Build a Cyber Security Career from Scratch.

A Step by Step Guide to Become a Cyber Security Specialist

Cyber Security Portal

All Candidates who purchase this book, will get free access to Infosec4TC Cyber Security Portal, where they will find all Cyber Security templates/ Business documents that was explained in the book, Cyber Security Checklists and all the resources needed to build your professional career. Send a Screenshot of your orders confirmation to Inforsec4tc@Infosec4tc.com to request your access.

Gift - The Ultimate Cyber Security Certificates Bundle.

Send a Screenshot of your orders confirmation to Inforsec4tc@Infosec4tc.com to provide you access to the Ultimate Cyber Security Certificates Bundle for free

1st Edition: November 2020

Contents

Introduction

Cyber security is one of the best careers In the job market today, in a recent study published “3.5 million unfulfilled jobs in the market by 2021” so time couldn’t be better.

The candidates who area applying for these jobs are fewer than 1 every 4 are even qualified.

The problem is that candidates who want to join Cyber Security career are not qualifying themselves the right way. Online courses and training are great resources to provide basic knowledge bit not enough to get a job as real experience is missing.

What if you have a chance to get hired in a real organization and start learning while you are working?

I strongly believe that real Cyber Security experience will come from working in the field and not just for online courses or training.

This book is following a top down approach where we are simulating a real company where you get hired with your current knowledge as a Cyber Security Specialist and you will be requested to implement an Information Security Management System- ISMS from Scratch.

In Each ISMS Security domain, you will learn.

1- The implementation of each security controls in a real business environment.
2- The challenge we are facing during the security controls implementation.
3- The real document / templates used in business environments
4- The Standards, we are following in the implementation
5- Cyber Security Check lists used to evaluate security controls in any organization.
6- Realistic Interview questions

Many peoples are thinking to shift their career to Cyber Security but they don’t know from where to start with question like:

- Is Cyber Security the right career for me?
- What technical background I need to have to work in Cyber Security?
- Is my age a barrier to start in this career?

Many technical questions I get from my students and other candidates who want to join Cyber Security career, they don’t know from where to start and how.

This book you will give you the answer to all your questions and a step by step guide to help you to build your realistic Cyber Security Career regardless of your technical background.

This Books is for:

1- You
2- Candidates who want to change their career to Cyber Security Career
3- IT Student who plan to work in Cyber Security
4- Network Administrator
5- Security Administrator

6- IT Support team
7- Developers
8- DB Admins
9- System Admins
10- Junior Cyber Security Specialist who need to enhance their skills.

Let me start by introducing myself I have been working as a Cyber Security Consultant for more than 20 years managing different types of Cyber security projects, I manager project such as (Business Continuity, Disaster Recovery Planning, Framework and compliance implementation, Vulnerability assessment and penetration testing) beside working as a Certified Instructor which helped me to help a lot of students building or changing their career in Cyber Security. In this book I will share my real life professional experience with you to make sure that you don't just learn the concept and definition but you also you will learn how to implement them in a real business environment.

How to use this Book

The Book will guide you on how to build an Information Security Management System (ISMS) from Scratch or to evaluate an implemented ISMS and work on the missing controls, and this is one of the main responsibility of a Cyber Security Specialist.

The Book will be divided to 12 Domains

1- Information Asset Management
2- IS Risk Management
3- Incident & Problem Management
4- Access Control
5- Comm & Operations Management
6- Business Continuity Planning
7- IS Aquisition, Development
8- Environmental & Physical Sec
9- Roles & Respons of HR
10- Compliance & Audit
11- IS Assurance & Performance
12- IS Management & Governance

If you cover all the 12 domains and understand the controls using the attached templates, you will gain the basic Cyber Security skills that you will need to start working in the field and applying for CS jobs and those are the skills needed.

The book will follow a top/down approach which mean that it will simulate that you are hired in an organization as an Cyber Security Professional and your main tasks is to build an Information Security Management System -ISMS for scratch and **with your current experience you will need to learn and build all the controls from scratch** , this approach will put you under a lot of pressure **but the achievement will be great in a short period of time** this is opposite to the normal learning approach which is down top approach where you will learn all the concepts first, then start to implement them in real business time , this will take long time.

You do not have to worry about the technical requirements as everything will be covered in this book form scratch.

You need to do effort while studying and do some research to understand each controls implementation challenge and weakness because you will need to explain a lot of those topics to business users during your work. Trust me this will be the best investment in your time.

You will also have access to a video library that provide a visual explanation for all the book topics and ISMS controls beside an especially important template library that is essential to your work. A very good practice to learn Cyber Security in a short period of time is to use mind mapping that will help you organize your thinking and relate topics to each other.

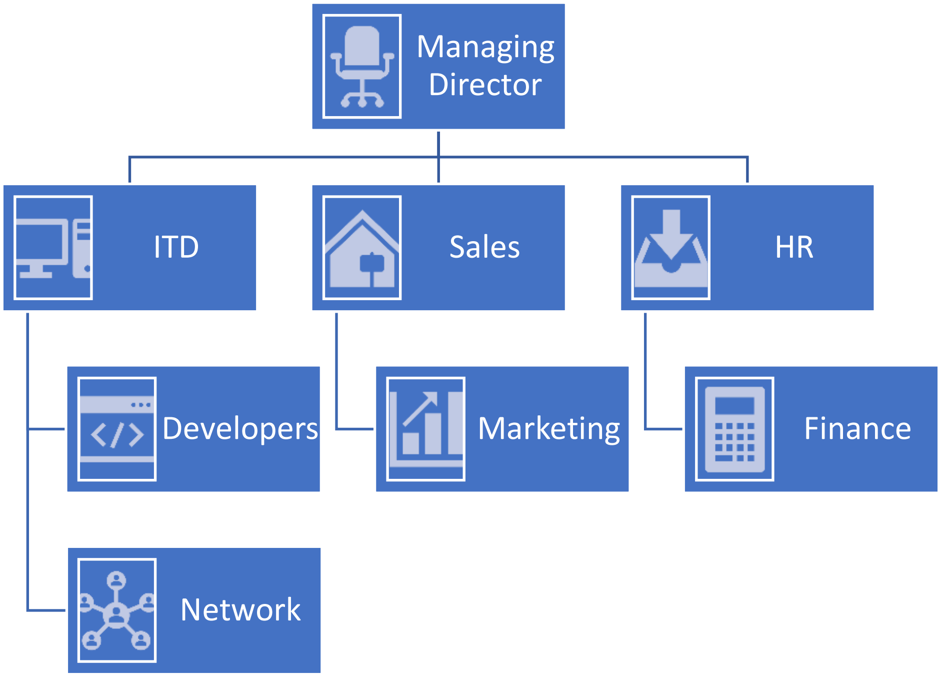
The Book will also qualify you to pass some of the most important Cyber Security professional exams and get certified (e.g. CISSP, CISM, CISA)

