**Status of WGITA-IDI Handbook on IT Audit Update**
2018 INTOSAI Working Group on IT Audit Meeting
April 17, 2018

Background

- The original WGITA – IDI Handbook on IT Audit was released in 2014 and integrated training and related audits conducted by over 20 SAIs in the AFROSAI region.
- Update Team selected Chapter 7 - Information Security for 1st Update

Status

- Updated Chapter 7 with Cybersecurity - October 2017
- Reviewed and comments incorporated - January 2018 (see Attachment 1 for latest draft)
- Expect completion and test of audit matrices by June 2018
- Chapter & Appendix to be turned over to WGITA at that time

Active IT Audit Tool

- At last 2017 WGITA Meeting, Active IT Audit Tool was discussed and presented
- Active IT Audit Tool will contain the updates to the chapter and appendix
- Active IT Audit Tool to be discussed at the EUROSAI IT Meeting in Tallinn, Estonia, 2018
- Active IT Audit Tool available for download – link

Any questions or comments, please contact Madhav Panwar, USA.

CHAPTER 7

# INFORMATION & CYBER SECURITY

## I. What Is Information & Cyber Security

Information Security can be defined as the ability of a system to protect information and system resources with respect to confidentiality, availability and integrity. The protection of information and information systems against unauthorised access or modification of information, whether in storage, processing, or transit, and against denial of service to authorised users. Information security includes those measures necessary to govern, prevent detect, document, and counter such threats. Information security allows an organisation to protect its Information System infrastructure from unauthorised users. Information security comprises computer security and communications security.

Both information security and cybersecurity are closely related and there are overlaps in the actions necessary to protect breaches. Specifically, Merriam-Webster defines cyber security as, “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack”[1]. Furthermore, The NIST cybersecurity framework states, "Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems[2], placing the Nation’s security, economy, and public safety and health at risk."[3] While not exclusively limited to, Cybersecurity is the process of protecting information by preventing, detecting, and responding to attacks, often from external sources. External attacks can be initiated by individuals, state sponsored entities, or groups who have an interest in the data or want to disrupt business operations. Both government and private information systems are subject to cyber-attacks (the use of information technology to disrupt, steal, destroy, IT systems and related data). Since many government systems collect information on citizens (medical records, payroll and tax, court history) and typically have large amounts of sensitive information in their databases, it is imperitive that the data and systems be protected from cyber-attacks. For our purposes and definition, Cybersecurity also includes the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. This chapter will discuss cybersecurity in more detail beginning section I.3.

A robust information security program provides for data availability, confidentiality and integrity to ensure that the organization meets business needs and has the ability to limit risk to its enterprise data. Information security needs to be many things to the enterprise. It is the gatekeeper of the enterprise’s information assets. That calls for the information security programme to protect organisational data while

[1] https://www.merriam-webster.com/dictionary/cybersecurity

[2] Critical infrastructure includes systems and assets so vital to the United States that incapacitating or destroying them would have a debilitating effect on national security. These critical infrastructures are grouped by the following industries or “sectors”: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology (IT); nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[3] Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1, National Institute of Standards and Technology, January 10, 2017

also enabling the enterprise to pursue its business objectives—and to tolerate an acceptable level of risk in doing so. Providing information to those who should have it is as significant as protecting it from those who should not have it. Security must enable the business and support its objectives rather than becoming self-serving.

## I.1 The necessity of Information & Cyber Security

Information Security is increasingly more important for government institutions as the interconnection of public and private networks and governmental transparency and the sharing of information resources increase the complexity of controlling access and preserving the confidentiality, integrity, and availability of data.

Information systems are incredibly complex assemblages of technology, processes, and people that collaboratively function together to accommodate the processing, storage, and transmission of information to support an organisation's mission and business functions. Therefore it is essential that every organisation builds an information security programme.

The objective of an information system security programme is to protect an organisation's information by reducing the risk of loss of confidentiality, integrity and availability of that information to an acceptable level. If the organisation does not have a guarantee of information security then it will deal with the risks and potential threats to the organisation's operations, the achievement of the overall objectives, and ultimately affect the credibility of the organisation.

