Introduction to Saudi Cybersecurity Frameworks

The First Unit : Introduction

At the end of the unit, the trainee should be able to:

- Identify the Saudi Cyber Security Framework
- Mention the points of the Saudi Cyber Security Framework
- Feel the importance of the Saudi Cyber Security
- Know Cyber Security
- Explain the objectives of Cyber Security
- Explain the difference between Information Security and Cyber Security

Lesson1 : Course Introduction

1.1 Introduction to the Framework

The current digital society has high expectations of flawless customer experience, continuous availability of services and effective protection of sensitive data. Information assets and online services are now strategically important to all public and private organizations, as well as to broader society.

These services are vital to the creation of a vibrant digital economy. They are also becoming systemically important to the economy and to broader national security.

All of which underlines the need to safeguard sensitive data and transactions, and thereby ensure confidence in the overall Saudi Financial Sector.

The stakes are high when it comes to the confidentiality, integrity and availability of information assets, and applying new online services and new developments (e.g. Fintech, block chain); while improving resilience against cyber threats.

Not only is the dependency on these services growing, but the threat landscape is rapidly changing. The Financial Sector recognizes the rate at which the cyber threats and risks are evolving, as well as the changing technology and business landscape.

SAMA established a Cyber Security Framework (“the Framework”) to enable Financial Institutions regulated by SAMA (“the Member Organizations”) to effectively identify and address risks related to cyber security. To maintain the protection of information assets and online

services, the Member Organizations must adopt the Framework.1.1 Introduction to the Framework The current digital society has high expectations of flawless customer experience, continuous availability of services and effective protection of sensitive data.

Information assets and online services are now strategically important to all public and private organizations, as well as to broader society.

These services are vital to the creation of a vibrant digital economy.

They are also becoming systemically important to the economy and to broader national security. All of which underlines the need to safeguard sensitive data and transactions, and thereby ensure confidence in the overall Saudi Financial Sector. The stakes are high when it comes to the confidentiality, integrity and availability of information assets, and applying new online services and new developments (e.g. Fintech, block chain); while improving resilience against cyber threats. Not only is the dependency on these services growing, but the threat landscape is rapidly changing.

The Financial Sector recognizes the rate at which the cyber threats and risks are evolving, as well as the changing technology and business landscape.

SAMA established a Cyber Security Framework (“the Framework”) to enable Financial Institutions regulated by SAMA (“the Member Organizations”) to effectively identify and address risks related to cyber security. To maintain the protection of information assets and online services, the Member Organizations must adopt the Framework.

1.2 Definition of Cyber Security

Cyber security is defined as the collection of tools, policies, security concepts, security safeguards,
guidelines, risk management approaches, actions, training, best practices, assurance, and technologies
that can be used to protect the member organization's information assets against internal and external
threats.
The general security objectives comprise the following:
· Confidentiality–Information assets are accessible only to those authorized to have access (i.e., protected from unauthorized disclosure or (un)intended leakage of sensitive data).

· Integrity–Information assets are accurate, complete and processed correctly (i.e., protected from
unauthorized modification, which may include authenticity and non-repudiation).
·Availability–Information assets are resilient and accessible when required (i.e., protected from unauthorized disruption).

Unit Two : NCA

At the end of the unit, the trainee will be able to:

- Explains basic cybersecurity controls
- Mentions cloud cybersecurity controls
- Shows the importance of national standards for data encryption
- Feels the role of cybersecurity for e-commerce
- Explains cybersecurity controls for remote work

Lesson1 : Controls: ECC, CCC, OTC, CSCC, TCC, DCC, Social Media

Essential Cybersecurity Controls (ECC)

Cloud Cybersecurity Controls (CCC)

Operational Technology Cybersecurity Controls (OTC)

Critical Systems Cybersecurity Controls (CSCC)

Telework Cybersecurity Controls (TCC)

Critical Systems Cybersecurity Controls (CSC)

Data Cybersecurity Controls (DCC)

1. Executive Summary

NCA's mandates and duties fulfill the regulatory cybersecurity needs related to the development of cybersecurity national policies, governance mechanisms, frameworks, standards, controls and guidelines, to support the important role of cybersecurity which has increased with the rise of security risks in cyberspace more than any time before.