The Bool will also give you a chance to work as a freelancer as many of the ISMS domain can be audited and implemented by an Freelancer or a consultant.

Finally, once you complete the book and understand it very well you can use the ISMS checklist to verify the controls in your organization and check the applied / missing controls.

Learning by Simulation:

XYZ-Solution is a software company that provide (IOS, Android) Mobile application development to their customer, the company was established in year 2000 and consist of 150 Employees working in different departments, the company consist of a managing director and other departments as shown in the below Hierarchy.



XYZ-Solution hired you to implement an Information Security Management System (ISMS) as a regulation / compliance requirement beside they are planning to get ISO 27001 which require to have ISMS Implemented.

Lets start to cover domain by domain in ISMS and in each domain, I will clarify the applicable departments and what will be your role.

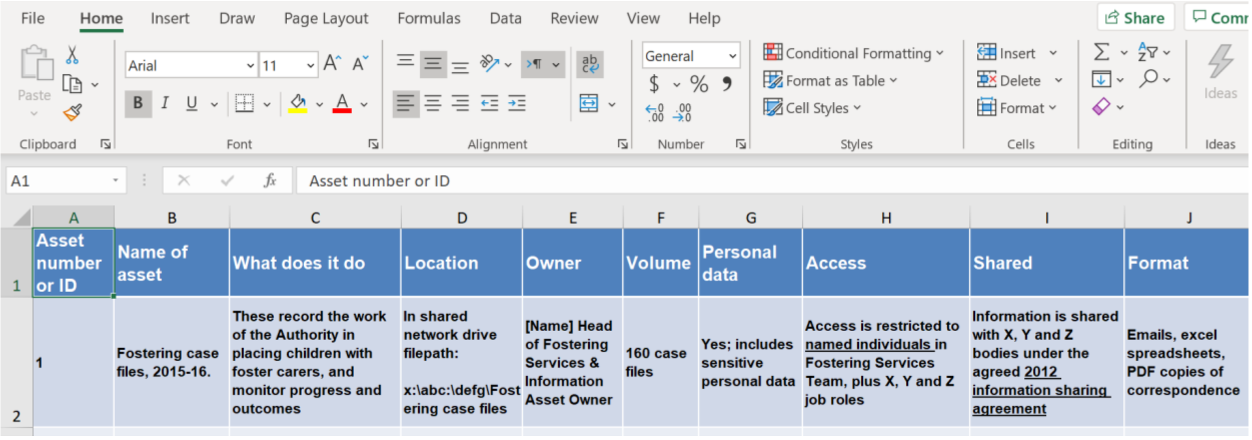
Two Important websites to get Cyber Security Standards and best practices

1- National institute for standard and technology
https://www.nist.gov/
2- Center of Internet Security
https://www.cisecurity.org/cybersecurity-tools/

Domain 1: Information Asset Management

Applicable: All company Departments.

The first step to implement an ISMS is to identity and document all your information assets (*check the Information asset register sample – IAR*), where all types of information should be mentioned (Soft / Hard documents, Databases, Computers or any mobile devices that hold information) with their classification, owner, custodian, location



Asset number or ID	Name of asset	What does it do	Location	Owner	Volume	Personal data	Access	Shared	Format
1	Fostering case files, 2015-16.	These record the work of the Authority in placing children with foster carers, and monitor progress and outcomes	In shared network drive filepath: x:\abc:\defg\Fostering case files	[Name] Head of Fostering Services & Information Asset Owner	160 case files	Yes; includes sensitive personal data	Access is restricted to named individuals in Fostering Services Team, plus X, Y and Z job roles	Information is shared with X, Y and Z bodies under the agreed 2012 information sharing agreement	Emails, excel spreadsheets, PDF copies of correspondence

Sample of IAR

Your Role in this domain:

1- Create a presentation for all department to explain what is IAR and how different department can maintain their IAR.
2- To make sure all departments have an information asset register (IAR) which is filled correctly and reviewed al least once a year
3- If any departments doesn't have IAR, you will need to do a presentation to explain the IAR documents and who to filled it and answer all their questions

