Choose a building block.

Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

Top 10 IT Security Actions: #6 Provide Tailored Cyber Security Training

ITSM.10.093

February 2020

MANAGEMENT

Canada

FOREWORD

This document is an UNCLASSIFIED publication that is part of a suite of documents that focus on each of the top 10 IT security actions recommended in *ITSM.10.189 Top 10 IT Security Actions to Protect Internet-Connected Networks and Information* [1][1].

EFFECTIVE DATE

This publication takes effect on February 20, 2020.

REVISION HISTORY

Revision	Amendments	Date
1	First release.	February 20, 2020

[1] Numbers in square brackets refer to a reference cited in the Supporting Content section of this document.

OVERVIEW

One of our top 10 recommended IT security actions is to provide cyber security training to all employees, including contractors, senior managers, and executives. Training ensures that all employees understand the cyber security issues that are relevant to your organization. Your training should clearly define employee roles and responsibilities for preventing and responding to threats and compromises. The guidance in this document is based on the security controls found in *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [2].

Your organization, regardless of its size, is a target for threat actors. There are many factors to consider when taking actions to protect your organization from attacks; you can lower your organization's level of risk by training your employees on cyber security issues and their roles and responsibilities in protecting networks, systems, and IT assets from compromises.

This document is part of a suite of documents that focus on each of the top 10 IT security actions recommended in *ITSM.10.189 Top 10 IT Security Actions to Protect Internet-Connected Networks and Information* [1]. While implementing all 10 of the recommended security actions can reduce your organization's vulnerability to cyber threats, you should review your current cyber security activities to determine whether additional actions are required. For more information on implementing the top 10 IT security actions, email or phone our Contact Centre:

Canadian Centre for Cyber Security (CCCS) Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

TABLE OF CONTENTS

1 IT Security Risk Management: An Overview 5

1.1 Top 10 IT Security Actions 5

1.2 Relationship to the IT Security Risk Management Process 6

2 Cyber Security Training 8

2.1 In-House Training 8

2.2 External Training 8

3 Cyber Security Policies and Procedures (AT-1) 9

3.1 Policies 9

3.2 Procedures 9

4 Basic Cyber Security Awareness (AT-2) 10

4.1 Insider Threat Awareness 10

4.2 Practical Exercises 10

5 Role-Based Training (AT-3) 11

6 Awareness and Training Activity Review (AT-4) 11

7 Summary 12

7.1 Contact Information 12

8 Supporting Content 13

8.1 List of Abbreviations 13

8.2 Glossary 13

8.3 References 14

LIST OF FIGURES

Figure 1: Top 10 IT Security Actions - #6 Provide Tailored Training 5

Figure 2: Applicable Security Control Classes and Families Described in ITSG-33 7

