INFO6027

Information Security Planning

Week 9

InfoSec Programs, ISO certifications, and SETA

FANSHAWE

Housekeeping

- **Final Exam on Wed Dec 14 at 10:00 am in R 1019**
- **Assignment #3** has been posted.

Agenda

- Discuss:
- Assignment 3
- Cloud Native Transformation
- Week 9
- Test 2 Review - scheduled for Nov 15. Material from Week 6 to 9

Security Planning in the News…

- **The Workaday Life of the World's Most Dangerous Ransomware Gang - https://www.wired.com/story/conti-leaks-ransomware-work-life/**

- **Hundreds of GoDaddy-hosted Websites Backdoored in Single Day**
- The backdoor infecting all sites is a 2015 Google search SEO-poisoning tool implanted on the wp-config.php to fetch spam link templates from the C2 that are used to inject malicious pages into search results. https://cyware.com/category/breaches-and-incidents-news

- **2,113 Mobile Apps Found Exposing User Data Via Cloud Misconfigurations**
- Mobile applications with tens of millions of downloads are leaking sensitive user data due to the misconfiguration of back-end cloud databases, according to research by Check Point. https://www.infosecurity-magazine.com/news/thousands-mobile-apps-expose-data/?&web_view=true

- **SolarWinds Warns of Attacks Targeting Web Help Desk Instances**
- SolarWinds warned customers of attacks targeting Internet-exposed Web Help Desk (WHD) instances and advised removing them from publicly accessible infrastructure (likely to prevent the exploitation of a potential security flaw). https://www.bleepingcomputer.com/news/security/solarwinds-warns-of-attacks-targeting-web-help-desk-instances/?&web_view=true

What we will cover today…

- **Organizing for Security** (Security in very large, large, medium, and small sized organizations)
- **Placing InfoSec** within an organization
- Components of the **Security Program**
- InfoSec **Roles**/Titles and **Responsibilities**
- ISO 27001/27002 **certification**
- Implementing **Awareness Programs** (SETA part 1)

Learning Objectives

Developing and Implementing an Information Security Program

(a different kind of ISP!)

- Upon completion of this material, you should be able to:
  - –Explain the **organizational approaches** to information security
  - –List and describe **the functional components** of an ISP/security management system
  - –Evaluate the **internal and external factors** that influence the activities and organization of an information security program
  - –**ISO 27001 Certification** overview
  - –Describe the **ISO 27001 Mandatory Documents**
  - –List and describe the typical **job titles** and functions in the ISP
  - –Describe the components of a security **awareness program**

Introduction – What is an I.S.P.?

- An InfoSec Program is comprised of InfoSec **elements**. It blends the organization's **strategic, operational, and tactical** areas.
  - *Remember these three from week 8? Remember ISMS?*
- Describes "*the entire set of activities, resources, personnel, and technologies used by an organization to manage the risks to its information assets*"
- The term "information security **program**" is used here to describe the **structure and organization** of the effort to manage **risks to an organization's information assets**.

Organizing for Security

Organizing for Security

- Lots of variables involved in ***structuring*** an information security program
  - –*Organizational culture* (What is our attitude toward infosec?)
  - –Size of the organization
  - –Security personnel (staffing) budget
  - –Security capital and operational budgets
- As organizations **increase in size**…

1. Security departments often do not keep up with the increasingly complex organizational structure
2. budget allocation **per user** decreases
   - ***BUT THIS IS CHANGING…. ANY IDEA WHY?***

Organizing for Security (cont'd)

- **Very large** organizations
  - –More than **10,000 computers**
  - –Security budgets often grow slower than IT budgets
    - –What is the role of advocacy in budgets?
  - –Even with a large budget, the average amount spent on security per user is *still* smaller than any other type of organization
    - Small organizations spend more than **$5,000 per user** on security; very large organizations spend about 1/18th of that, roughly **$300 per user. But this is changing.**
    - **Security accounts for just 5.7% of IT spend: Gartner https://www.cybersecuritydive.com/news/security-budget-gartner/587911/**
    - Companies in the software publishing and internet services industry spend the most on security, 9.5%, followed by banking and financial services with 7.6% spend, and government (state and local) with 5.7% of the IT budget.
  - –Do a better job in the policy and resource management areas
  - –Only 1/3 of organizations handled incidents according to an Incident Response plan

Organizing for Security (cont’d)

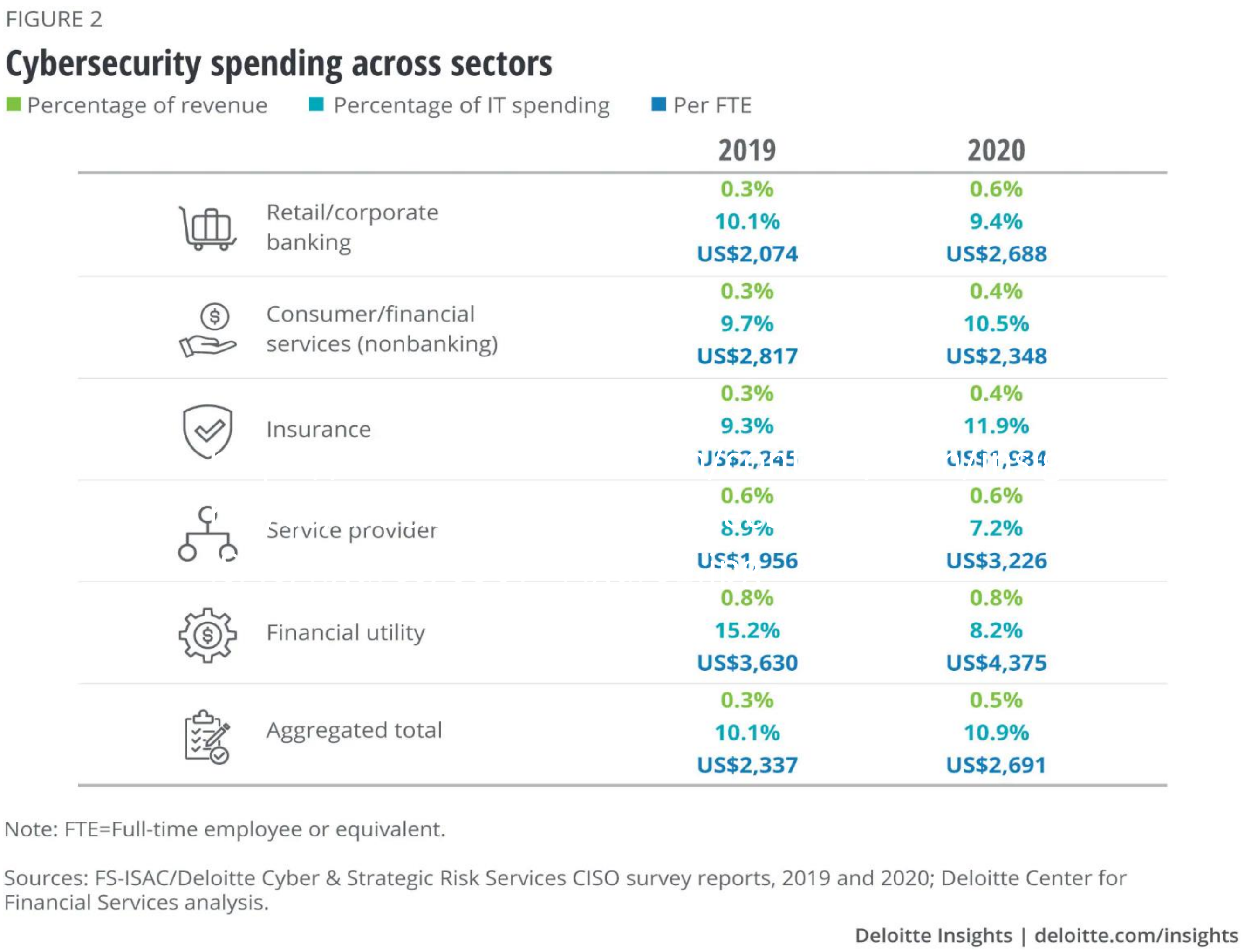


FIGURE 2

Cybersecurity spending across sectors

🟩 Percentage of revenue 🟦 Percentage of IT spending 🟦 Per FTE

	2019	2020
Retail/corporate banking	0.3% 10.1% US$2,074	0.6% 9.4% US$2,688
Consumer/financial services (nonbanking)	0.3% 9.7% US$2,817	0.4% 10.5% US$2,348
Insurance	0.3% 9.3% US$2,245	0.4% 11.9% US$1,984
Service provider	0.6% 8.9% US$1,956	0.6% 7.2% US$3,226
Financial utility	0.8% 15.2% US$3,630	0.8% 8.2% US$4,375
Aggregated total	0.3% 10.1% US$2,337	0.5% 10.9% US$2,691

Note: FTE=Full-time employee or equivalent.

Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2019 and 2020; Deloitte Center for Financial Services analysis.

Deloitte Insights | deloitte.com/insights

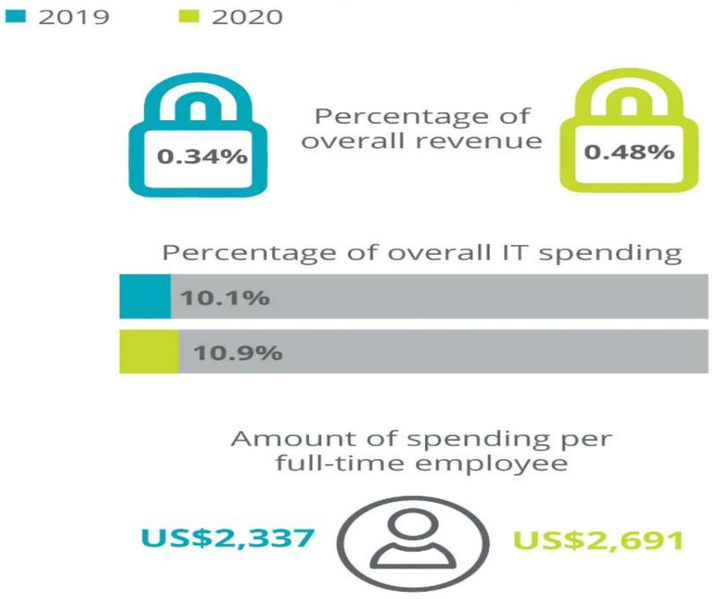
https://www2.deloitte.com/content/dam/insights/us/articles/6507_Cybersecurity-FS-ISAC/figures/6507_Figure1.jpg

Organizing for Security (cont’d)

FIGURE 1

Companies continue to spend more on cybersecurity

Overall cybersecurity spending benchmarks



Sources: FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO survey reports, 2019 and 2020; Deloitte Center for Financial Services analysis.

Deloitte Insights | deloitte.com/insights

https://www2.deloitte.com/content/dam/insights/us/articles/6507_Cybersecurity-FS-ISAC/figures/6507_Figure1.jpg

Organizing for Security

- **<u>Large</u>** organizations
  - –Have **1,000 to 10,000 computers**
  - –Security approach has often matured, integrating planning and policy into the organization's culture
  - –Do not always put large amounts of resources into security
    - Considering the vast numbers of computers and users often involved
  - –Tend to spend proportionally less on security

- Use more Groups/Committees/Teams
  - Smaller organizations typically create **fewer groups than larger ones,** often having only **one general group** of specialists

Security in Large Organizations

- One approach is to separate functions into **4 areas**:
  1. Functions performed by **non-technology business units** outside of IT (ex. legal and training)
  2. Functions performed by IT **groups outside of the information security area** (ex. Centralized authentication, SysSec admin, NetSec admin
  3. Functions performed within information security department as **customer service** (Risk Assessment, systems testing, IRP, DRP, performance measurement, VA)
  4. Functions performed within the information security department as **compliance**. (ex. Policy, Compliance/Audit, Risk Management)

Security in Large Organizations

- The CISO has responsibility for information security functions
  - CISO should ensure tasks are adequately performed somewhere within the organization (not always in IT!)
- The deployment of full-time security personnel depends on:
  - **Sensitivity** of the information being protected
  - Industry **regulations** (and relevant **legislation**)
  - General **profitability** (what the company can afford)
  - A Vostrom report (2010) indicated on average InfoSec spending constituted roughly ***10% of overall IT budgets.***

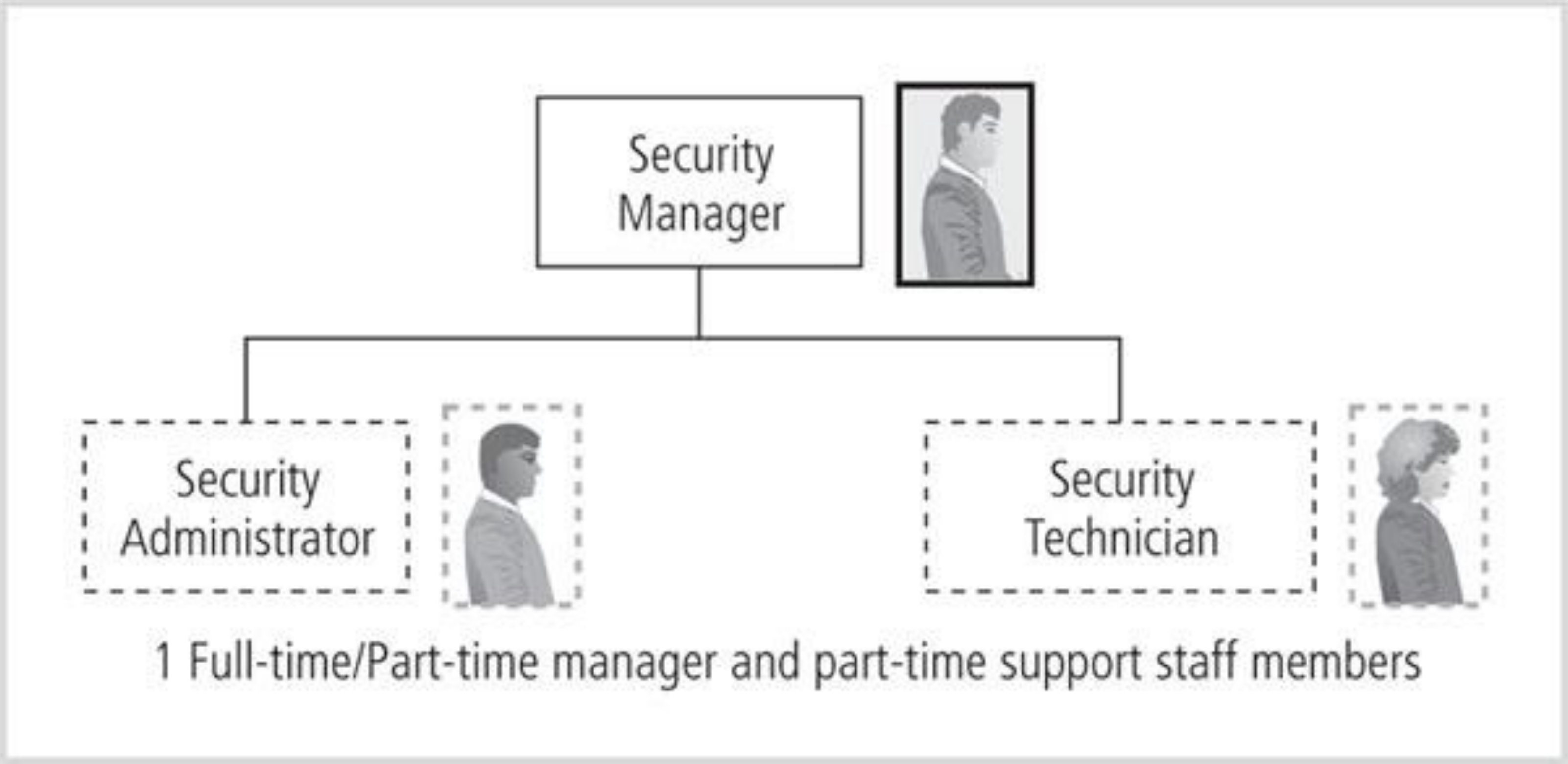
(http://www.infosecisland.com/blogview/8327-How-Many-Information-Security-Staff-Do-We-Need.html)