As the potential, complexity and role of information technologies grow, information security becomes an increasingly important topic of IT audits. It is a critical factor of organisations' activities, because information security weaknesses may lead to severe damage:

- **Law** – violations of legal and regulatory requirements.
- **Reputation** – damage to the organisation's standing, causing breach of trust with other organisations or damaging the image of government or state.
- **Finance** – e.g. fines, compensations, reduced sales, repair or restore costs.
- **Productivity** – reduction of effectiveness and/or efficiency in a project, programme or whole service provided by the organisation.
- **Vulnerability** – systems and data accessed in an unauthorised way are prone to malware and may be opened for further intrusions.

This damage may be caused by:

- Security breaches, both detected and undetected.
- Unauthorised external connections to remote sites.
- Exposure of information – intentional and unintentional disclosure of corporate assets and sensitive information to unauthorised parties.

With respect to cybersecurity, a recent GAO report[4] mentioned that Cyber terrorists can make use of various techniques, tactics, and practices, or exploits, to adversely affect an organization's computers, software, or networks, or social engineering to intercept or steal valuable or sensitive information. These

[4] Federal Information Security: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices, GAO-17-543, September 2017.

exploits are carried out through various conduits, including websites, e-mails, wireless and cellular communications, Internet protocols, portable media, and social media. Further, adversaries can leverage computer software programs as a means by which to deliver a threat by embedding exploits within software files that can be activated when a user opens a file within its corresponding program. Protection against such activities requires constant vigilance and monitoring of IT activities. Additionally, all of the controls of Information Security must also be undertaken to reduce the risk of business data loss or disruption of services.

Furthermore, leading associations[5] see Cyber security threats becoming a prevalent issue today facing most organizations, one that is recognized by companies to be an enterprise wide issue requiring thoughtful attention. They further state that investments in controls are essential to protecting organizations from increasingly sophisticated and widely available attack methods. These controls also provide a framework and strategy which along with management review, risk assessments and audits of the cyber security controls are required to reduce the risk of the cyber threat. Limiting the attractiveness of the target by taking more defensive measures and making it longer for the hacker to penetrate a system should be a primary goal of cyber security according to ISACA.

Finally, the National Institute of Standards and Technology, (NIST)[6] which establishes standards, states that cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the security, economy, and public safety and health at risk. If cybersecurity weaknesses are left un-mitigated and risks exposed, it can drive up costs and impact organization's ability to conduct their business operations.

Cybersecurity is increasingly more important for government institutions as the interconnection of public and private networks and the sharing of information resources increase the complexity of monitoring network access, detecting if intrusion is or has taken place, controlling access and preserving logs to determine what might have been compromised and also ensuring the confidentiality, integrity, and availability of data.

Government and private business depend on transmission of information to support an organization's mission and business functions. Unless secured and monitored, the information could be potentially compromised by hackers. Therefore it is essential that every organization build, implement, and periodically audit their cybersecurity program.

In addition, many countries and leading institution place emphasis on the importance of ensuring that the protection of critical infrastructure from cyber-related threats. For example, consistent with other countries and leading institution's definitions, the Ministry of Transport and Communications of Qatar[7] defines the objectives of Cybersecurity as safeguarding national critical information infrastructure, responding to, resolving and recovering from cyber incidents and attacks through timely information sharing, collaboration, and action, and fostering a culture of cyber security that promotes safe and appropriate use of cyberspace.

## I.2 Key Elements of Information Security

### a. Information Security Attributes & Policies

To support the successful implementation of Information Security effectively, there are some critical elements that must be met. These are:

[5] Auditing Cyber Security: Evaluating Risk and Auditing Controls, 2017.

[6] Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1, National Institute of Standards and Technology, January 10, 2017

[7] http://www.motc.gov.qa/en/cyber-security

**Confidentiality** is preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The confidentiality aspect is very important because it involves privacy issues that must be provisioned. To constantly maintain it, the system must ensure that each individual keep up the right to control on what information is collected about them, how it is used, who has used it, who maintains it, and what purpose it is used for.