LIST OF ANNEXES

Annex A ITSG-33 Security Control Catalogue 15

A.1 Operational Security Controls: Awareness and Training 15

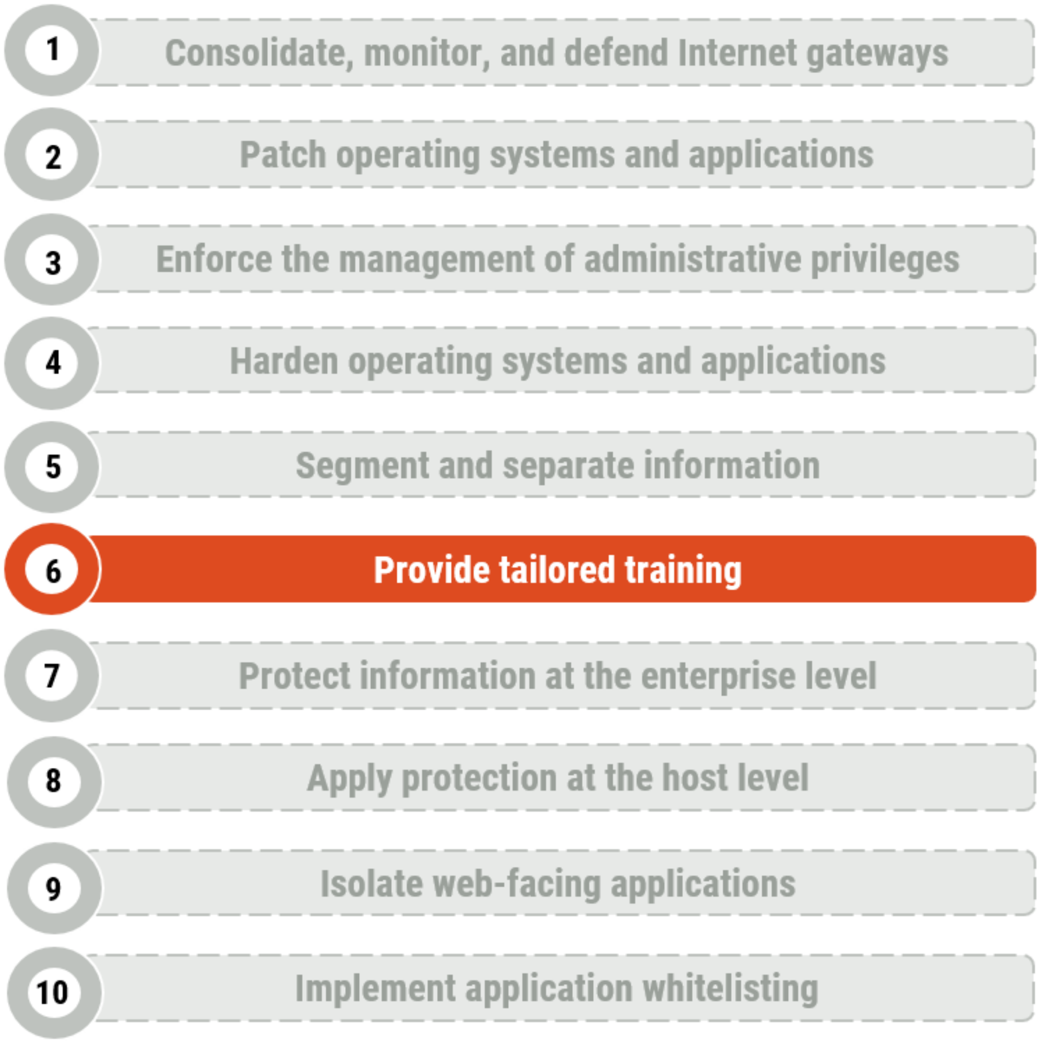
1 IT SECURITY RISK MANAGEMENT: AN OVERVIEW

1.1 TOP 10 IT SECURITY ACTIONS

This document outlines how you can provide tailored cyber security training in your organization. This document is based on the advice in ITSM.10.189 [1] and the security controls listed in Annex 3A of ITSG-33 [2].

Our top 10 recommended IT security actions, which are listed in in Figure 1 below and ITSM.10.189 [1], are based on our analysis of trends in cyber security threat activities and the impact of those threat activities on Internet-connected networks. By implementing all 10 of the actions, you can address many of your organization's IT security vulnerabilities.

Cyber security threats that are common to many organizations may impact you differently. To ensure your organization's security needs are appropriately met, review your current security and risk management activities.



1. Consolidate, monitor, and defend Internet gateways
2. Patch operating systems and applications
3. Enforce the management of administrative privileges
4. Harden operating systems and applications
5. Segment and separate information
6. **Provide tailored training**
7. Protect information at the enterprise level
8. Apply protection at the host level
9. Isolate web-facing applications
10. Implement application whitelisting