Security in Large Organizations

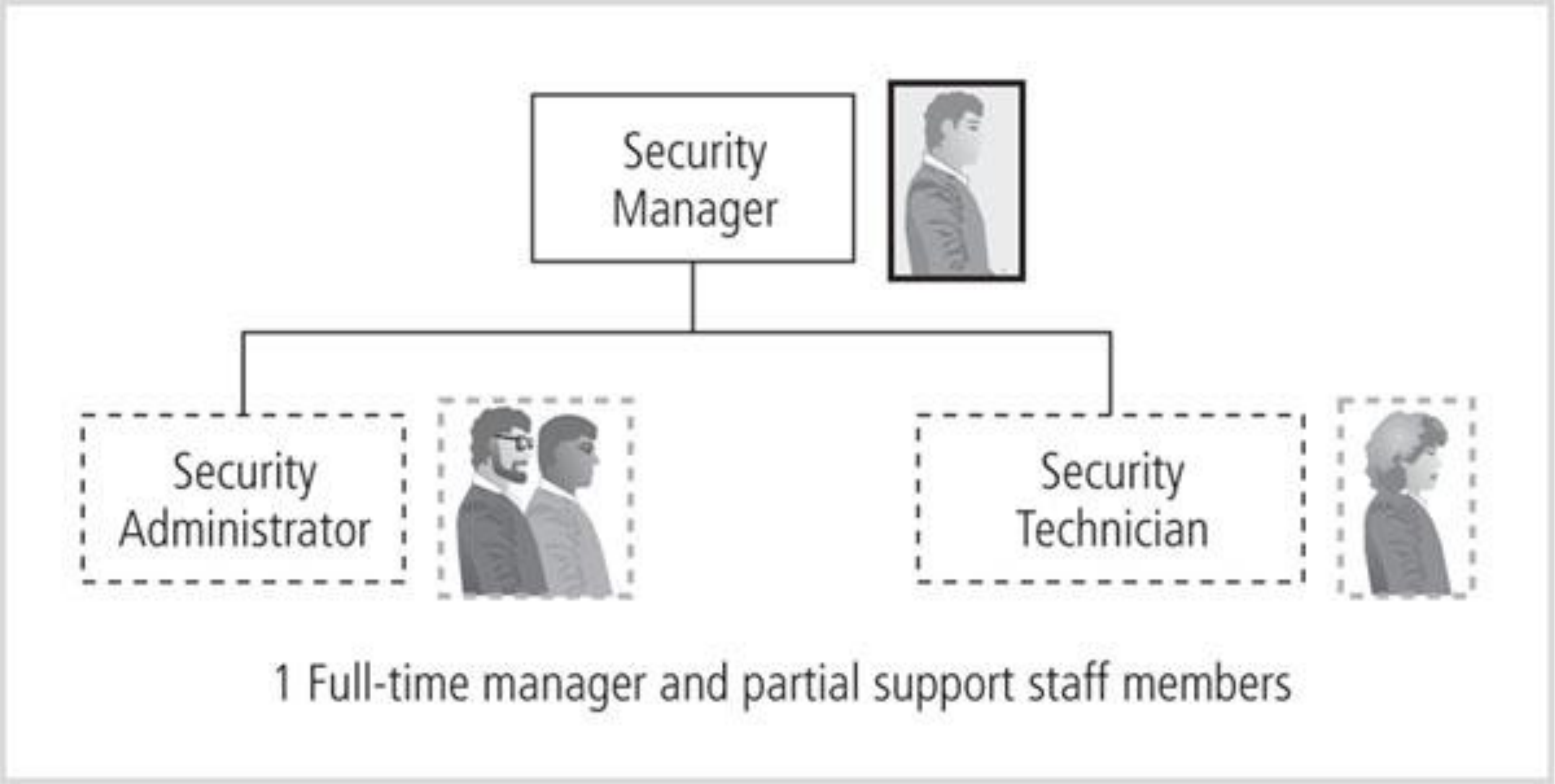
- The more money the company can dedicate to its personnel budget, the more likely it is to maintain a large information security staff.

- Let’s take a look at the differences in org charts depending on the size of the organization….

In a small sized organization

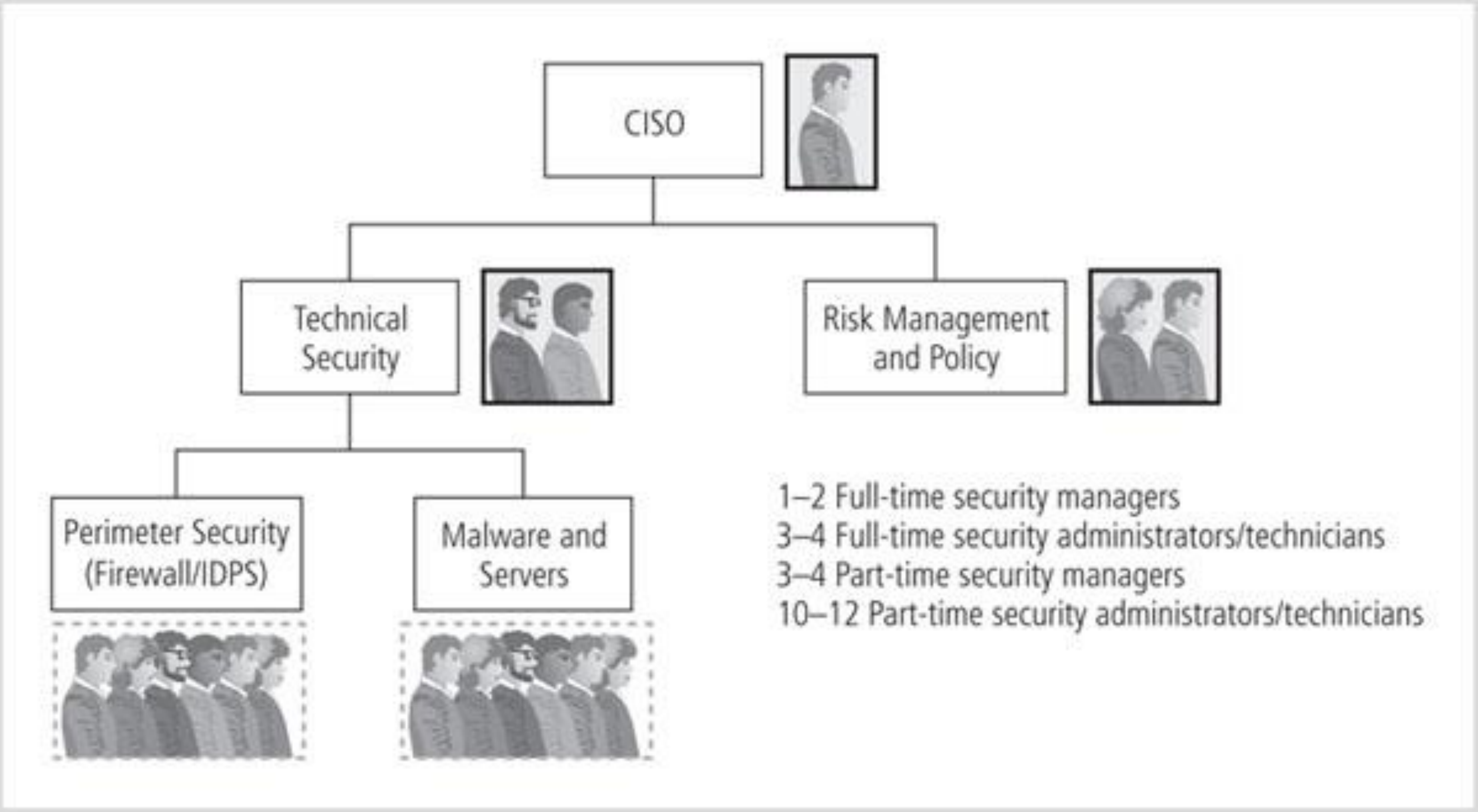

Security Manager
Security Administrator
Security Technician
1 Full-time/Part-time manager and part-time support staff members

