentiality	SC-9-A, SC-9-1, SC-9-2, SC-9-100
SC-10 Network Disconnect	SC-10-A
SC-11 Trusted Path	SC-11-A
SC-12 Cryptographic Key Establishment and Management	SC-12-A, SC-12-2, SC-12-3, SC-12-4, SC12-5
SC-13 Use of Cryptography	SC-13-A, SC-13-1, SC-13-2, SC-13-3, SC-13-4, SC-13-100, SC-13-101, SC-13-102, SC-13-103, SC-13-104
SC-14 Public Access Protections	SC-14-A
SC-15 Collaborative Computing Devices	SC-15-A, SC-15-B, SC-15-1, SC-15-2
SC-16 Transmission of Security Attributes	SC-16-A, SC-16-1
SC-18 Mobile Code	SC-18-C, SC-18-1, SC-18-3, SC-18-4
SC-20 Secure Name/Address Resolution Service (Authoritative Source)	SC-20-A, SC-20-1
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)	SC-21-A, SC-21-1
SC-22 Architecture and Provisioning for Name/Address Resolution Service	SC-22-A
SC-23 Session Authenticity	SC-23-A, SC-23-1, SC-23-2, SC-23-3, SC-23-4
SC-24 Fail in Known State	SC-24-A
SC-25 Thin Nodes	SC-25-A
SC-26 Honeypots	SC-26-A, SC-26-1
SC-27 Operating System-Independent Applications	SC-27-A
SC-28 Protection of Information at Rest	SC-28-A, SC-28-1
SC-29 Heterogeneity	SC-29-A
SC-30 Virtualization Techniques	SC-30-A, SC-30-1, SC-30-2
SC-32 Information System Partitioning	SC-32-A

Security Control Type	Security Control Number
SC-33 Transmission Preparation Integrity	SC-33-A
SC-34 Non-Modifiable Executable Programs	SC-34-A, SC-34-B, SC-34-1
SC-100 Source Authentication	SC-100-A, SC-100-1, SC-100-2, SC-100-3
SC-101 Unclassified Telecommunications Systems in Secure Facilities	SC-101-A, SC-101-B, SC-101-C, SC-101-D
SI-2 Flaw Remediation	SI-2-1, SI-2-2, SI-2-4
SI-3 Malicious Code Protection	SI-3-A, SI-3-C, SI-3-1, SI-3-2, SI-3-3, SI-3-4
SI-4 Information System Monitoring	SI-4-A, SI-4-C, SI-4-1, SI-4-2, SI-4-3, SI-4-4, SI-4-5, SI-4-6, SI-4-7, SI-4-8, SI-4-10, SI-4-11, SI-4-12, SI-4-13, SI-4-14, SI-4-15
SI-6 Security Functionality Verification	SI-6-A, SI-6-1 SI-6-2
SI-7 Software and Information Integrity	SI-7-A, SI-7-2, SI-7-3
SI-8 Spam Protection	SI-8-A, SI-8-1, SI-8-2
SI-9 Information Input Restrictions	SI-9-A
SI-10 Information Input Validation	SI-10-A
SI-11 Error Handling	SI-11-A, SI-11-B, SI-11-C

2.2 Example Protected A/Low Integrity/Low Availability

This section uses the Protected A/Low Integrity/Low Availability security control profile defined within the ITSG-33 (Annex 4 - Profile 2) as the approved set of security controls within the technology-related control elements selection process defined in *Section 2.1 Technology-Related Control Element Selection*. The results of the process are provided.

Step 1: Table 1 is used to identify which security controls within the Protected A/Low Integrity/Low Availability security control profile are operating environment and which are information system security controls. The results are listed in *Table 4 - PA/L/L Operating Environment and Information System Security Controls* (**Table 4**); and

Step 2: Table 2 and Table 3 are used to identify the technology-related and procedural-related control elements from the information system security controls identified in Table 4. The results are listed in *Table 5 - PA/L/L Technology-Related Control Elements* and *Table 6 - PA/L/L Procedural-Related Control Elements* respectively.