Figure 1: Top 10 IT Security Actions - #6 Provide Tailored Training

1.2 RELATIONSHIP TO THE IT SECURITY RISK MANAGEMENT PROCESS

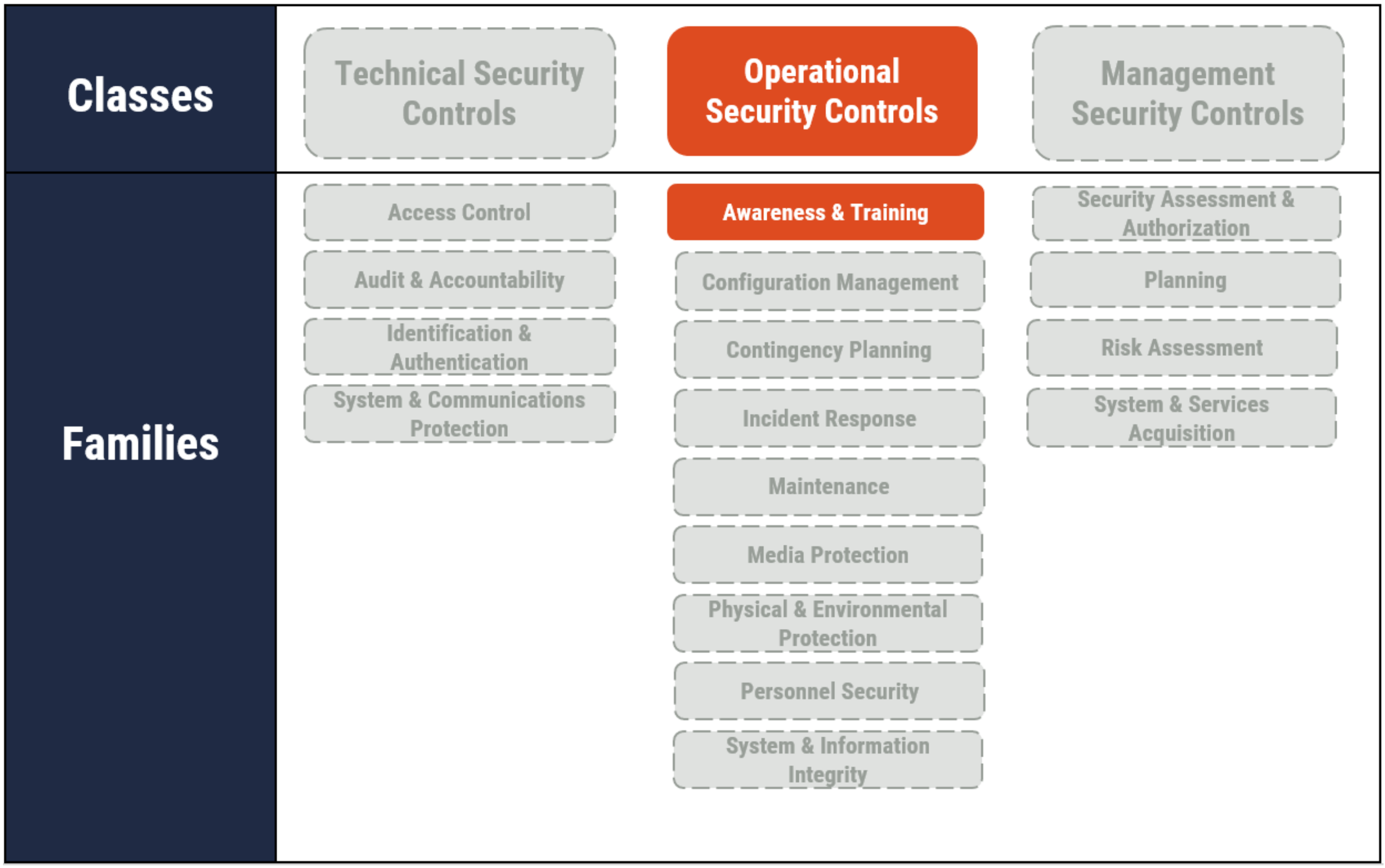
Our top 10 security actions are taken from the security controls listed in Annex 3A of ITSG-33 [2]. ITSG-33 [2] describes the roles, responsibilities, and activities that help organizations manage their IT security risks and includes a catalogue of security controls (i.e. standardized security requirements to protect the confidentiality, integrity, and availability of IT assets). These security controls are divided into three classes, which are further divided into several families (or groupings) of related security controls:

- **Technical security controls:** Security controls that are implemented and executed by information systems primarily through security mechanisms contained in hardware, software, and firmware components.
- **Operational security controls:** Information system security controls that are primarily implemented and executed by people and typically supported using technology, such as supporting software.
- **Management security controls:** Security controls that focus on managing IT security and IT security risks.

As illustrated in Figure 2, the guidance in this document addresses operational security controls that fall under the awareness and training (AT) family. This document includes actions that satisfy the following security controls:

- **AT-1 Security Awareness and Training Policy and Procedures**
- **AT-2 Security Awareness**
- **AT-3 Role-Based Security Training**
- **AT-4 Security Training Records**

See Annex A of this document for more information on controls AT-1, AT-2, AT-3, and AT-4.



Classes	Technical Security Controls	Operational Security Controls	Management Security Controls
Families	Access Control Audit & Accountability Identification & Authentication System & Communications Protection	Awareness & Training Configuration Management Contingency Planning Incident Response Maintenance Media Protection Physical & Environmental Protection Personnel Security System & Information Integrity	Security Assessment & Authorization Planning Risk Assessment System & Services Acquisition

Figure 2: Applicable Security Control Classes and Families Described in ITSG-33

You can use the security controls discussed in this document and in Annex 3A of ITSG-33 [2] as a foundation when determining how best to manage your organization's cyber security risks and protect its networks, systems, and IT assets. However, keep in mind that implementing these controls is only one part of the IT security risk management process.