In a medium sized organization



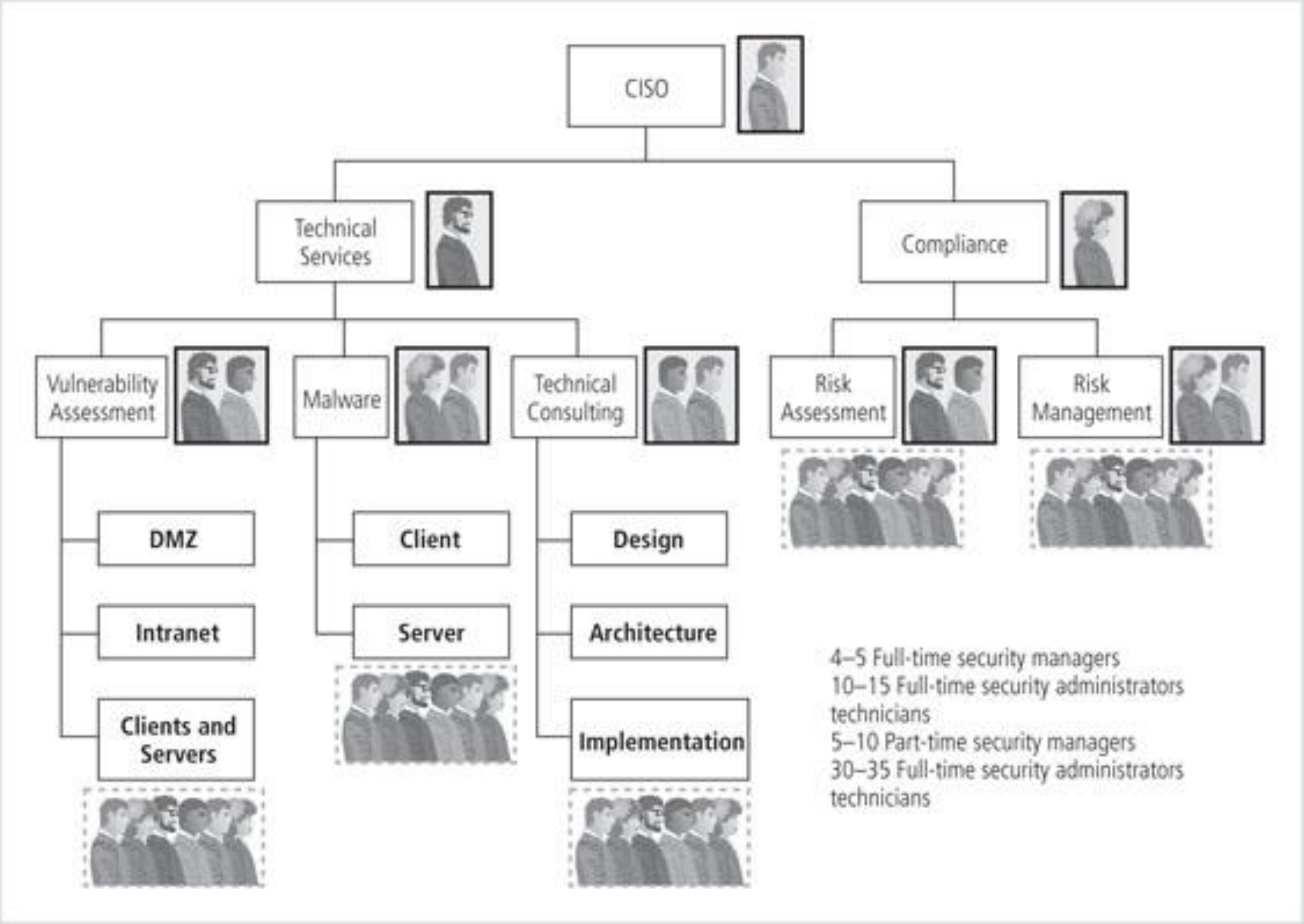
1 Full-time manager and partial support staff members

In a large organization


CISO
Technical Security
Risk Management and Policy
Perimeter Security (Firewall/IDPS)
Malware and Servers

1–2 Full-time security managers
3–4 Full-time security administrators/technicians
3–4 Part-time security managers
10–12 Part-time security administrators/technicians

In a very large organization



Security in Medium-Sized Organizations

- **Medium-sized organizations**
  - –Have between 100 and 1000 computers
  - –Have a smaller total budget
  - –Have *same sized security staff as the small organization, but more full-time employees and a **larger need***
  - –May be large enough to implement a multi-tiered approach to security
    - With fewer dedicated groups and more functions assigned to each group
  - –Tend to **ignore** some security functions
  - –Must rely on help from other IT staff for plans and practices
  - –Ability to set policy, handle incidents, and effectively allocate resources is **worse than any other size**
  - –Usually **1 full-time** employee and **2-3 part-time** employees

Security in Small Organizations

- Small organizations
  - –Have between 10 and 100 computers
  - –Have a simple, centralized IT organizational model
  - –**Spend disproportionately more on security *(WHY?)***
  - –Information security is often the responsibility of a single security administrator
  - –Have little in the way of formal **policy**, planning, or security measures
  - –Commonly **outsource** their Web presence or electronic commerce operations
  - –Security training and awareness is commonly conducted on a 1-on-1 basis
  - –Policies (when they exist) are often **issue-specific and reactive**
  - –Formal planning is often part of IT planning
  - –Threats from insiders are less likely
    - Every employee knows every other employee (less anonymity)
    - Smaller, less lucrative target. No bragging rights, etc

Placing InfoSec Within an Organization

FANSHAWE

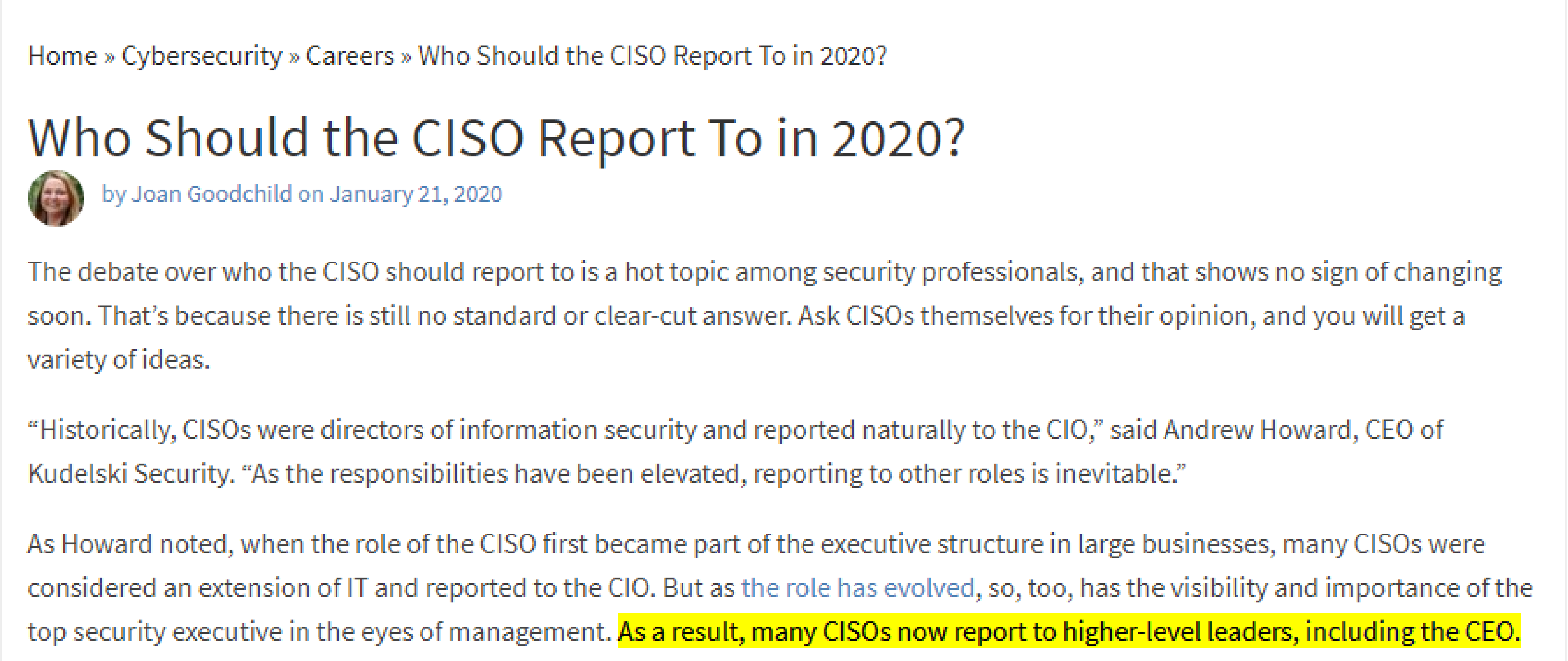
Placing Information Security Within An Org.