Table 4 - PA/L/L Operating Environment and Information System Security Controls

Security Control Type	Security Control Number
Operating Environment	AT-1, AT-2, AT-3, AT-4, CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CM-2, CM-3, CM-4, CM-9, CP-2, CP-3, IR-1, IR-2, IR-4, IR-6, IR-7, IR-8, MA-2, MA-5, MP-2, MP-3, PE-1, PE-2, PE-3, PE-6, PE-7, PE-8, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, PE-18, PL-1, PL-2, PL-4, PL-5, PL-6, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, RA-1, RA-2, RA-3, RA-5, SA-1, SA-2, SA-3, SA-4, SA-5, SA-6, SA-7, SA-8, SA-9, SA-12, SI-5, SI-12
Information System	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-9. AC-11, AC-14, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-1, AU-2, AU-3, AU-4, AU-6, AU-8, AU-9, AU-11, AU-12, CM-1, CM-5, CM-6, CM-7, CM-8, CP-1, CP-9, CP-10, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, MA-1, MA-4, MP-1, MP-6, SC-1, SC-2, SC-7, SC-10, SC-12, SC-13, SC-14, SC-15, SC-17, SC-18, SC-19, SC-22, SC-23, SC-24, SC-28, SI-1, SI-2, SI-3, SI-4, SI-8, SI-10

Table 5 - PA/L/L Technology-Related Control Elements

Security Control Type	Security Control Number
AC-2 Account Management	AC-2-1, AC-2-2, AC-2-3, AC-2-4, AC-2-5
AC-3 Access Enforcement	AC-3-A, AC-3-4
AC-4 Information Flow Enforcement	AC-4-A
AC-5 Separation of Duties	AC-5-C
AC-6 Least Privilege	NA
AC-7 Unsuccessful Login Attempts	AC-7-A, AC-7-B
AC-8 System Use Notification	AC-8-A, AC-8-B, AC-8-C
AC-9 Previous Logon (Access) Notification	AC-9-A, AC-9-1, AC-9-2, AC-9-3
AC-10 Concurrent Session Control	NA
AC-11 Session Lock	AC-11-A, AC-11-B, AC-11-1
AC-16 Security Attributes	AC-16-A, AC-16-2, AC-16-4, AC-16-5
AC-17 Remote Access	AC-17-C, AC-17-D, AC-17-E, AC-17-1, AC-17-2, AC-17-3, AC-17-5, C-17-7, AC-17-8, AC-17-100
AC-18 Wireless Access	AC-18-B, AC-18-C, AC-18-D, AC-18-1, AC-18-2, AC-18-4
AC-19 Access Control for Mobile Devices	AC-19-B, AC-19-C, AC-19-D, AC-19-E
AC-21 User-Based Collaboration and Information Sharing	AC-21-B
AU-3 Content of Audit Records	AU-3-A, AU-3-1
AU-4 Audit Storage Capacity	AU-4-A
AU-5 Response to Audit Processing Failures	AU-5-A, AU-5-B, AU-5-1
AU-6 Audit Review, Analysis, and Reporting	NA
AU-7 Audit Reduction and Report Generation	NA
AU-8 Time Stamps	AU-8-A, AU-8-1
AU-9 Protection of Audit Information	AU-9-A, AU-9-4

Security Control Type	Security Control Number
AU-10 Non-Repudiation	NA
AU-12 Audit Generation	AU-12-A, AU-12-B, AU-12-C
AU-14 Session Audit	NA
CM-5 Access Restrictions for Change	CM-5-A, CM-5-1, CM-5-6
CM-6 Configuration Settings	CM-6-B, CM-6-3
CM-7 Least Functionality	CM-7-A
CM-8 Information System Component Inventory	CM-8-2, CM-8-3
CP-9 Information System Backup	CP-9-A, CP-9-B, CP-9-C
CP-10 Information System Recovery and Reconstitution	NA
IA-2 Identification and Authentication (Organizational Users)	IA-2-A, IA-2-8, IA-2-9, IA-2-100
IA-3 Device Identification and Authentication	IA-3-A, IA-3-1
IA-4 Identifier Management	NA
IA-5 Authenticator Management	IA-5-1, IA-5-2
IA-6 Authenticator Feedback	IA-6-A
IA-7 Cryptographic Module Authentication	IA-7-A
IA-8 Identification and Authentication (Non-Organizational Users)	IA-8-A
MA-4 Non-Local Maintenance	MA-4-C
SC-2 Application Partitioning	SC-2-A, SC-2-1
SC-3 Security Function Isolation	NA
SC-4 Information in Shared Resources	NA
SC-5 Denial of Service Protection	NA
SC-6 Resource Priority	NA
SC-7 Boundary Protection	SC-7-A, SC-7-B, SC-7-1, SC-7-2, SC-7-3, SC-7-4, SC-7-5, SC-7-6, SC-7-7, SC-7-8, SC-7-9, SC-7-11, SC-7-12, SC-7-13, SC-7-18