ITSG-33 [2] describes a process based on two levels of risk management activities: departmental-level activities and information system-level activities. These two levels of activities will help your organization identify its security needs for both the entire organization and its information systems. Once you understand your security needs at each level, you can identify which security controls your organization needs to implement and maintain based on your accepted level of risk.

2 CYBER SECURITY TRAINING

This document outlines the specific actions you can take to implement cyber security awareness and training in your organizations. These actions are based on the security controls AT-1, AT-2, AT-3, and AT-4. These actions include the following:

- Creating policies and procedures
- Providing basic cyber security awareness training
- Using practical exercises to increase employee awareness

2.1 IN-HOUSE TRAINING

Employees need to understand their cyber security roles and responsibilities because their activities and overall awareness impacts your organization's cyber security posture. Training your employees on current cyber security issues can help you protect your networks, systems, and IT assets from cyber attacks and compromises. For example, with proper training, employees can successfully identify and handle malicious emails. Proper training also helps employees contribute positively to your organization's cyber security culture.

You should frequently review your cyber security awareness program and activities to ensure they are effective and updated as required. To gain support from your senior management and executive teams, provide documentation that demonstrates how training activities support employee awareness of cyber security. For example, you can coordinate with your organization's IT security team to send regular reports on cyber attacks and compromises to executives. These reports can be used to demonstrate the need for increased cyber security training or the effectiveness of current training.

2.2 EXTERNAL TRAINING

While this document focuses on how you can implement in-house training, you should also explore training opportunities that are offered outside of your organization.

Our Cyber Centre Learning Hub (CCLH) offers in-class and online learning activities and programs for various audiences, including non-technical employees, IT practitioners, and senior-level managers. Currently, these activities and programs are offered primarily to those who work within the Government of Canada (GC) or with our domestic partners; however, provincial and municipal governments and organizations, as well as industry partners who work with GC departments may also participate.

All CCLH courses can be delivered organization-wide or to individual employees or small groups. Courses cover topics including the following:

- IT security risk management
- Cyber security for developers and IT practitioners
- Communications security
- Cryptographic security

Course offerings may change, but you can review the CCLH course calendar on our website for more information on available courses.

Cyber Centre Learning Hub
education@cyber.gc.ca
https://cyber.gc.ca/en/learning-and-innovation-hub

3 CYBER SECURITY POLICIES AND PROCEDURES (AT-1)

The guidance in this section is based on **AT-1 Security Awareness and Training Policy and Procedures**. See Annex A of this document for more information on control AT-1.

3.1 POLICIES

Cyber security policies establish the expected employee behaviours and the acceptable use of company networks, systems, IT assets, and information. Policies define the roles and responsibilities of all employees, which include contractors, senior management, and executives, to prevent, identify, and respond to cyber security threats and compromises. Your policy should also address management's role and responsibility to support cyber security awareness and training in the organization.

You may want to create separate policies that address the acceptable use of email, social media, the Internet, removable media (e.g. mobile devices and USB drives), and any other business applications and services used. You should also have a policy that addresses requirements for securing and handling IT equipment, assets, and sensitive information.

All policies should be written in plain language and use business-relevant terms. To be effective, a policy should be enforceable and include a compliance monitoring plan. You should ensure that all new employees, including contractors, senior management, and executives, are made aware of their responsibility to follow corporate policies by reading and acknowledging them. Orientation sessions and training for new employees should include an overview of all policies.

3.2 PROCEDURES

Procedures guide employees on how to fulfill policy requirements and how to carry out business processes. You should create procedures that will help employees fulfill their cyber security responsibilities, such as reporting security incidents and following the organization's incident management plan. Some commonly implemented procedures include the following:

- Physically storing and securing IT equipment and assets
- Performing back ups
- Conducting security audits
- Identifying and reporting malicious emails
- Reporting security incidents

4 BASIC CYBER SECURITY AWARENESS (AT-2)

The guidance in this section is based on **AT-2 Security Awareness**. Subsections 4.1 and 4.2 include ways to enhance basic awareness and training by addressing insider threats and using practical exercises; these enhancements are based on the control enhancements for AT-2. See Annex A of this document for more information.

Your organization is responsible for determining training plans. We recommend that you provide basic cyber security training to all new and existing personnel, including senior managers, executives, and contractors. Basic training sessions should communicate expected behaviours and policy requirements.