- In large organizations, InfoSec is often located within the IT department headed by the CISO who reports **directly to the top computing executive,** the CIO, or even higher.

- **Why report to someone higher than the CIO?**
  - An InfoSec program is sometimes **at odds** with the goals and objectives of the IT department as a whole
  - **Security priorities vs Availability priorities** *(see next slide)*

Placing Information Security Within An Organization

- Because the goals and objectives of the CIO and the CISO may come in conflict
  - It is not difficult to understand the **current movement to separate information security from the IT division**
  - The challenge is to design a reporting structure for the InfoSec program that **balances the needs of each of the communities of interest**



Home » Cybersecurity » Careers » Who Should the CISO Report To in 2020?

Who Should the CISO Report To in 2020?

by Joan Goodchild on January 21, 2020

The debate over who the CISO should report to is a hot topic among security professionals, and that shows no sign of changing soon. That's because there is still no standard or clear-cut answer. Ask CISOs themselves for their opinion, and you will get a variety of ideas.

"Historically, CISOs were directors of information security and reported naturally to the CIO," said Andrew Howard, CEO of Kudelski Security. "As the responsibilities have been elevated, reporting to other roles is inevitable."

As Howard noted, when the role of the CISO first became part of the executive structure in large businesses, many CISOs were considered an extension of IT and reported to the CIO. But as the role has evolved, so, too, has the visibility and importance of the top security executive in the eyes of management. As a result, many CISOs now report to higher-level leaders, including the CEO.

Findings from PWC's "2018 Global State of Information Security Survey" finds 40% of CISOs now report to a CEO.

Placing Information Security Within an Organization

- **What are some other options for positioning the IT Security Department?**
  - Legal
  - Internal auditing
  - Accounting and finance through IT
  - Human resources
  - Facilities management and Operations
  - **Physical security department?** They share the same objectives

No matter where it reports to, InfoSec dept. MUST HAVE support from top management.

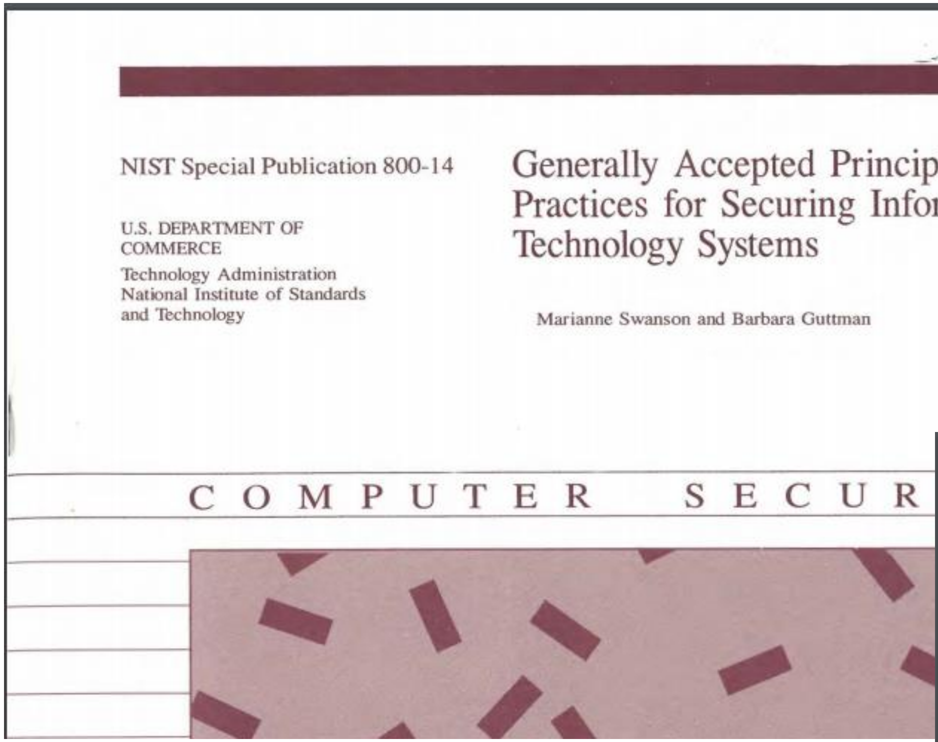
Components of the Security Program

FANSHAWE

Components of the Security Program

- Organization's information security needs
  - **Unique** to the culture, size, and budget of the organization
  - Determining what level the information security program operates on depends on the organization's strategic plan, the **vision and mission statements**.
    - The CIO and CISO should use these documents to formulate the **mission statement for the information security program**

- *NIST (SP 800-14) identifies the following components:*
  - Policy
  - Program management
  - Risk management
  - Life-cycle planning
  - Disaster planning, Incident handling
  - Awareness and training
  - Physical Security
  - Access Control, Auditing, Cryptography



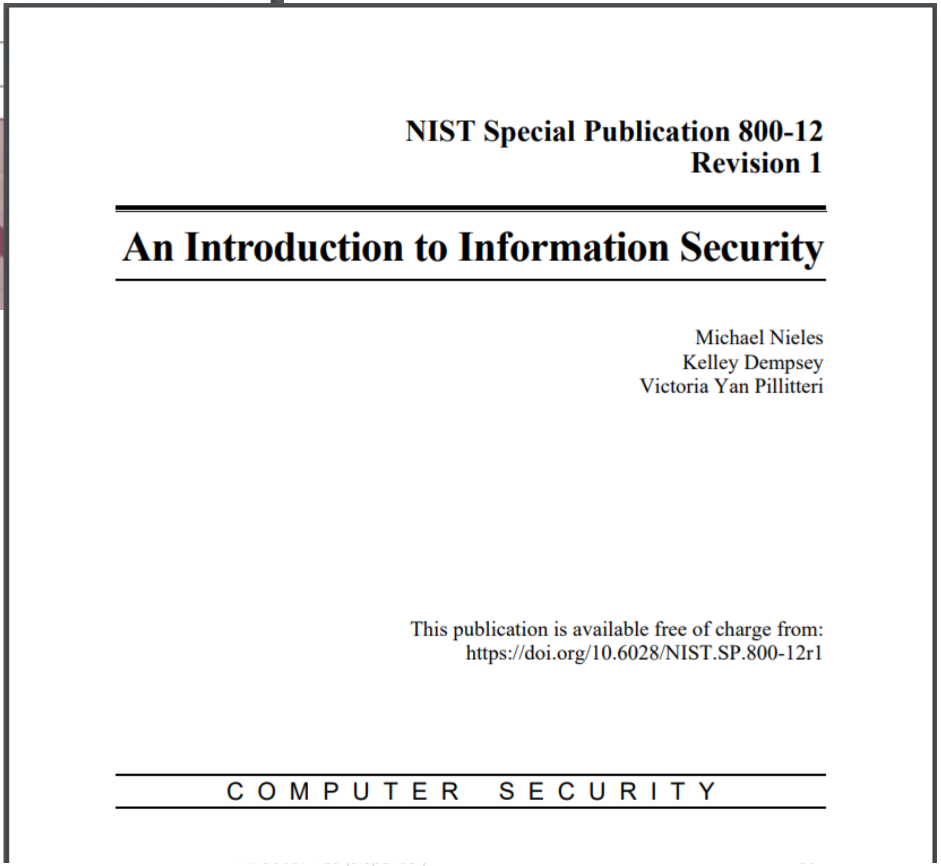
NIST Special Publication 800-14

U.S. DEPARTMENT OF
COMMERCE
Technology Administration
National Institute of Standards
and Technology