**Integrity** is guarding against improper information modification or destruction, which includes ensuring information non-repudiation and authenticity[44]. To certify the integrity of the information, an authentication mechanism is necessary to ensure that users are the persons they claim to be. While the process of ensuring that the information created or transmitted needs to meet the requirements of non-repudiation[45].

**Authenticity** is the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.

**Non-repudiation** is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. Non-repudiation may not be necessary to evaluate integrity to meet an audit objective.

**Availability** is ensuring that all information systems including hardware, communication networks, software applications and the data they hold shall be available to users at necessary times to carry out business activities. It should also ensure timely and reliable access to and use of information.

Information security is about minimising exposure, based upon risk management, in all areas of IT. Failure to implement and monitor risk mitigation processes in one area may cause damage in the entire organisation. Even if it is broadly known that managing the information security risks effectively is essential to an organisation's safety, these risks are often overlooked or safety precautions are not updated in response to changing conditions.

Having a good security policy is important. It might not be necessary to write a security policy from scratch as various templates are available[8] to help organizations get started. A policy for security typically contains the following areas:

Definition of information security – objectives and scope (including data confidentiality)

Detailed security principles, standards and compliance requirements

IT department personnel should not have operational or accounting responsibilities

Definition of general and specific responsibilities for all aspects of information security

Use of information assets and access to email, Internet

Mode and method of access

Back-up procedures

Procedures to deal with malicious software/ programs

Elements of security education and training

Process for reporting suspected security incidents

Business Continuity & Disaster Recovery Planning (See Chapter 6)

Methods of communicating to staff the policy and procedures adopted for IS security

[8] SANS – Information Security Policy Templates - https://www.sans.org/security-resources/policies/

## b. Implementing Information Security

Typically, a group or organization, in the Chief Information Officer's (CIO) chain of command is responsible for planning, generating training, and responsible for implementing an agencies information security policy. In many organizations, this could be the work given to a unit or an individual, who work with the IT organisation (which is typically under the CIO) to acquire appropriate tools and implement the right processes to implement the security policy effectively. Employees of the organization have specific responsibilities with respect to information security (password protection, incident reporting, following appropriate procedures) and are typically provided training for these by the organization. Additionally, most policies require an annual refresher IS training. This training may include updates and new topics as the IT organization see fit. There is also a need to ensure that the data of the organisation that is accessed by or transferred to external organisations is suitably protected. This too is a part of the training and a joint responsibility of the employee (process, procedures, etc.) and the IT organization which may provide the requisite tools to facilitate data exchange in a secure manner. The auditor will need to see if this entity is able to implement the IS requirements as documented by the organisation.

## Human resources security

Employees and or contract personnel who handle personal or organizational sensitive data in an organisation need to receive appropriate awareness training and regular updates in an effort to safeguard the data entrusted to them. Appropriate roles and responsibilities assigned for each job description need to be defined and documented in alignment with the organisation's security policy. The institution's data must be protected from unauthorised access, disclosure, modification, destruction or interference. The management of human resources security and privacy risks is necessary during all phases of employment association with the organisation.

The three areas of Human Resources Security are:

- **Pre-Employment:** This topic includes defining roles and responsibilities of the job, defining appropriate access to sensitive information for the job, and determining the depth of candidate's screening levels – all in accordance with the company's IT security policy. During this phase, contract terms should also be established.

- **During Employment:** Employees with access to sensitive information in an organisation should receive periodic reminders of their responsibilities and receive ongoing, updated security awareness training to ensure their understanding of current threats and corresponding security practices to mitigate such threats.

- **Termination or Change of Employment:** To prevent unauthorised access to sensitive information, access should be revoked immediately upon termination/separation of an employee with access to such information. This also includes the return of any assets of the organisation that was held by the employee.

A programme of security awareness should be in place, reminding all staff of the possible risks and exposure and of their responsibilities as custodians of corporate information.

## Physical and environmental security

Physical security describes measures that are designed to deny access to unauthorised personnel (including attackers or even accidental intruders) from physically accessing a building, facility, resource, or stored information; and guidance on how to design structures to resist potentially hostile acts. Physical security can be as simple as a locked door or as elaborate as multiple layers of barriers, armed security guards and guardhouse placement.