Training should also be provided when new information systems are implemented or changed. You can provide computer-based training to enable employees to refresh their understanding of policies and procedures as required.

Although additional topics may be required to support your organizational environment, your training programs should cover the following topics at a minimum:

- Identifying and handling malicious emails
- Handling and securing IT assets and sensitive information
- Recognizing potential indicators of an insider threat
- Reporting security incidents and potential insider threats

4.1 INSIDER THREAT AWARENESS

An **insider threat** is a threat to your business that comes from within, such as current or former employees and contractors. An insider threat can access or modify sensitive information (e.g. financial or personal information or information about business security practices, data, and systems) for personal or financial gain. An insider threat can also take actions that could prevent your organization from conducting its business (e.g. lock out accounts, encrypt or delete critical information, or destroy important assets).

You should train employees on the potential indicators of insider threats. Indicators may include behaviours such as prolonged job dissatisfaction and increasingly hostile behaviour, attempts to gain unauthorized access to information and credentials, unexplained access to financial resources, or violations of other organizational policies and procedures. You should also train employees on how they can report potential insider threats without fear of reprisal.

4.2 PRACTICAL EXERCISES

You can test your employees' understanding of cyber security policies and procedures and reinforce training objectives by including practical exercises in your training sessions. Some examples include the following exercises:

- Spotting spear phishing emails from among actual emails
- Identifying compromised applications and testing employees' understanding of how to report security incidents
- Reviewing social engineering attempts that try to collect information or gain unauthorized access

All exercises should be done in coordination with IT and security operations.

5 ROLE-BASED TRAINING (AT-3)

This section is based on **AT-3 Role-Based Security Training** and its control enhancements. See Annex A of this document for more information.

You should tailor your training program and activities to address the intended audience's roles and responsibilities (i.e. role-based training). Certain roles (e.g. developers, system administrators, auditors, enterprise architects, or information security officer) may require access to information systems that hold or process sensitive information and system-level software; you should provide training to employees before they are granted access to these systems and software.

Role-based training activities should also include practical exercises. As an example, for managers, a role-based activity may include a tabletop exercise that is based on a compromise scenario. You can use this scenario to review the key roles and responsibilities and the process for handling a compromise or incident. For employees, role-based training activities may include exercises to help them recognize suspicious communications and uncharacteristic system behaviours (e.g. malicious code).

You should also address the different management, operational, and technical roles and responsibilities that support the security of your organization's networks, systems, and IT assets. You should also cover how to use and operate any environmental controls (e.g. fire suppression and detection systems, smoke detectors, sprinkler systems, power, temperature and humidity) or physical controls (e.g. intrusion alarms, surveillance equipment, access control devices, security guards) that are used to protect IT assets, as some of these controls may require specialized training.

6 AWARENESS AND TRAINING ACTIVITY REVIEW (AT-4)

This section is based on **AT-4 Security Training Records**. See Annex A of this document for more information on control AT-4.

Much like other aspects of your organization, your cyber security needs and requirements will change over time. You should review all your training activities annually to ensure that the training covers current cyber security strategies. If there are any changes to your organization's cyber security policies, training modules should reflect those changes.

Be sure to document and monitor all training activities for their ongoing effectiveness. You should also keep individual training records to ensure that employees have participated in and completed training activities.

7 SUMMARY

One of our top 10 recommended IT security actions is to provide tailored cyber security training to all employees. Being secure requires more than implementing technical controls; you can lower your organization's level of risk by training your employees on cyber security issues and their roles and responsibilities in protecting networks, systems, and IT assets from compromises.

Your organization creates and maintains a strong cyber security culture by ensuring that cyber security policies and procedures are in place and that employees have access to cyber security training. However, training is just one aspect of improving your cyber security posture. To best protect your organization against cyber threats, you should review and implement all the actions recommended in ITSM.10.189 [1].