Generally Accepted Principles and Practices for Securing Information Technology Systems

Marianne Swanson and Barbara Guttman

COMPUTER SECUR



NIST Special Publication 800-12
Revision 1

An Introduction to Information Security

Michael Nieles
Kelley Dempsey
Victoria Yan Pillitteri

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-12r1

COMPUTER SECURITY

NIST SP 800-12 (2017) and -14

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

FANSHAWE

Information Security Roles and Titles

Information Security Roles and Titles

- Three types of InfoSec positions
  1. Those that ***define***
     - Provide the policies, guidelines, and standards
     - Do the consulting and the risk assessment
     - Develop the product and technical architectures
     - Senior people with a lot of broad knowledge, but often not a lot of depth
  2. Those that ***build***
     - The real “techies” who *create and install* security solutions
  3. Those that ***administer***
     - Operate and administer the security tools
     - Security monitoring
     - Continuously improve the processes

Information Security Roles and Titles

- A typical organization has a number of individuals with information security responsibilities
- While the titles used may be different, most of the job functions fit into one of the following:
  - CISO (may also called CSO)
  - Security managers
  - Security administrators, engineers, architects, and analysts
  - Security technicians, consultants, specialists
  - Security officers and investigators
  - Front line (ex. Service Desk personnel)
    - ****not always identified as an "infosec role" but very important!*****

Help Desk Personnel

- Help desk
  - –An important part of the information security team
  - –Classifies and Prioritizes CFS for specialized roles
  - –Enhances the security team's ability to identify potential problems
    - –Ex. When a user calls the help desk with a complaint , the user's problem may turn out to be **related to a bigger problem**, such as a hacker, denial-of-service attack, or a virus
  - –Because help desk technicians **perform a specialized role** in information security, they have a **need for specialized training**

Is ISMS the same as a Security program?

- ISMS is an ISO-specific term. Security Program is more broadly used
- An Information Security Management System is defined by the **scope** that is written and approved by the company
  - (the same way that a Security program is)
- The advantage of creating an ISMS in accordance with an International Standard**?**
- missing any vital components is unlikely as it **is a more disciplined and systematic approach.**
- Also more likely to achieve ISO **certification** if ISMS is used

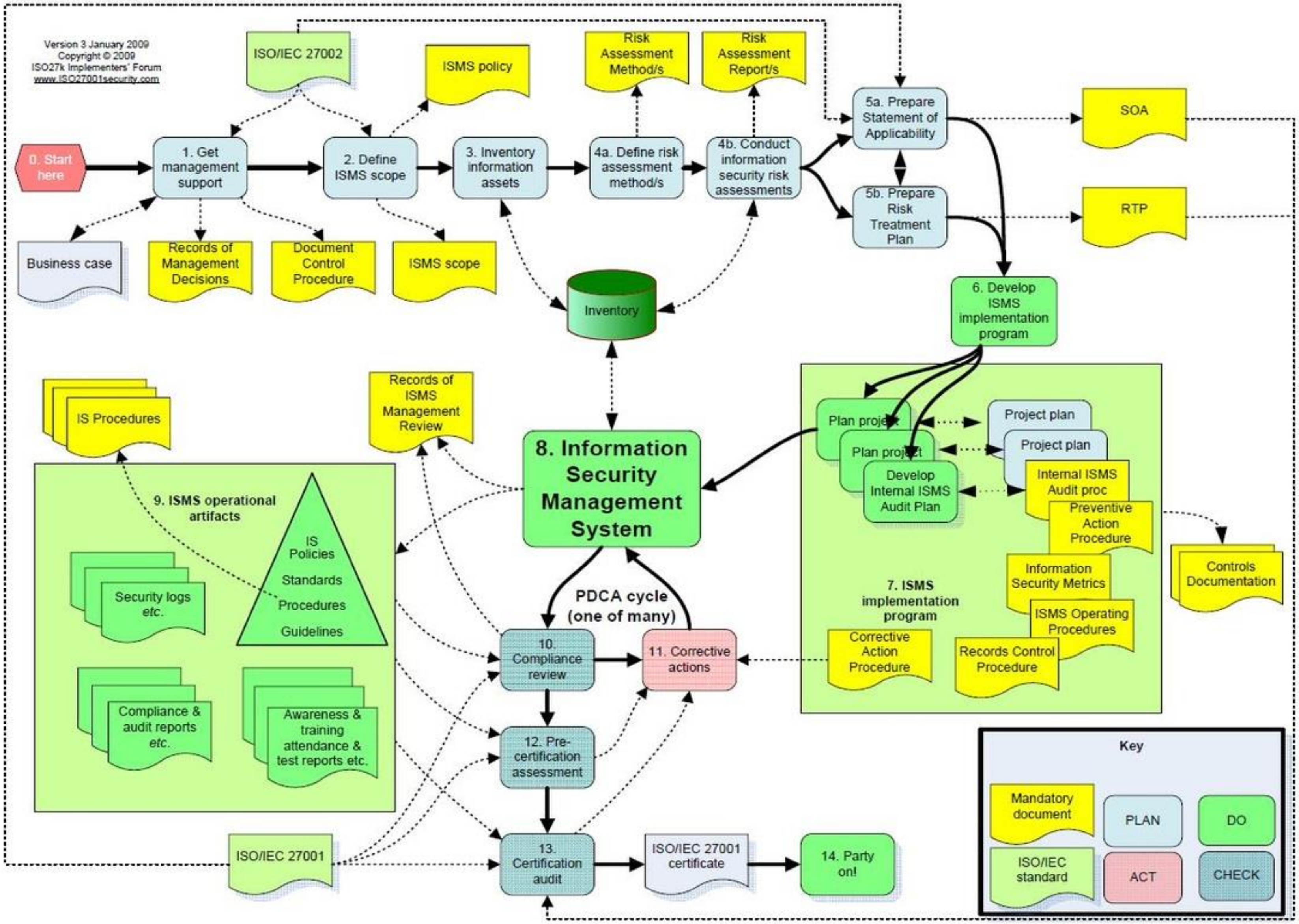
ISO Certification

- Certification under the *ISO 27000 series* is an independent **assessment of a company's ISMS** carried out by a **third party.**
- They check compliance of the ISMS *against the standard*. It is a means of providing assurance that an effective ISMS has been implemented.

“One of the biggest myths about ISO 27001 is that it is focused on IT…while IT is certainly important, **IT alone cannot protect information**. Physical security, legal protection, human resources management, organizational issues – all of them **together** are required to secure the information.” (Kosutic, 2015)

Information Security Management System

- What are the essential elements of an ISMS as defined in ISO27001?
- Remember certification under ISO27001 is **not compulsory**, small companies may find it too expensive but they can still benefit from using the standard as a guide **where applicable.**
  - May depend on cost/benefit and ROI
  - Company size
  - Capacity given resources available
  - Applicability to the environment
  - Demand in that company's specific industry (competitive edge)
  - Etc.