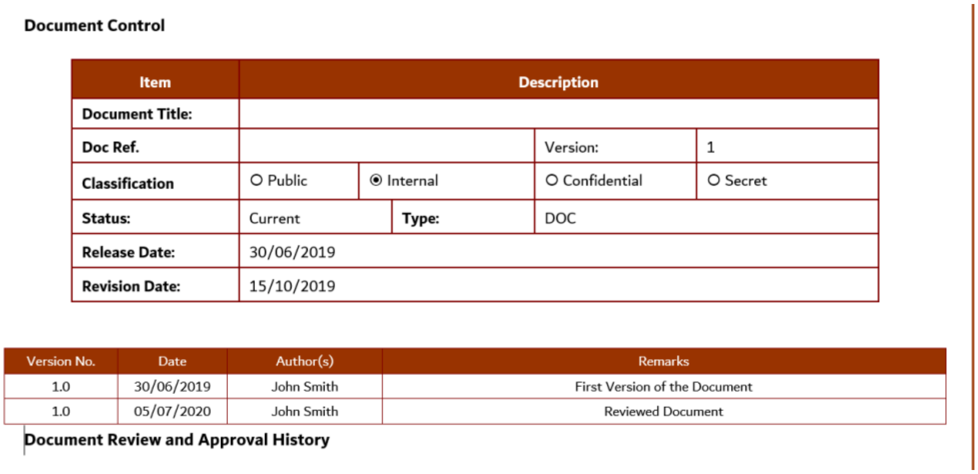
Control 1.1

Identifies & documents a register of all information assets for the entire entity, including the information and data assets and the related information processing facilities and components, such as software assets, people assets, physical assets, etc. and consider other details such as, physical location, license details, business value, and any other necessary information that may be required to avoid risks and recover from disasters. *Check the sample (IAR)*

Control 1.2:

Reviews & maintains the information asset register on a regular basis.

Any Security Document will start with a document control section showing all the document history, from where you can verify that the document has been reviewed on a regular basis.



Document Control

Item	Description			
Document Title:				
Doc Ref.			Version:	1
Classification	○ Public	◉ Internal	○ Confidential	○ Secret
Status:	Current	**Type:**	DOC	
Release Date:	30/06/2019			
Revision Date:	15/10/2019			

Version No.	Date	Author(s)	Remarks
1.0	30/06/2019	John Smith	First Version of the Document
1.0	05/07/2020	John Smith	Reviewed Document

Document Review and Approval History

Document Control Sample

Control 1.3:

Assigns the information assets owner the responsibility of defining the proper access control to the information and ensuring periodic review of access in accordance with assigned classification level and the entity’s access control policy.

The information asset owner is usually the organization or the department.

Control 1.4:

Assigns the custodians the responsibility of maintaining the day to day operational tasks related to the information assets, while considering the higher authority of the assets by the owners.

The information asset custodian is usually the employee who is managing the asset which could be an excel file that include the customer information , the database admin or the server admin, this will be the responsible for the asset.

Control 1.5

Defines and implements an information classification scheme/process to be used within the entity based on information assets criticality, value, legal and protection requirements, etc.

Any organization should have a classification level that they are using for all their information and should be written to all their documents. This is important to identify the confidential information and provide them with the proper technical and physical control.

Control 1.6

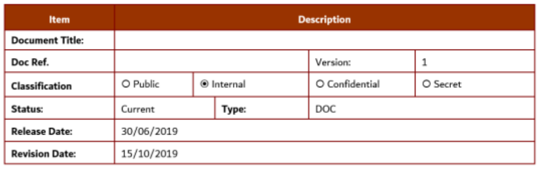
Develops, distributes, and maintains information classification policy and related procedures.

Your organization should have a policy that they are follow to classify the information, policy and procedure details and source will be covered in an upcoming domain in depth.

Control 1.7

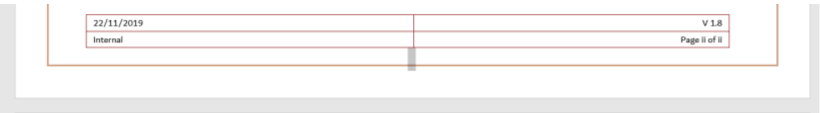
Defines and implements adequate labelling and handling controls for the information assets (electronic and physical); according to the requirements of each classification level, considering the handling requirements, storage procedures, distribution limitations, etc., for each information asset.

There is a difference between classification and labeling, classification is to follow a policy to be able to classify any document and distinguish between what is public, internal or secret while labeling is to add the classification on the document in a the document control, or the page footer or even as a stamp.



Item	Description			
Document Title:				
Doc Ref.			Version:	1
Classification	○ Public	● Internal	○ Confidential	○ Secret
Status:	Current	Type:	DOC	
Release Date:	30/06/2019			
Revision Date:	15/10/2019			

Classification shown in Document Control



22/11/2019	V 1.8
Internal	Page ii of ii

Classification shown in the page footor

Control 1.8

Develops, distributes and maintains procedure for the information assets labelling and handling requirements.

Control 1.9

Identifies and implements the required safety and security measures prior to the disposal of information or information assets based on their value, criticality and sensitivity.

Control 1.10

Develops, distributes and maintains clear procedure for the process of disposal of information and information assets, as part of the labelling and handling procedure.

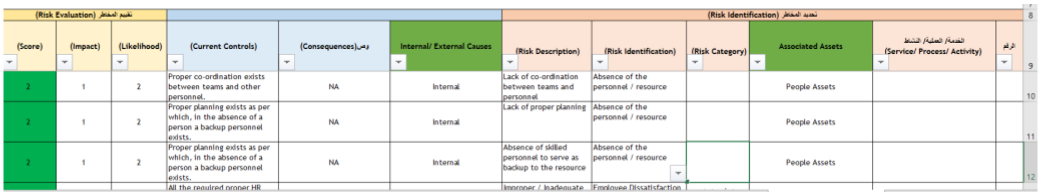
Control 1.10

Develops, distributes and maintains an acceptable use policy governing the acceptable use of information and assets.

Domain 2: Risk Management

Applicable: All company Departments.