Security Control Type	Security Control Number
SC-8 Transmission Integrity	NA
SC-9 Transmission Confidentiality	NA
SC-10 Network Disconnect	SC-10-A
SC-11 Trusted Path	NA
SC-12 Cryptographic Key Establishment and Management	SC-12-A
SC-13 Use of Cryptography	SC-13-A, SC-13-4
SC-14 Public Access Protections	SC-14-A
SC-15 Collaborative Computing Devices	SC-15-A, SC-15-B, SC-15-2
SC-16 Transmission of Security Attributes	NA
SC-18 Mobile Code	SC-18-C, SC-18-1, SC-18-3, SC-18-4
SC-20 Secure Name/Address Resolution Service (Authoritative Source)	NA
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)	NA
SC-22 Architecture and Provisioning for Name/Address Resolution Service	SC-22-A
SC-23 Session Authenticity	SC-23-A, SC-23-1, SC-23-2, SC-23-3, SC-23-4
SC-24 Fail in Known State	SC-24-A
SC-25 Thin Nodes	NA
SC-26 Honeypots	NA
SC-27 Operating System-Independent Applications	NA
SC-28 Protection of Information at Rest	SC-28-A
SC-29 Heterogeneity	NA
SC-30 Virtualization Techniques	NA
SC-32 Information System Partitioning	NA
SC-33 Transmission	NA

Security Control Type	Security Control Number
Preparation Integrity	
SC-34 Non-Modifiable Executable Programs	NA
SC-100 Source Authentication	NA
SC-101 Unclassified Telecommunications Systems in Secure Facilities	NA
SI-2 Flaw Remediation	NA
SI-3 Malicious Code Protection	SI-3-A, SI-3-C, SI-3-1, SI-3-2, SI-3-3, SI-3-4
SI-4 Information System Monitoring	SI-4-A, SI-4-C, SI-4-5, SI-4-6, SI-4-7, SI-4-8, SI-4-10, SI-4-11
SI-6 Security Functionality Verification	NA
SI-7 Software and Information Integrity	NA
SI-8 Spam Protection	SI-8-A, SI-8-1, SI-8-2
SI-9 Information Input Restrictions	NA
SI-10 Information Input Validation	SI-10-A
SI-11 Error Handling	NA

Table 6 - PA/L/L Procedural-Related Control Elements

Security Control Type	Security Control Number
AC-1 Access Control Policy and Procedures	AC-1-A, AC-1-B
AC-2 Account Management	AC-2-A, AC-2-B, AC-2-C, AC-2-D, AC-2-E, AC-2-F, AC-2-G, AC-2-H, AC-2-I , AC-2-J
AC-4 Information Flow Enforcement	NA
AC-5 Separation of Duties	AC-5-A, AC-5-B
AC-6 Least Privilege	AC-6-A, AC-6-1, AC-6-2, AC-6-5
AC-14 Permitted Actions Without Identification or Authentication	AC-14-A, AC-14-B, AC-14-1
AC-17 Remote Access	AC-17-A, AC-17-B, AC-17-AA, AC-17-4, AC-17-6
AC-18 Wireless Access	AC-18-A, AC-18-3
AC-19 Access Control for Mobile Devices	AC-19-A, AC-19-F, AC-19-G, AC-19-1, AC-19-2, AC-19-3
AC-20 Use of External Information Systems	AC-20-A, AC-20-B
AC-21 User-Based Collaboration and Information Sharing	AC-21-A, AC-21-100
AC-22 Publicly Accessible Content	AC-22-A, AC-22-B, AC-22-C, AC-22-D, AC-22-E
AU-1 Audit and Accountability Policy and Procedures	AU-1-A, AU-1-B
AU-2 Auditable Events	AU-2-A, AU-2-B, AU-2-C, AU-2-D, AU-2-3, AU-2-4
AU-6 Audit Review, Analysis, and Reporting	AU-6-A, AU-6-B, AU-6-1
AU-11 Audit Record Retention	AU-11-A
CM-1 Configuration Management Policy and Procedures	CM-1-A, CM-1-B
CM-5 Access Restrictions for Change	CM-5-2, CM-5-5
CM-6 Configuration Settings	CM-6-A, CM-6-C, CM-6-D, CM-6-4,
CM-7 Least Functionality	CM-7-1, CM-7-3
CM-8 Information System	CM-8-A, CM-8-B, CM-8-C, CM-8-D, CM-8-E, CM-8-1, CM-8-4, CM-8-5