7.1 CONTACT INFORMATION

For more information on implementing the top 10 IT security actions, email or phone our Contact Centre:

CCCS Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
AT	Awareness and Training (security control family code)
CCCS	Canadian Centre for Cyber Security
CCLH	Cyber Centre Learning Hub
GC	Government of Canada
IT	Information Technology

8.2 GLOSSARY

Term	Definition
Availability	A value that is assigned to information assets, software, and hardware (infrastructure and its components). Data with the highest possible availability rating must always be accessible. Implied in its definition is that availability includes the protection of assets from unauthorized access and compromise.
Confidentiality	A value that is assigned to a set of information to indicate its sensitivity level and any access restrictions that prevent unauthorized people from accessing it.
Cyber attack	The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.
Integrity	A value that is assigned to information to indicate how sensitive it is to data loss. Implied in its definition is that integrity includes protecting information from being modified or deleted unintentionally or when it's not supposed to be. Integrity helps determine that information is what it claims to be. Integrity also applies to business processes, software application logic, hardware, and personnel.
IT asset	The components of an information system, including business applications, data, hardware, and software.
Malware	Malicious software designed to infiltrate or damage a computer system without the owner's consent. Common forms of malware include computer viruses, worms, trojans, spyware, and adware.
Management security control	A class of security controls that focus on the management of IT security and IT security risks.
Operational security control	A class of security controls primarily implemented and executed by people and typically supported by technology (e.g. supporting software).
Phishing	An attempt to solicit confidential information from an individual, group, or organization by mimicking or spoofing a specific, usually well-known brand. Phishers attempts to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.
Risk	In the cyber security context, the likelihood and the impact of a threat using a vulnerability to access an asset.

Term	Definition
Security control	A management, operational, or technical high-level security requirement needed for an information system to protect the confidentiality, integrity, and availability of its IT assets. Security controls can be applied by using a variety of security solutions, including security products, security policies, security practices, and security procedures.
Spear phishing	The use of spoofed email or electronic communications to persuade people within an organization to reveal sensitive information (e.g. usernames or passwords). Spear-phishing attacks are small-scale and well-targeted.
Technical security control	A class of security controls that are implemented and executed by information systems primarily through security mechanisms contained in hardware, software, and firmware components.
Threat	Any potential event or act (deliberate or accidental) or natural hazard that could compromise IT assets and information.
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited by a threat actor to adversely affect an organization's assets or operations.

8.3 REFERENCES

Number	Reference
1	Canadian Centre for Cyber Security. *ITSM.10.189 Top 10 Information Technology Security Actions to Protect Internet-Connected Networks and Information.* October 2018.
2	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach.* December 2014.

Annex A ITSG-33 Security Control Catalogue

A.1 Operational Security Controls: Awareness and Training

Table 1 lists the awareness and training (AT) controls as defined in Annex 3A of ITSG-33 [2].

Table 1: ITSG-33 Operational Security Controls: Awareness and Training

Number	Control	Requirement	Control Enhancements	Related ITSG-33 Controls
AT-1	Security awareness and training policies and procedures	(A) The organization develops, documents, and disseminates to [*organization-defined personnel or roles*]: i. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance ii. Procedures to help implement the security awareness and training policy and associated security awareness and training controls	None	None
		(B) The organization reviews and updates the current: i. Security awareness and training policy ii. Security and awareness training procedures	None	None
AT-2	Security awareness	(A) The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): i. As part of initial training for new users ii. When required by information system changes iii. [*Organization-defined frequency*] thereafter	**Practical exercises:** The organization includes practical exercises in security awareness training that simulate actual cyber attacks.	CA-2 CA-7 CP-4 IR-3
			Insider threat: The organization includes security awareness training on recognizing and	PL-4 PS-3 PS-6

Number	Control	Requirement	Control Enhancements	Related ITSG-33 Controls
			reporting potential indicators of insider threat.	
AT-3	Role-based security training	(A) The organization provides role-based security training to personnel with assigned security roles and responsibilities: i. Before authorizing access to the information system or performing assigned duties ii. When required by information system changes iii. [*Organization-defined frequency*] thereafter	**Environmental controls:** The organization provides [*organization-defined personnel or roles*] with initial and [*organization-defined frequency*] training in using and operating environmental controls.	PE-1 PE-13 PE-14 PE-15
			Physical security controls: The organization provides [*organization-defined personnel or roles*] with initial and [*organization-defined frequency*] training in using and operating physical controls.	PE-2 PE-3 PE-4 PE-5
			Practical exercises: The organization includes practical exercises in security training that reinforce training objectives.	None
			Suspicious communications and anomalous system behaviour: The organization provides training to its personnel on [*organization-defined indicators of malicious code*] to recognize suspicious communications and anomalous behaviour	None

Number	Control	Requirement	Control Enhancements	Related ITSG-33 Controls
			in organizational information systems.	
AT-4	Security training records	(A) The organization documents and monitors individual information system security training activities, including basic security awareness training and specific information system security training.	None	AT-2 AT-3
		(B) The organization retains individual training records for [*organization-defined time period*].	None	AT-2 AT-3