Risk assessment is the second important steps in the ISMS implementation and any auditor will ask for the organization risk register during the ISMS audit.
In this phased you are not required to do a risk assessment yourself, as this is a not an easy process and need experience but by the end of this book you will have some basic skills to accomplish this task, you will need to manage the risk assessments.
One of the main factors used for a risk register is the Information asset register accordingly if the IAR was not done probably it will be reflected in the risk register



(Risk Evaluation) تقييم المخاطر						(Risk Identification) تحديد المخاطر					
(Score)	(Impact)	(Likelihood)	(Current Controls)	(Consequences)وص	Internal/ External Causes	(Risk Description)	(Risk Identification)	(Risk Category)	Associated Assets	الخدمة/ العملية/ النشاط (Service/ Process/ Activity)	الرقم
2	1	2	Proper co-ordination exists between teams and other personnel.	NA	Internal	Lack of co-ordination between teams and personnel	Absence of the personnel / resource		People Assets		
2	1	2	Proper planning exists as per which, in the absence of a person a backup personnel exists.	NA	Internal	Lack of proper planning	Absence of the personnel / resource		People Assets		
2	1	2	Proper planning exists as per which, in the absence of a person a backup personnel exists.	NA	Internal	Absence of skilled personnel to serve as backup to the resource	Absence of the personnel / resource		People Assets		
			All the required proper HR			Improper / Inadequate	Employee Dissatisfaction				

Risk Assessment

Your Role in this domain:

1- You need to make sure that each department has its own risk assessment that should be reviewed al least once a year and document control should be updated.
2- You need to make sure that all High / Meduim risks have been mitigated by departments employees and evaluate the evidence.
3- You need to make sure that all risks that was not mitigated has been added to the risk acceptance sheet and signed by management.

Control 2.1:
Develops a risk assessment methodology that aligns with the requirements of the entity's information security program/management system.

Control 2.2
Determines a periodic plan for conducting the risk assessment across the entity.

Control 2.3:
Identifies the criteria of acceptable risks as part of the risk assessment methodology.

Control 2.4:
Identifies the scope of the risk assessments, in terms of the business processes & respective information assets that will be included in the assessment.

Control 2.5:
Identifies threats and vulnerabilities pertaining to the identified assets.

Control 2.6
Plans and implements a periodic awareness of the risk assessment program across the entity.

Control 2.7:
Conducts a detailed risk assessment through identification & valuation of information assets & corresponding threats and vulnerabilities.

Control 2.8:
Analyses risks and prioritizes them based on the criticality, in order to set treatment plans and controls.

Control 2.9:
Determines and identifies the acceptable risks in accordance with the risk assessment methodology.

Control 2.10:
Documents the risk assessment results and approves it officially by the senior management or the Information Security Steering Committee.

Control 2.11
Selects the proper risk treatment plans (mitigate, avoid, transfer, etc.) for the identified risks.

Control 2.12
Determines and selects the appropriate security operational controls (under operational domains within this document) for mitigating the identified risks.

Control 2.13
Signs off and authorizes officially the implementation of the risk mitigations controls.

Control 2.14
Performs and immplements the mitigation controls for the risks identified.

Control 2.15
Reviews and monitors the implemented risk mitigation controls for effectiveness.

Control 2.16:
Documents the residual non treated risks with justifications and gets it signed off from the senior management along with the detailed plan for treatment at a later date.

Domain 3: Incident Management

Applicable: All company Departments.

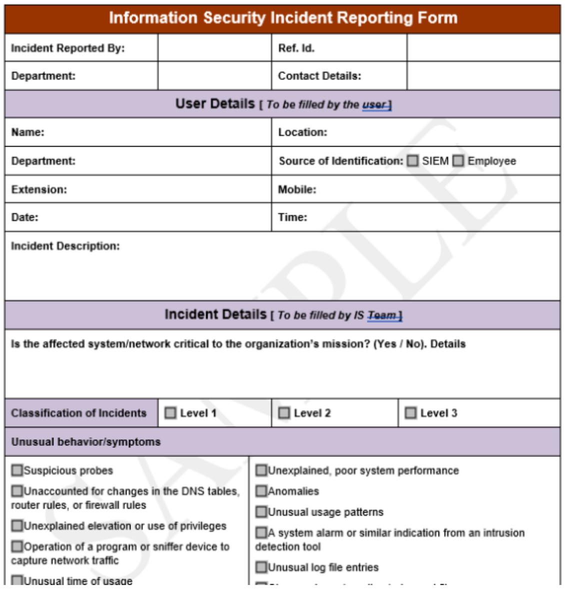
Any organization need to have an incident management policy that explain how they are dealing with security incidents.

Your Role in this domain:

1- Incident Management policy

2- Incident Register that log all the organization information security incidents

3- All Employees need have an awareness session about how to identify and report security incident.



Information Security Incident Reporting Form

Incident Reported By:		Ref. Id.	
Department:		Contact Details:	
User Details *[To be filled by the user]*			
Name:		Location:	
Department:		Source of Identification: □ SIEM □ Employee	
Extension:		Mobile:	
Date:		Time:	
Incident Description:			
Incident Details *[To be filled by IS Team]*			
Is the affected system/network critical to the organization's mission? (Yes / No). Details			
Classification of Incidents	□ Level 1	□ Level 2	□ Level 3
Unusual behavior/symptoms			

□Suspicious probes

□Unaccounted for changes in the DNS tables, router rules, or firewall rules

□Unexplained elevation or use of privileges

□Operation of a program or sniffer device to capture network traffic

□Unusual time of usage

□Unexplained, poor system performance

□Anomalies

□Unusual usage patterns

□A system alarm or similar indication from an intrusion detection tool

□Unusual log file entries

Information Security Incident Report

Control 3.1

Develops, distributes and maintains a formal policy and procedure for the management of information security incidents.

Control 3.2

Establishes a capability (incident response team) for the information security incidents response and handling across the entity.

Control 3.3

Assigns responsibility to all employees or any users dealing with the entity's information, through any means, for reporting promptly any observed or suspected information security incidents or weaknesses in systems or services, to the responsible entity's team.

Domain 4: Access Control

Applicable: All company Departments.

One of your main responsibilities as a Cyber Security Professional is to make sure that all the company systems has proper logical or physical access control according to their criticality which you can easily identify from the IAR

Your Role in this domain:

1- Access Control Policy.
2- Make sure that all company system are controlled with access control to prevent unauthorized access.
3- All logical Access Controls such as password need follow standards such as (*8 Characters, Complexity, Password expiration,….*)
4- Access Control need to be reviewed at least twice per year.