Security Control Type	Security Control Number
Component Inventory	
CP-1 Contingency Management Policy and Procedures	CP-1-A, CP-1-B, CP-1-AA
CP-9 Information System Backup	CP-9-D, CP-9-1
CP-10 Information System Recovery and Reconstitution	CP-10-A
IA-1 Identification and Authentication Policy and Procedures	IA-1-A, IA-1-B
IA-3 Device Identification and Authentication	IA-3-3
IA-4 Identifier Management	IA-4-A, IA-4-B, IA-4-C, IA-4-D, IA-4-E, IA-4-2, IA-4-3, IA-4-4
IA-5 Authenticator Management	IA-5-A, IA-5-B, IA-5-C, IA-5-D, IA-5-E, IA-5-F, IA-5-G, IA-5-H, IA-5-I, IA-5-3, IA-5-6, IA-5-7, IA-5-8
MA-1 System Maintenance Policy and Procedures	MA-1-A, MA-1-B
MA-4 Non-Local Maintenance	MA-4-A, MA-4-B, MA-4-D
MP-4 Media Storage	NA
SC-1 System and Communication Protection Policy and Procedures	SC-1-A, SC-1-B
SC-7 Boundary Protection	NA
SC-12 Cryptographic Key Establishment and Management	SC-12-1
SC-15 Collaborative Computing Devices	SC-15-3
SC-17 Public Key Infrastructure Certificates	SC-17-A
SC-18 Mobile Code	SC-18-A, SC-18-B, SC-18-2
SC-19 Voice Over Internet Protocol	SC-19-A, SC-19-B
SC-31 Covert Channel Analysis	NA
SC-34 Non-Modifiable Executable Programs	NA
SI-1 System and Information Integrity Policy and Procedures	SI-1-A, SI-1-B
SI-2 Flaw Remediation	SI-2-A, SI-2-B, SI-2-C

Security Control Type	Security Control Number
SI-3 Malicious Code Protection	SI-3-B, SI-3-D, SI-3-5, SI-3-6
SI-4 Information System Monitoring	SI-4-B, SI-4-D, SI-4-E, SI-4-9
SI-6 Security Functionality Verification	NA
SI-7 Software and Information Integrity	NA
SI-8 Spam Protection	SI-8-B
SI-13 Predictable Failure Prevention	NA

2.3 Example Protected B/Medium Integrity/Medium Availability

This section uses the Protected B/Medium Integrity/Medium Availability security control profile defined within the ITSG-33 (Annex 4 - Profile 1) as the approved set of security controls within the technology-related control elements selection process defined in *Section 2.1 Technology-Related Control Element Selection*. The results of the process are provided.

Step 1: Table 1 is used to identify which security controls within the Protected B/Medium Integrity/Medium Availability security control profile are operating environment and which are information system security controls. The results are listed in *Table 7 - PB/M/M Operating Environment and Information System Security Controls* (**Table 7**).

Step 2: Table 2 and Table 3 are used to identify the technology-related control elements and procedural-related control elements from the information system security controls identified in Table 7. The results are listed in *Table 8 - PB/M/M Technology-Related Control Elements* and *Table 9 - PB/M/M Procedural-Related Control Elements* respectively.