Physical security is primarily concerned with restricting physical access by unauthorised people (commonly interpreted as intruders) to controlled facilities, although there are other considerations and situations in which physical security measures are valuable (for example, limiting access within a facility and/or to specific assets, and environmental controls to reduce physical incidents such as fires and floods).

Security inevitably incurs costs and, in reality, it can never be perfect or complete – in other words, security can reduce but cannot entirely eliminate risks. Given that controls are imperfect, strong physical security applies the principle of defence in depth using appropriate combinations of overlapping and complementary controls. For instance, physical access controls for protected facilities are generally intended to:

- Deter potential intruders (e.g. warning signs and perimeter markings).
- Distinguish authorized from unauthorized people (e.g. using pass cards/badges and keys).
- Delay, frustrate and ideally prevent intrusion attempts (e.g. strong walls, door locks and safes).
- Detect intrusions and monitor/record intruders (e.g. intruder alarms and CCTV systems).
- Trigger appropriate incident responses (e.g. by security guards and police).

## Access control

Access control refers to exerting control over who can interact with a resource. Often but not always, this involves an authority, who does the controlling. The resource can be a given building, group of buildings, or computer-based IT system. Access control is – whether physical or logical – in reality, an everyday phenomenon. A lock on a car door is essentially a simple form of access control. A PIN on an ATM system at a bank is another means of access control as well as biometric devices. The possession of access control is of prime importance when persons seek to secure important, confidential, or sensitive information and equipment.

In a government environment, access control is important because many government entities process sensitive data and privacy concerns limit who should view various parts of the information. Access control ensures that only users with the process credentials have access to sensitive data.

## I.3 Key Elements of Cyber Security

As SAIs get more connected to the internet and provide 24/7 access to IT auditors to the infrastructure, both from the worksite and remote locations, they face the risk of attacks on their systems and infrastructure from external sources. Many examples of distributed denial of service attacks (DDoS) have been in the News all over the world.. Such outside attacks exploit not only weaknesses in the operating systems but also poor security practices that many organizations have in place. Cyber Security encompasses all measures taken to identify and protect digital information, networks, and equipment from threats generally arising from external attacks.

### Implementing Cyber Security

There is a general consensus that a robust cyber security program should include intrusion detection, event logging, incident response, and a degree of forward intelligence on threats. These along with existing measure taken to protect the infrastructure go a long way to ensure hackers do get into your systems undetected and disrupt operations.

To support the successful implementation of a cyber security program, NIST has defined a framework (known as the Cybersecurity Framework)[9] that includes the following functions, Identify, Protect, Detect, Respond, and Recover. IT auditors can choose to measure how well each of these "core functions" are implemented. The implementation tiers are Partial, Risk Informed, Repeatable, and Adaptive.

a. **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

   Identification of threats that have the potential to impact business operations are an important step. Threats can include human error, espionage, sensitive data disclosure, social media exploits, sabotage, fraud), to environmental threats (e.g., power/heating, ventilating, air conditioning, cable cuts, theft, sensitive media disposal), to technical threats (e.g., lack of logging, malicious code, unauthorized access, session takeover, mobile media loss, hardware/software failure, remote access).[10]

b. **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. Protection includes defining access control procedures, providing periodic awareness and training on security, and developing and implementing processes for the protection of business processes.

c. **Detect** - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. Along with a help desk for incident management detection controls include

[9] Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1, National Institute of Standards and Technology, January 10, 2017

[10] Auditing Cyber Security: Evaluating Risk and Auditing Controls, 2017.

anomalies and event logging and detection, continuous monitoring of security related applications and procedures, and installing automated detection technologies that raise alarms and messages when unusual activity is detected.

**d. Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. A response plan should be developed, tested, communicated and updated periodically as conditions change. Coordinate with stakeholders periodically to ensure response planning and steps are appropriate.