ACCESS TO INFORMATION REQUEST FORM

Government Dept.
Enrollment

Provide details regarding the information being sought

Method of access preferred □ receive copies of originals □ Examine originals in government offices

Name of applicant

Street/Box Address

City or town

Province/Territory Postal Code Telephone No.

This request for access under the NND Privacy Act and Access to Information Act is being made by □ a Canadian citizen, permanent resident or another individual present in Canada, or □ a corporation present in Canada

Access Control request

Control 4.1

Develops, distributes and maintains an access control policy that addresses all security requirements for the implementation of an effective access control within the entity.

Control 4.2

Develops, distributes and maintains an access control procedure that provides implementation details for access control, based on role-based access control.

Control 4.3

Maintains a secure repository of all information systems access controls.

Control 4.4

User Access Control

a. Defines and Implements a process for users registration, de-registration, and users access privileges modification, disabling or removal, etc.
b. Provides each user with a unique identifier (user ID) for their individual business use only.
c. Implements a unified users ID standard across the entity.
d. Implements a proper authentication technique for the validation of claimed identities of users regarding access being onsite and remote.

e. Develops, distributes, and maintains appropriate authentication policy(ies) (e.g. a password management policy that clearly addresses the password allocation process, users' responsibilities on passwords use and the recommended password structure, etc.).

Control 4.5
Identifies the categories of users requiring regular and special privileges through ensuring the availability of the following:
A- A valid and approved access authorization.
B- Intended system usage.
C- Other attributes as required by the entity or associated missions/business functions.
D- Utilization of access accounts with special privileges must be restricted for their intended purpose."

Control 4.6
Maintains records of all users' access privileges, and monitors them on a continuous basis;

Control 4.7
Limits the number of special/high privileged user IDs to those individuals who absolutely must have such privileges for authorized business purposes.

Control 4.8
Implements proper security and independent monitoring controls over the usage of special or high privileged IDs.

Control 4.9
Implements proper process for guest and temporary user IDs request and employs automated user IDs termination

Control 4.10
Allocates access privileges on a restricted basis while employing least privilege concept and separation of duties

Control 4.11
Employs a process for review and re-authorization of user access rights on a periodic basis, as defined by the entity.

Control 4.12
Network Access Control

a. Develops, distributes and maintains a policy for network access control, which covers details about accessible networks and networks services, authorization process for granting network access, etc.
b. Defines a process for authorizing, activating and terminating any network connections in the entity.
c. Implements a proper network access control tool/method for network equipment/devices connectivity detection, identification and authentication.
d. Implements proper authentication tool for remote access connections.
e. Manages and controls access to configuration ports on network equipment/devices.

a. Implements proper segregation controls on the different types of networks (internal, external, wireless, IP telephony, etc.)
b. Implements proper security and operational controls for any network connections beyond the entity’s direct control.
c. Operating System Access Control
d. Manages and controls access to operating systems through secure log-on process.
e. Assigns each user with a unique user ID and apply the proper authentication method for identity verification.
f. Limits the use of generic user IDs to only exceptional and business justified circumstances, and implements the proper accountability technique for such use.
g. Implements an entity wide authentication mechanism to enforce various authentication controls.
h. Manages and controls the use of utility programs.
i. Implements session time-out controls to prevent unauthorized access.
j. Implements lock-out policy.
k. Restricts connection times for critical information systems and applications.
l. Records and continuously reviews logs of administrators system IDs
m. Applications Access Control
n. Provides access to applications based on job responsibilities and business justifications, in alignment with the entity access control policy/procedure.
o. Implements proper physical or logical isolation controls for highly critical information systems and application environments.
p. Remote Access Security
q. Develops, distributes and maintains a policy addressing remote access to the entity's resources.
r. Enforces formal authorization prior to remote access connections.
s. Ensures that adequate security controls are implemented on the VPN client machines, such as authentication, encryption, antivirus software, personal firewalls, session timeout, etc.
t. Provides remote access users with access to the services that they have been specifically authorized to use.
u. Monitors and periodically reviews the remote access connections logs.
v. Mobile Computing
w. Develops, distributes and maintains a formal policy governing the appropriate use of mobile computing and communication facilities.

Control 4.13
Implements appropriate security controls to protect against the risks of mobile computing and communication facilities’ usage, such as:

a. Implement encryption mechanisms to protect sensitive information
b. Ensure secure handling for the portable computing devices.
c. Implement proper mechanisms to disable portable computing devices when lost or stolen.
d. Proper data backup procedures for the portable computing devices."

Control 4.14
Wireless Access Management

a. Develops, distributes and maintains a formal policy on the wireless network usage.
b. Authorizes formally the wireless access to the network prior to any connection.
c. Implements the proper authentication controls for the wireless access.

d. Enforces proper security controls for wireless connections to the entity's network and establishes usage restrictions and implementation guidance for such use.
e. Provides wireless connection users with access to services that they have been specifically authorized to use.
f. Monitors continuously the unauthorized wireless access to the network.