Table 7 - PB/M/M Operating Environment and Information System Security Controls

Security Control Type	Security Control Number
Operating Environment	AT-1, AT-2, AT-3, AT-4, CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CM-2, CM-3, CM-4, CM-9, CP-2, CP-3, IR-1, IR-2, IR-4, IR-6, IR-7, IR-8, MA-2, MA-5, MP-2, MP-3, PE-1, PE-2, PE-3, PE-6, PE-7, PE-8, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, PE-18, PL-1, PL-2, PL-4, PL-5, PL-6, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, RA-1, RA-2, RA-3, RA-5, SA-1, SA-2, SA-3, SA-4, SA-5, SA-6, SA-7, SA-8, SA-9, SA-12, SI-5, SI-12
Information System	AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-7, AC-8, AC-9. AC-11, AC-14, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-1, AU-2, AU-3, AU-4, AU-6, AU-8, AU-9, AU-11, AU-12, CM-1, CM-5, CM-6, CM-7, CM-8, CP-1, CP-9, CP-10, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, MA-1, MA-4, MP-1, MP-6, SC-1, SC-2, SC-7, SC-10, SC-12, SC-13, SC-14, SC-15, SC-17, SC-18, SC-19, SC-22, SC-23, SC-24, SC-28, SI-1, SI-2, SI-3, SI-4, SI-8, SI-10

Table 8 - PB/M/M Technology-Related Control Elements

Security Control Type	Security Control Number
AC-2 Account Management	AC-2-1, AC-2-2, AC-2-3, AC-2-4, AC-2-5, AC-2-7
AC-3 Access Enforcement	AC-3-A, AC-3-4
AC-4 Information Flow Enforcement	AC-4-A
AC-5 Separation of Duties	AC-5-C
AC-6 Least Privilege	NA
AC-7 Unsuccessful Login Attempts	AC-7-A, AC-7-B
AC-8 System Use Notification	AC-8-A, AC-8-B, AC-8-C
AC-9 Previous Logon (Access) Notification	AC-9-A, AC-9-1, AC-9-2, AC-9-3
AC-10 Concurrent Session Control	NA
AC-11 Session Lock	AC-11-A, AC-11-B, AC-11-1
AC-16 Security Attributes	AC-16-A, AC-16-2, AC-16-4, AC-16-5
AC-17 Remote Access	AC-17-C, AC-17-D, AC-17-E, AC-17-1, AC-17-2, AC-17-3, AC-17-5, C-17-7, AC-17-8, AC-17-100
AC-18 Wireless Access	AC-18-B, AC-18-C, AC-18-D, AC-18-1, AC-18-2, AC-18-4
AC-19 Access Control for Mobile Devices	AC-19-B, AC-19-C, AC-19-D, AC-19-E
AC-21 User-Based Collaboration and Information Sharing	AC-21-B
AU-3 Content of Audit Records	AU-3-A, AU-3-1
AU-4 Audit Storage Capacity	AU-4-A
AU-5 Response to Audit Processing Failures	AU-5-A, AU-5-B, AU-5-1
AU-6 Audit Review, Analysis, and Reporting	AU-6-3, AU-6-4
AU-7 Audit Reduction and Report Generation	AU-7-A, AU-7-1
AU-8 Time Stamps	AU-8-A, AU-8-1
AU-9 Protection of Audit Information	AU-9-A, AU-9-2, AU-9-4

Security Control Type	Security Control Number
AU-10 Non-Repudiation	NA
AU-12 Audit Generation	AU-12-A, AU-12-B, AU-12-C, AU-12-1, AU-12-2
AU-14 Session Audit	NA
CM-5 Access Restrictions for Change	CM-5-A, CM-5-1, CM-5-6, CM-5-7
CM-6 Configuration Settings	CM-6-B, CM-6-1, CM-6-2, CM-6-3
CM-7 Least Functionality	CM-7-A, CM-7-2
CM-8 Information System Component Inventory	CM-8-2, CM-8-3
CP-9 Information System Backup	CP-9-A, CP-9-B, CP-9-C
CP-10 Information System Recovery and Reconstitution	CP-10-2
IA-2 Identification and Authentication (Organizational Users)	IA-2-A, IA-2-8, IA-2-9, IA-2-100
IA-3 Device Identification and Authentication	IA-3-A, IA-3-1
IA-4 Identifier Management	NA
IA-5 Authenticator Management	IA-5-1, IA-5-2
IA-6 Authenticator Feedback	IA-6-A
IA-7 Cryptographic Module Authentication	IA-7-A
IA-8 Identification and Authentication (Non-Organizational Users)	IA-8-A
MA-4 Non-Local Maintenance	MA-4-C, MA-4-4, MA-4-6
SC-2 Application Partitioning	SC-2-A, SC-2-1
SC-3 Security Function Isolation	NA
SC-4 Information in Shared Resources	NA
SC-5 Denial of Service Protection	SC-5-A, SC-5-2
SC-6 Resource Priority	NA
SC-7 Boundary Protection	SC-7-A, SC-7-B, SC-7-1, SC-7-2, SC-7-3, SC-7-4, SC-7-5, SC-7-6, SC-7-7, SC-7-8, SC-7-9, SC-7-11, SC-7-12, SC-7-13, SC-7-18