Version 3 January 2009
Copyright © 2009
ISO27k Implementers' Forum
www.ISO27001security.com
0. Start here
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4a. Define risk assessment method/s
4b. Conduct information security risk assessments
5a. Prepare Statement of Applicability
5b. Prepare Risk Treatment Plan
6. Develop ISMS implementation program
7. ISMS implementation program
8. Information Security Management System
9. ISMS operational artifacts
10. Compliance review
11. Corrective actions
12. Pre-certification assessment
13. Certification audit
14. Party on!
ISO/IEC 27002
ISMS policy
Risk Assessment Method/s
Risk Assessment Report/s
SOA
RTP
Business case
Records of Management Decisions
Document Control Procedure
ISMS scope
Inventory
IS Procedures
Records of ISMS Management Review
IS Policies
Standards
Procedures
Guidelines
Security logs etc.
Compliance & audit reports etc.
Awareness & training attendance & test reports etc.
Plan project
Plan project
Project plan
Project plan
Develop Internal ISMS Audit Plan
Internal ISMS Audit proc
Preventive Action Procedure
Information Security Metrics
ISMS Operating Procedures
Records Control Procedure
Corrective Action Procedure
Controls Documentation
PDCA cycle (one of many)
ISO/IEC 27001
ISO/IEC 27001 certificate
Key
Mandatory document
PLAN
DO
ISO/IEC standard
ACT
CHECK

http://www.iso27001security.com/ISO27k_ISMS_implementation_and_certification_process_v3.pdf

ISO27001

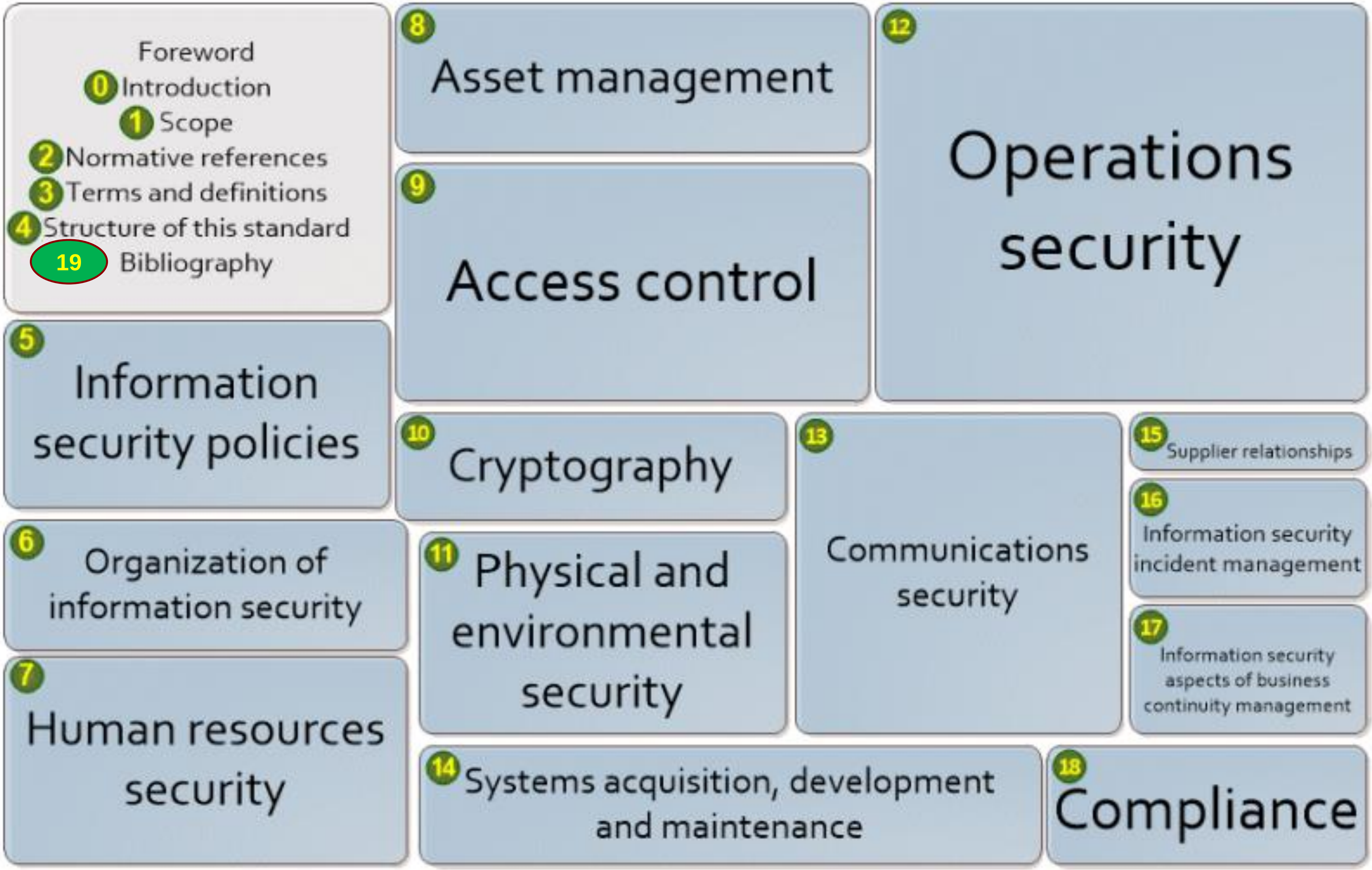
- ISO27001 formally specifies how to establish an Information Security Management System (**ISMS**).
- The adoption of an ISMS is a **strategic decision**.
- The design and implementation of an organization's ISMS is influenced by:
  - its business and security **objectives**,
  - its security **risks** and **control** requirements,
  - the **processes** employed and
  - the size and structure of the organization (ie. a simple situation requires a simple ISMS.)
- The ISMS will evolve systematically in response to **changing risks**.
- Compliance with ISO27001 can be formally assessed and certified. A certified ISMS builds confidence in the organization's approach to information security management among stakeholders.

ISO27002

- ISO27002 is a “Code of Practice” recommending a large number of **information security controls**.
- Control objectives throughout the standard are generic, high-level statements of business requirements for securing or protecting information assets.
- The numerous information security controls recommended by the standard are meant to be implemented in the context of an ISMS, in order to **address risks** and satisfy applicable control objectives systematically.
- a generic, advisory document, not a formal specification or certification standard such as ISO 27001

ISO27002 – 19 sections

https://www.iso27001security.com/html/27002.html



Foreword

0 Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Structure of this standard

19 Bibliography

5 Information security policies

6 Organization of information security

7 Human resources security

8 Asset management

9 Access control

10 Cryptography

11 Physical and environmental security

12 Operations security

13 Communications security

14 Systems acquisition, development and maintenance

15 Supplier relationships

16 Information security incident management

17 Information security aspects of business continuity management

18 Compliance

ISO 27001: The ISMS Documentation

- It is important to be able to demonstrate the **relationship** from the selected **controls** back to the **risk assessment** and **risk treatment** process, and subsequently back to the **ISMS policy and objectives**.

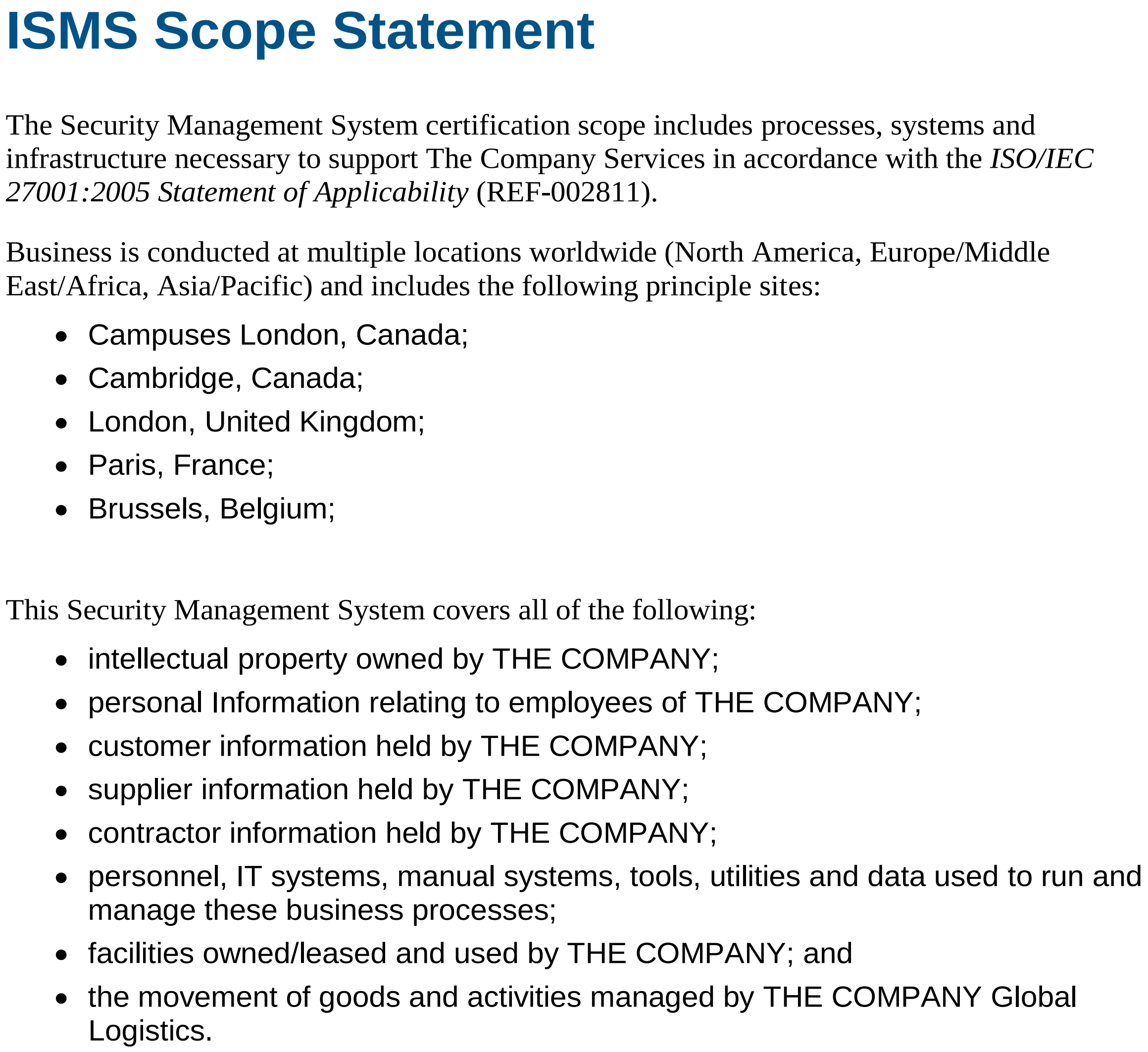
ISMS documentation should include:

- Documented statements of the ISMS **policy** and objectives;
- The **scope** of the ISMS;
- Procedures and other controls in support of the ISMS;
- A description of the risk assessment methodology;
- A risk assessment report and Risk Treatment Plan (**RTP**);
- Procedures for effective planning, operation and control of the information security processes, describing how to measure the effectiveness of controls;
- Various records specifically required by the standard;
- The Statement of Applicability (**SOA**).

ISO 27001: Mandatory Documents

- ISMS Scope (people, places, technology),
- Enterprise Information Security Policy (this is underpinned by issue-specific policies, standards & procedures)
- Statement of Applicability (details of relevant controls),
- Risk Assessment Methodology,
- Risk Assessment Report(s),
- Risk Treatment Plan (how to deal with identified risks),
- Asset register (what, where, value, security classification, any risks).

A sample ISMS Scope Statement



ISMS Scope Statement

The Security Management System certification scope includes processes, systems and infrastructure necessary to support The Company Services in accordance with the *ISO/IEC 27001:2005 Statement of Applicability* (REF-002811).

Business is conducted at multiple locations worldwide (North America, Europe/Middle East/Africa, Asia/Pacific) and includes the following principle sites:

- Campuses London, Canada;
- Cambridge, Canada;
- London, United Kingdom;
- Paris, France;
- Brussels, Belgium;

This Security Management System covers all of the following:

- intellectual property owned by THE COMPANY;
- personal Information relating to employees of THE COMPANY;
- customer information held by THE COMPANY;
- supplier information held by THE COMPANY;
- contractor information held by THE COMPANY;
- personnel, IT systems, manual systems, tools, utilities and data used to run and manage these business processes;
- facilities owned/leased and used by THE COMPANY; and
- the movement of goods and activities managed by THE COMPANY Global Logistics.

ISO 27001: The Inventory of Assets

- An inventory of all important information assets should be developed and maintained, recording details such as:
  - **Type of asset;**
  - Format/Type (*i.e.* software, physical/printed, services, people, intangibles)
  - Location; (physical and logical location)
  - Backup information;
  - License/SMA information;
  - Business value (*e.g.* which business processes **depend** on it?).

ISO 27001: Types of Assets

- **Information assets**: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information
- **Software assets**: application software, system software, development tools, and utilities
- **Physical assets**: computer equipment, communications equipment, removable media, and other equipment
- **Services**: computing and communications services, general utilities, (heating, lighting, power, and air-conditioning)
- **People**, and their qualifications, skills, and experience
- **Intangibles**, such as reputation and image of the organization.

ISO 27001: Risk Assessment

- Risk assessments should **identify, quantify, and prioritize information security risks** against defined criteria for risk acceptance and objectives relevant to the organization.
- The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.
- Assessing risks and selecting controls may need to be **performed repeatedly** across different parts of the organization and information systems, and **to respond to changes.**
- The process should systematically estimate the magnitude of risks (**risk analysis**) and compare risks against risk criteria to determine their significance (**risk evaluation**).
- The information security risk assessment should have a clearly defined scope and complement risk assessments in other aspects of the business, where appropriate.

ISO 27001: Risk Treatment Plan

- The organisation should formulate a risk treatment plan (**RTP**) identifying:
  - The appropriate management actions, resources, responsibilities
  - The priorities for dealing with its information security risks.
- The RTP should be set within the context of the organization's information security policy and should clearly identify the approach to risk and the criteria for accepting risk.
- The RTP is the key document that links all four phases of the PDCA cycle for the ISMS (next 2 slides).

ISO 27001: PDCA Model

- **Plan** (establish the ISMS)
  - Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall policies and objectives.
- **Do** (implement and operate the ISMS)
  - Implement and operate the ISMS policy, controls, processes and procedures.
- **Check** (monitor and review the ISMS)
  - Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
- **Act** (maintain and improve the ISMS)
  - Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

ISO27001: Procedures

ISO 27001 requires **four documented procedures**:

1. Control of documents,
2. Internal ISMS audits,
3. Corrective actions,
4. Preventive action.

should define who is responsible for approving documents and for reviewing them, how to identify the changes and revision status, how to distribute the documents, etc

- The term “documented” means that “the procedure is established, documented, implemented and maintained” (ISO/IEC 27001, 4.3.1 Note 1).

Consider these four mandatory procedures as the “pillars” of your management system (together with the security policy)

ISO27001: Internal ISMS Audits

- The procedure for internal audits must define:
  - **Responsibilities** for planning and conducting audits
  - How audit results are **reported**
  - How the records are **maintained**.
- This means that the main **rules** for conducting the audit **must be set**.

ISO27001: Corrective Actions

- The procedure for **corrective action** (similar to **preventive action** – often the same doc) should define:
  - how the non-conformity and its cause are identified,
  - how the necessary actions are defined and implemented, what records are taken,
  - How you are eliminating the cause of the non-conformity
  - how the review of the actions is performed.

- The purpose of this procedure is to define how each corrective action should eliminate the cause of the nonconformity so that it will not occur again.

ISO 27001: Pre-Certification Assessment

- Prior to certification, the organization should carry out a comprehensive review of the ISMS and SOA.
- The organization will need to demonstrate compliance with both the full PDCA cycle and clause 8 of ISO27001, the **“requirement for continual improvement”.**
- Certification auditors will seek evidence (in the form of records of processes such as risk assessments, management reviews, incident reports, corrective actions *etc.*) that the *ISMS is operating and continually improving*.
- The ISMS therefore needs a while to settle down, operate normally and generate the records after it has been implemented.

ISO 27001: Certification Audit

- Certification involves the organization’s ISMS being assessed for **compliance** with ISO27001.
- The certification body needs to gain **assurance** that the organization’s information security risk assessment properly reflects its business activities for the **full scope of the ISMS**.
- The assessors will check that the organization has properly **analysed and treated its information security risks** and continues managing its information security risks systematically.
- A **certificate** of compliance from an accredited certification body has **credibility** with other organizations. **VALID FOR 3 YEARS**

Reminders

- **Test #2** is next week
  - If you are studying part time or abroad and need to write at an alternate time, please email me **ASAP**

- **Assignment 2 will be marked shortly** Assignment 3 has been posted- due Aug.