Control 4.15
Physical Access Policy and Procedure

a. Enforces formal authorization prior to physical access to any facilities with information processing resources
b. Physical Security Controls
c. Enforces appropriate physical access control perimeters for all physical access points to the entity.
d. Verifies and ensures that only authorized employees are provided access to protected areas.
e. Controls entry to the data centre, or any facility containing information systems using physical access control devices.
f. Controls and monitors physical access to the information processing facilities areas or any other public areas.
g. Safeguards and enforces adequate protection controls on physical access devices.
h. Keeps inventory of all physical access devices owned by the entity.
i. Reviews logs of physical access on a regular basis.
j. Deploys mechanism to monitor the movement of employees & non-employees within the entity.
k. Enforces formal authorization prior to logical access required by external party through deploying a "need to know" criteria.
l. Controls physical access to any areas that includes information systems and other areas such as delivery, loading, or any other points where unauthorized personnel may enter by authenticating visitors before authorizing access.
m. Authorizes, monitors, and controls entering and exiting the data centre facilities or any other public areas and maintains such records.
n. Places adequate security controls on accessing all soft/hard documents/information in alignment with its criticality.
o. Determines and assigns the needed access rights for the protected documents/information.
p. Sets a clear policy on archiving of documents, along with defining a clear retention period for archiving, and supplements it with procedures and guidelines for the details of implementation and usage.
q. Employs a clear procedure for the disposal of documents, with assigning clear authorization and responsibilities.
r. Implements audit trails in information processing systems, as necessary.
s. Logs, maintains and periodically reviews logical and physical access control lists.

Domain 5: Communication and Operation

Technology & Operations Capacity Management

Applicable to IT Department

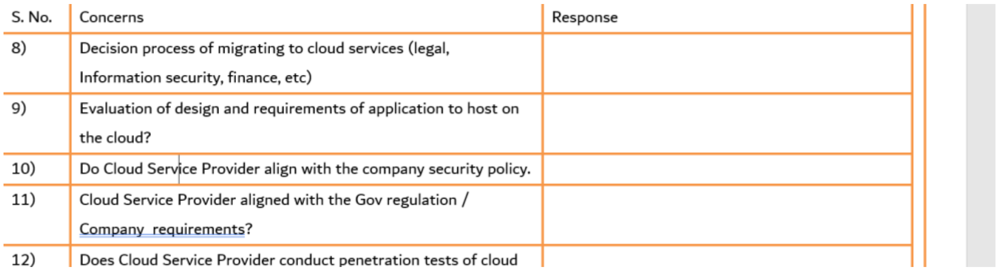
Confirming the Information Technology department are following standards, best practice procedures are very important.

Your role in this domain:

1- Use Cyber Security Checklist from our Cyber Security Portal to evaluate security standards in all IT Department systems.

2- Another website that can help you to evaluate security standards in all IY Department is https://www.cisecurity.org/cybersecurity-tools/

3- You need understand that you will not be the one who are configuring the technical equipment and system , you just need to make sure that the technical control are implemented by the right team.



S. No.	Concerns	Response
8)	Decision process of migrating to cloud services (legal, Information security, finance, etc)	
9)	Evaluation of design and requirements of application to host on the cloud?	
10)	Do Cloud Service Provider align with the company security policy.	
11)	Cloud Service Provider aligned with the Gov regulation / Company requirements?	
12)	Does Cloud Service Provider conduct penetration tests of cloud	

Check list

Control 5.1

Ensures advanced planning and preparation for availability of adequate capacity and resources for the information processing systems and their technology components.

Control 5.2

Conducts an annual projection review of capacity requirements and resources for the information processing systems and their technology components.

Control 5.3

Documentation of Operational Procedures

Control 5.4

Develops and maintains a complete set of operating procedures documentations of all information processing systems detailing inputs, outputs and dependencies.

Control 5.5

Documents and maintains up to date baseline configurations manuals of all information processing systems including an inventory of constituent system components.

Control 5.6

Places adequate security protection controls on the documentation of operational procedures of all critical information processing systems, through defining a clear distribution list and permitted users and ensures their availability to authorized users whenever required.

Control 5.7
Change Management

Control 5.8
Develops, distributes and maintains a formal documented change management policy that defines the overall change management process employed by the entity, outlining roles and responsibilities of different business owners.

Control 5.9
Supplements, as necessary, the change management policy with a detailed procedure to facilitate the implementation of the change and configuration management process and provide guidelines for all users.
"Implements a change management process that must include the following details, as a minimum:

Domain 6: Business Continuity Planning

Applicable: All Department.

Control 6.1
Develops and periodically conducts a business impact analysis for all information systems and processes in order to define and determine the impact of potential operational failures.

Control 6.2
Sets and accounts the responsibility of the Business Impact Analysis to the senior management, with involvement from all affected divisions.

Control 6.3
Organizes and accounts responsible a committee of senior management and business owners for the business continuity plan, with defined and clear responsibilities.
"Develops, maintains and periodically tests and reassesses a business continuity plan that covers the following:
A-The plan should be based on the Business Impact Analysis and Risk Assessment.
B-The plan should address requirements for resilience, alternative processing and recovery capability of all critical business and IT services.
C-The plan should cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach."

Control 6.4
Designs a business continuity process in a manner to reduce the impact of a major disruption on key business functions and processes.

Control 6.5
Identifies the most critical business systems and applications in accordance with the risk assessment conducted by the entity.

Control 6.6
Deploys a proper recovery plan for the identified critical business systems, as the entity's operations specify.

Control 6.7
Determines the type of recovery scheme that is applicable for its requirement.

Control 6.8
Exercises and periodically tests the decided recovery plan.
Implements disaster recovery sites in case their business systems result in a major loss for the whole government, through using an effective approach based on feasibility studies.

Control 6.9
Backup and Storage Policy and Procedure
"Develops, distributes and maintains a formal documented backup, storage and retention policy that includes:
A.users' responsibilities.

B.requirements for backup and recovery systems.
C.backup protection controls
D.legal and business requirements (e.g. recovery point objective, recovery time objective, etc.)"

Control 6.10
Supplements, as necessary, the backup policy with a detailed procedure for backup and storage specifications and implements them

Control 6.10
Backup Testing & Restoration

a. Plans and executes a periodic testing and restoration process of all backup and storage media.
b. Maintains, exercises and tests in a periodic manner the Business Continuity Plan, Business Impact Analysis, Backup and Restoration, and Disaster Recovery Plan.

Domain 7. IS Acquisition, Development

Applicable: All Department.

Control 7.1

Develops, distributes and maintains a formal documented policy and procedures for addressing the entity's requirements for ensuring the security on any in house developed or external party applications regarding the Acquisition, Development and Management of information systems.