Security Control Type	Security Control Number
SC-8 Transmission Integrity	SC-8-A, SC-8-1
SC-9 Transmission Confidentiality	SC-9-A, SC-9-1
SC-10 Network Disconnect	SC-10-A
SC-11 Trusted Path	NA
SC-12 Cryptographic Key Establishment and Management	SC-12-A
SC-13 Use of Cryptography	SC-13-A, SC-13-4
SC-14 Public Access Protections	SC-14-A
SC-15 Collaborative Computing Devices	SC-15-A, SC-15-B, SC-15-2
SC-16 Transmission of Security Attributes	NA
SC-18 Mobile Code	SC-18-C, SC-18-1, SC-18-3
SC-20 Secure Name/Address Resolution Service (Authoritative Source)	NA
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)	NA
SC-22 Architecture and Provisioning for Name/Address Resolution Service	SC-22-A
SC-23 Session Authenticity	SC-23-A, SC-23-1, SC-23-2, SC-23-3, SC-23-4
SC-24 Fail in Known State	SC-24-A
SC-25 Thin Nodes	NA
SC-26 Honeypots	NA
SC-27 Operating System-Independent Applications	NA
SC-28 Protection of Information at Rest	SC-28-A
SC-29 Heterogeneity	SC-29-A
SC-30 Virtualization Techniques	NA
SC-32 Information System Partitioning	NA
SC-33 Transmission	NA

Security Control Type	Security Control Number
Preparation Integrity	
SC-34 Non-Modifiable Executable Programs	NA
SC-100 Source Authentication	NA
SC-101 Unclassified Telecommunications Systems in Secure Facilities	NA
SI-2 Flaw Remediation	NA
SI-3 Malicious Code Protection	SI-3-A, SI-3-C, SI-3-1, SI-3-2, SI-3-3, SI-3-4
SI-4 Information System Monitoring	SI-4-A, SI-4-C, SI-4-1, SI-4-2, SI-4-3, SI-4-4, SI-4-5, SI-4-6, SI-4-7, SI-4-8, SI-4-10, SI-4-11, SI-4-12, SI-4-13, SI-4-14, SI-4-15
SI-6 Security Functionality Verification	NA
SI-7 Software and Information Integrity	SI-7-A, SI-7-2, SI-7-3
SI-8 Spam Protection	SI-8-A, SI-8-1, SI-8-2
SI-9 Information Input Restrictions	SI-9-A
SI-10 Information Input Validation	SI-10-A
SI-11 Error Handling	SI-11-A, SI-11-B, SI-11-C

Table 9 - PB/M/M Procedural-Related Control Elements

Security Control Type	Security Control Number
AC-1 Access Control Policy and Procedures	AC-1-A, AC-1-B
AC-2 Account Management	AC-2-A, AC-2-B, AC-2-C, AC-2-D, AC-2-E, AC-2-F, AC-2-G, AC-2-H, AC-2-I , AC-2-J
AC-4 Information Flow Enforcement	NA
AC-5 Separation of Duties	AC-5-A, AC-5-B
AC-6 Least Privilege	AC-6-A, AC-6-1, AC-6-2, AC-6-5
AC-14 Permitted Actions Without Identification or Authentication	AC-14-A, AC-14-B, AC-14-1
AC-17 Remote Access	AC-17-A, AC-17-B, AC-17-AA, AC-17-4, AC-17-6
AC-18 Wireless Access	AC-18-A, AC-18-3
AC-19 Access Control for Mobile Devices	AC-19-A, AC-19-F, AC-19-G, AC-19-1, AC-19-2, AC-19-3, AC-19-100
AC-20 Use of External Information Systems	AC-20-A, AC-20-B, AC-20-1, AC-20-2
AC-21 User-Based Collaboration and Information Sharing	AC-21-A, AC-21-100
AC-22 Publicly Accessible Content	AC-22-A, AC-22-B, AC-22-C, AC-22-D, AC-22-E
AU-1 Audit and Accountability Policy and Procedures	AU-1-A, AU-1-B
AU-2 Auditable Events	AU-2-A, AU-2-B, AU-2-C, AU-2-D, AU-2-3, AU-2-4
AU-6 Audit Review, Analysis, and Reporting	AU-6-A, AU-6-B, AU-6-1, AU-6-7
AU-11 Audit Record Retention	AU-11-A
CM-1 Configuration Management Policy and Procedures	CM-1-A, CM-1-B
CM-5 Access Restrictions for Change	CM-5-2, CM-5-5
CM-6 Configuration Settings	CM-6-A, CM-6-C, CM-6-D, CM-6-4
CM-7 Least Functionality	CM-7-1, CM-7-3
CM-8 Information System	CM-8-A, CM-8-B, CM-8-C, CM-8-D, CM-8-E, CM-8-1, CM-8-4, CM-8-5, CM-8-