**e. Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

### Auditing Cyber Security

Appendix VII contains the audit matrices for the audit of Information and Cybersecurity. Combined, these enable an IT auditor to get an assessment of the entity's preparedness for protecting their operations against security related threats. For those IT auditors who wish to provide more details on the Cyber Security preparedness of an entity, they can utilize the *"Baldrige Cybersecurity Excellence Builder"* and the NIST Cybersecurity Framework which provides a tiered approach to assign a level of maturity to an entity across the areas listed above. For example an entity may have a more robust program to protect their infrastructure but perhaps a not as robust program to facilitate a quick and efficient recovery.

The Tiers in the NIST framework represent a range, from Partial to the highest, Adaptive. Other tiers include Risk Informed and Repeatable. For example if an organization's policies are not documented and cyber security practices are ad hoc or reactive, the organization generally would be considered at the Partial level of maturity or Tier. Organizations that have integrated risk management activities to cyber security practices and controls would be at the Risk Informed tier. Finally, at the highest tier, Adaptive, organizations modify their cyber security practices to lessons learned and implement a continuous learning and improvement process to stay on top of emerging threats and take actions to prevent them. Using the tiers provides an IT auditor with a new set of tools to investigate and report on an entity's cyber security preparedness and actions.

## II. Risks to the audited entity

IT Security policies, procedures, and their enforcement enables an organisation to protect its IT infrastructure from unauthorised users. IT security policy for an organisation lays out the high level requirements for the organisation and its employees to follow in order to safeguard critical assets. It also provides for training of staff on security issues and ensures that they follow established procedures for data access and control. Additionally, the IT policy refers to laws and other regulations that the organisation is required to follow. There are many obstacles that organisations face in regard to the implementation of an effective information security system. Without effective governance to deal with these obstacles, IT security will have a higher risk of failure in meeting the organisation's objectives.

Every organisation faces its own unique challenges as its individual environmental, political, geographical, economic and social issues differ. Any one of these issues can present obstacles to providing effective IT governance, and it is the responsibility of the IT auditor to point out information security risks to the management.

The following are all significant risks identified at most organisations:

- Unauthorised disclosure of information
- Unauthorised modification or destruction of information

- Vulnerability of IS attack
- Destruction of the IS infrastructure
- Disruption of access to or use of information or an information system
- Disruption of information system processing
- Information or data stolen.

Looking for audited organisations' risk exposures, special attention should be given to following areas:

- Information security **strategies** not aligned with IT or business requirements
- **Policies** not applied uniformly with varying enforcement
- **Non-compliance** with internal and external requirements
- Information security not included in **projects'** portfolio maintenance and development processes
- **Architecture** design resulting in ineffective, inefficient or misguided information security solutions
- Inadequate **physical** security measures and assets management
- Inadequate hardware system application **configuration**
- Inefficient **organisation** of information security processes and undefined or confusing IS responsibility structure
- Inappropriate **human resources** solutions
- Ineffective use of **financial resources** allocated to information security, information security **value** (cost-benefit) structure not aligned with business needs or goals
- Information security not **monitored** or monitored ineffectively.

The IT auditor should begin with assessing the adequacy of risk assessment methods and take into consideration audit issues related to the implementation of information security. An audit matrix will assist the IT auditor to raise audit questions, criteria for evaluation, documents required and technical analysis can be used. At the end, the IT auditor may develop a detailed audit programme according to the needs and development during the audit fieldwork.

When carrying out an information security audit, the IT auditor should address issues identified above. Some references are provided below. The IT auditor should make an informed decision on which to utilize as well as look at part reports from other SAIs for overall guidance.

The audit matrix for this section can be found in Appendix VII.

References / Further Reading

ISO 27000 series *Information Security Management System*
ISO 27005 *information security risk management*
ISACA *RiskIT Framework*
*COBIT 4.1 Framework*, 2007, IT Governance Institute
*COBIT 5 Framework*, 2012, ISACA
ISACA ITAF – *A Professional Practices Framework for IT Assurance*. USA. 2008
ISACA *Information Security Audit/Assurance Program*, 2010
ISACA *IT Risk Management Audit/Assurance Program*, 2012
COSO *Enterprise Risk Management Framework*.
NIST, Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1, January 10, 2017
Baldrige Cybersecurity Excellence Builder (BCEB), Version 1.0