Control 7.2

Develops a System Development Life Cycle (SDLC) methodology and officially incorporates information security requirements within it.

Control 7.3

Defines and documents information security requirements in all business cases, requests for proposals and work requests, related to acquisitioned or in house developed information systems, in order to ensure integrating adequate security controls and minimize any cost related to security, and ensure that sufficient resources are allocated to implement these controls.

Control 7.4

Develops and approves the information systems design documents addressing the security requirements.

Control 7.5

Develops the secure coding standards for information systems software development.

Control 7.6

Designs the security architecture for the development & deployment of information systems. Implements adequate configuration management process during information systems design, development, implementation and operation.

Control 7.7

Conducts proper testing to validate integrity of data input controls on information systems/applications. Integrates validation checks into information systems/applications processing to detect and any loss of integrity in processed information.

Control 7.8

Identifies integrity requirements for processed messages and information in the information systems/applications and ensures implementing adequate controls to protect it.

Control 7.8

Conducts proper testing to validate integrity of data output from information systems/applications.

Control 7.9

Implements restrictive information system procedures on the installation of software in the operational information systems environments.

Control 7.10

Implements proper protection controls on the use of testing data.

Control 7.11
Implements proper access control procedures on information systems/application source codes.

Control 7.12
Implements proper change management controls on the software development processes.

Control 7.13
Tests and verifies the operational status of all information systems/applications after implementing any change.

Control 7.14
Implements proper controls to limit the risk of changes to software packages.

Control 7.15
Implements proper controls to prevent information leakage in all information system/application environments.

Control 7.16
Implements proper security controls on outsourced software development.

Control 7.17
Performs technical security reviews and vulnerability tests in order to periodically assess the information systems/applications security against latest threats and vulnerabilities.

Control 7.18
Conducts periodic code reviews on all information systems/applications developed in house or by an external party.

Control 7.19
Deploys the information systems/ applications into production environment after successful completion of testing & fixing of defects identified.

Control 7.20
Implements security sign off process to confirm the proper implementation of security controls on all

Control 7.21
information systems/applications prior to deployment.

Control 7.22
Develops, distributes and maintains a policy on the use of cryptography and key management wherever applicable.

Control 7.23
Implements proper cryptography and key management mechanisms as required by the entity.

Control 7.24
Implements proper protection and security controls on all cryptographic keys used by the entity.

Domain 8: Environmental & Physical Security

Applicable: All Department.

Control 8.1
Controls humidity and temperature level on information processing facilities, and continuously monitors it.

Control 8.2
Implements proper fire suppression and detection systems.

Control 8.3
Implements proper control for monitoring water leakage at the physical information processing facilities.

Control 8.4
Implements adequate physical security mechanisms on offices, data centers, and other working areas, based on criticality of such areas.

Control 8.5
Provides employees with proper guidelines and awareness on the implemented protection controls in the working areas.

Control 8.6
Develops, distributes and maintains a clear desk and clear screen policy that addresses users' responsibilities on securing desks, working areas, and electronic user devices (e.g. PCs, printers, etc.).

Control 8.7
Places information systems related equipment in secure and protected locations

Control 8.8
Protects power equipment and cabling of information processing facilities from damages.

Control 8.9
Implements UPS (uninterruptable power supply) systems to avoid power failures where deemed necessary.

Control 8.10
Implements proper maintenance procedures on all information processing facilities.

Control 8.11
Implements proper protection controls over equipment and information processing facilities residing off site.

Control 8.12

Implements adequate security controls on the disposal or re-use of any equipment or information processing facility.

Control 8.13

Conducts proper testing and assessment periodically over all implemented environmental and physical protection controls.

Domain 9: Roles and Responsibly

Applicable: HR Department / All Department

Control 9.1
Ensures that all employees, contractors and outsourced employees are provided with information security awareness programs on a regular basis

Control 9.2
Implements proper security controls on the process of terminating or changing employment.

Control 9.3
Communicates termination responsibilities to the terminated employee in relation to confidentiality agreements and employment contracts.

Control 9.4
Implements a process for returning all entity's assets upon termination of employment.

Control 9.5
Implements a process for revoking or changing access rights and privileges upon termination or change of employment.

Control 9.6
Implements a process for returning all entity's assets upon termination of employment.

Control 9.7
Implements a process for revoking or changing access rights and privileges upon termination or change of employment.

Domain 10: Compliance and audit

Applicable: Legal Department /All Department.

Control 10.1
Ensures compliance with all laws and regulations.
 security."

Control 10.2
Identifies the laws or regulations that are applicable to the entity’s scope of services.

Control 10.2
Develops, distributes and maintains a formal Intellectual Property Rights (IPR) policy that defines the

Control 10.2
legal obligations pertaining to the use of information assets (e.g. hardware, software, etc.)

Control 10.3
Ensures compliance with Intellectual Property Rights (e.g. software license agreements).

Control 10.4
Prohibits employees from manipulating, making or distributing unauthorized copies of copyrighted/licensed materials, software or applications.

Control 10.5
Conducts continuous awareness sessions on the requirements of protecting private data and information for the responsible personnel.

Control 10.6
Restricts, minimizes and monitors access to personal and private data, and applies proper controls on the process of collecting, processing and transmission of personal data, which should be on "a need-to-know" basis.

Control 10.7
Sets proper accountability procedures in the event of any private information and personal data leakage.

Control 10.8
Conducts periodic reviews to verify compliance of the implemented information security policies and procedures.

Domain 11 : IS Assurance and performance

Applicable: Management .