Security Control Type	Security Control Number
Component Inventory	6
CP-1 Contingency Management Policy and Procedures	CP-1-A, CP-1-B, CP-1-AA
CP-9 Information System Backup	CP-9-D, CP-9-1, CP-9-2, CP-9-3, CP-9-5
CP-10 Information System Recovery and Reconstitution	CP-10-A, CP-10-4, CP-10-6
IA-1 Identification and Authentication Policy and Procedures	IA-1-A, IA-1-B
IA-3 Device Identification and Authentication	IA-3-3
IA-4 Identifier Management	IA-4-A, IA-4-B, IA-4-C, IA-4-D, IA-4-E, IA-4-1, IA-4-2, IA-4-3, IA-4-4
IA-5 Authenticator Management	IA-5-A, IA-5-B, IA-5-C, IA-5-D, IA-5-E, IA-5-F, IA-5-G, IA-5-H, IA-5-I, IA-5-3, IA-5-6, IA-5-7, IA-5-8
MA-1 System Maintenance Policy and Procedures	MA-1-A, MA-1-B
MA-4 Non-Local Maintenance	MA-4-A, MA-4-B, MA-4-D, MA-4-1, MA-4-2, MA-4-3, MA-4-5
MP-4 Media Storage	MP-4-A, MP-4-B, MP-4-1
SC-1 System and Communication Protection Policy and Procedures	SC-1-A, SC-1-B
SC-7 Boundary Protection	NA
SC-12 Cryptographic Key Establishment and Management	SC-12-1
SC-15 Collaborative Computing Devices	SC-15-3
SC-17 Public Key Infrastructure Certificates	SC-17-A
SC-18 Mobile Code	SC-18-A, SC-18-B, SC-18-2
SC-19 Voice Over Internet Protocol	SC-19-A, SC-19-B
SC-31 Covert Channel Analysis	NA
SC-34 Non-Modifiable Executable Programs	NA
SI-1 System and Information Integrity Policy and Procedures	SI-1-A, SI-1-B
SI-2 Flaw Remediation	SI-2-A, SI-2-B, SI-2-C

Security Control Type	Security Control Number
SI-3 Malicious Code Protection	SI-3-B, SI-3-D, SI-3-5, SI-3-6
SI-4 Information System Monitoring	SI-4-B, SI-4-D, SI-4-E, SI-4-9
SI-6 Security Functionality Verification	NA
SI-7 Software and Information Integrity	SI-7-1, SI-7-4
SI-8 Spam Protection	SI-8-B
SI-13 Predictable Failure Prevention	NA

3. References

[1] *ITSG-33 - IT Security Risk Management: A Lifecycle Approach - Overview;* **CSEC** (Nov 2012)

[2] *ITSG-41 - Security Requirements for Wireless Local Area Networks*; **CSEC** (March 2013)

[3] *ITSG-41 Annex 1 - Government Hot Spot High-Level Design Guidance*; **CSEC** (March 2013)

[4] *ITSG-41 Annex 2 - Wireless User to Wired Network Connection High-Level Design Guidance*; **CSEC** (March 2013)

[5] *ITSG-41 Annex 3 - Wired Network to Wired Network via Wireless Bridge High-Level Design Guidance*; **CSEC** (March 2013)