Control 11.1

"Develops, selects and implements a set of Information Security Key Performance Indicators (KPIs) that are:
A.In support of the government entity strategic and operational planning processes to secure the entity's mission.
B.Integrated into the annual reporting of effectiveness of the government entity's information security controls.
C.Reviewed regularly and used to support policy, resources allocation, budget decisions, and as an assessment of information security program posture and operational risks.
D.Used to address issues and deficiencies and take corrective actions such as revising policies and procedures, or provide information security trainings for employees.
E.Built from inputs of a variety of entity's stakeholders, such as IT operations, incident response team, human resources, physical security team, or others using different data sources, such as risk assessments, penetration testing, and continuous monitoring.
F.Yielding quantifiable information for comparison purposes, while using formulas for analysis, and tracking changes using the same point of reference. Percentage, average or absolute numbers can be used, depending on the activity being measured. H.Measured over consistent and repeatable information security processes."

Control 11.2

Integrates information security measurements and Key Performance Indicators(KPIs) in entity’s business processes and assigns business process owners the responsibility of achieving such measures.

Control 11.3

Approves the entity’s information security measurements and Key Performance Indicators(KPIs) by the higher management of the entity.

Control 11.4

Conducts periodic reviews on the results of information security measurements.

Control 11.5

Records actions and events that could have an impact on the effectiveness or performance of the Laws and Regulation.

Control 11.6

Implements, as necessary, an integrated dashboard (or incorporates into an existing entity Performance

Control 11.7

Measurement tool) for combining all measured information security KPIs to be reviewed and monitored in a periodic manner, by the senior management and the responsible stakeholders, in order to ease the decision making process, and facilitate the overall planning for the information security program/management system.

Domain 12: IS Management and governance

Applicable: Management.

Control 12.1

The board of directors should accept the responsibility of information security and present commitment towards it.

Control 12.2

The entity's board of directors is assigned the responsibility of overseeing a properly managed and implemented information security program/management system and reviewing risk assessment reports.

Control 12.3

Director General/ CEO

"The CEO or Director General who might be reporting to the board of directors has responsibility for:
A- Accepting and endorsing the overall responsibility of information security
B- Enforcing organization wide information security management system
C- Enforcing information security policies implementation across the entity
D- Overseeing and monitoring divisions compliance to information security management system and information security policies.
E- Enforcing accountability towards information security"

Control 12.4

Information Security Steering Committee

"An information security steering committee should be established and should include representatives from each division in the entity. The steering committee should maintain the following roles and responsibilities:
A- Supervise and ensure the implementation of an Information Security Management System and its controls across the Entity.
B- Conduct periodical reviews on the implementation of ISMS and any information security controls and objectives
C- Review and maintain periodically the information security policies and procedures that are implemented in the entity
D- Promote Information Security culture within the Entity
E- Ensure that information security methodology is part of all business
processes and any new initiatives in Information Technology division.
F- Follow up and review both internal and external audits that are to be conducted in accordance with the ISMS.
G- Review and approve the information security risk assessment methodology that is used across the entity.
H- Ensure that adequate resources are provided to implement, support and operate the information security management system.
I- Make recommendations for both corrective and preventive actions based on the risk assessment approach
J- Review the Information Security Incidents and their responses
K- Ensure that recommendations approved by the committee are implemented"

Control 12.5
Senior Management
"The entity's senior management is assigned the following responsibilities:
A- Ensure that each employee understands his/her information security-related responsibilities and acknowledges that he/she understands and intends to comply with those requirements by having them review the Information Security Policy
B- Determine the criticality and business risk of their information systems and information assets.
C- Periodically assess information assets and their associated risks.
D- Determine and review the privileges related to their information assets and information systems on a periodic basis
E- Implement information security policies and procedures to cost-effectively reduce risk to acceptable levels
F- Periodically, ensure conducting technical security testing on the information systems
G- Report any evidence of information security compromise or any suspicious activity that could potentially expose, corrupt or destroy information to the entity's information security responsible personnel.
H- Respond to information security incidents"

Control 12.6
Employees
Senior management assigns the coordination of information security activities to certain employees acting as Information security champions/representatives/coordinators across all divisions.

Control 12.7
The entity assigns all employees responsible for adhering to the information security policies/processes/program and for reporting any security breaches or incidents to their direct management.

Control 12.8
Review of Information Security Policy

Control 12.9
Sets a clear responsibility for a regular review of the information security policy, which is to be done in a frequency of at least once a year, or along with any changes that the entity might undergo.
Reports any update or review of the information security policy to the senior management and sets the declaration of changes to the entity's CEO/Director General.

Control 12.10
Designs, develops, and implements an information security awareness program (that is categorized based on job roles, divisions or as the entity specifies) which is composed of targeted information security awareness creation activities.

Control 12.11
Provides basic information security training and awareness to all personnel within the entity, as part of initial training for new users, when required by information systems changes, and in an entity specified periodic intakes.

Control 12.12
Provides adequate information security trainings for the employees taking part in operating the information security program/management system within their respective business areas.

Control 12.13
Designs the information security awareness materials to be in accordance to the entity's daily business operation's security risks, and to provide rules to follow in order to reduce possible risks.

Control 12.14
Develops continuous security awareness surveys to measure the awareness level of all personnel, in order to point out common mistakes or misunderstandings in information security concepts, and to improve the overall awareness program.

Control 12.15
Documents information security training and awareness attendance records for all personnel.

Control 12.16
Develops, and regularly reviews a non-disclosure or confidentiality agreement which is signed by all employees and external parties, and addresses in legally enforceable terms, the need for all

Control 12.17
Government Entity to protect the government information from being leaked internally or externally, and emphasizing the "need to know" concept.

Control 12.18
Educates personnel and makes them aware of the confidentiality of government information and how information leakage, written or spoken, can impact the entity.

Control 12.19
Determines and assesses risks related to its relations with external parties, such as customers, external party services providers, business consultants, temporary employments, etc. This also includes outsourcing and cloud services providers.

Control 12.20
Selects and applies the appropriate information security controls and measures to control the identified risks.

Control 12.21
Develops and implements the required agreements to secure relations with the external parties, including integrity, availability and confidentiality.