The cloud services subject is trending globally, and improves in a very fast pace in the Kingdom of Saudi Arabia which results in a new cybersecurity risk that require cybersecurity controls to transact with cloud services taking into consideration international common practices in this field; and to be an extension to the already published Essential Cybersecurity Controls (ECC-1: 2018).

As a result, the Cloud Cybersecurity Controls (CCC – 1: 2020) is developed to minimize the cybersecurity risks of Cloud Service Providers (CSPs), and Cloud Customers, also known as Cloud Service Tenants (CSTs). This document highlights the details of the cloud cybersecurity controls for cloud services, objectives, scope, statement of applicability, compliance approach and monitoring.

All CSPs and CSTs shall implement all necessary measures to ensure continuous compliance with the CCC as per Paragraph III of Article 10 of NCA's mandate and as per the Royal Decree number 57231, dated 10/11/1439AH.

2. Introduction

The National Cybersecurity Authority (referred to in this document as "The Authority" or "NCA") developed the Cloud Cybersecurity Controls (CCC – 1: 2020) after conducting a comprehensive study of multiple national and international cybersecurity frameworks, standards and controls, and reviewing common industry practices and experiences in the field of cybersecurity. A mapping study is conducted with international cloud computing standards and controls such as US FedRAMP (the number of FedRAMP requirements ranges from 125 to 421), Multi-Tier Cloud Security Standard for Singapore (MTCS SS) which contains 535 requirements, Germany C5 which contains 114 requirements, Cloud Controls Matrix (CCM) which contains 133 controls, and ISO/IEC 27001 which contains 114 controls. Details of this mapping is represented in a separate document extended to the CCC.

3. Objectives

The Cloud Cybersecurity Controls (CCC – 1: 2020) is developed as an extension to the ECC; to achieve higher levels of national cybersecurity goals by focusing on cloud computing services from the perspective of Cloud Service Providers (CSPs) and Cloud Service Tenants (CSTs). Also, the CCC aims to set the minimum requirements for cybersecurity of cloud computing, for both CSPs and CSTs, to contribute to enable the CSPs and the CSTs to provide and use secure cloud computing services and mitigating cyber risks against them.

The cybersecurity of cloud computing services, for both CSPs and CSTs, must be able to protect the confidentiality, integrity and availability of the data and information within the cloud environment. To that aim, CCC take into consideration the following four main cybersecurity pillars:

Strategy

People

Procedures

Technology

4. Scope of Work and Applicability

Scope of Work of the CCC

The cybersecurity controls shall apply to the CSPs and CSTs. These controls represent the minimum cybersecurity requirements for cloud computing.

CSPs within the scope of CCC are any CSP which provides cloud computing services to the CSTs within the scope of work. CSTs within the scope of CCC are any government organization in the Kingdom of Saudi Arabia inside or outside the Kingdom (including ministries, authorities, establishments and others) and its companies and entities, as well as private sector organizations owning, operating or hosting Critical National Infrastructures (CNIs) that currently use or planning to use any cloud service.

The cybersecurity controls shall apply to the CSPs and CSTs. These controls represent the minimum cybersecurity requirements for cloud computing.

The NCA strongly encourages all other organizations in the Kingdom to leverage these controls to implement best practices to improve and enhance their cloud cybersecurity.11

Examples of CSPs outside Scope of Work

CSPs who provide cloud computing services for non-saudi organizations outside KSA, and not provided services to CSTs within scope of work.

CSPs who provide cloud computing services for individuals, and private sector organizations not owning, operating or hosting Critical National Infrastructures (CNIs), and not provided services to CSTs within scope of work.

CCC Statement of Applicability

The ECC and the CCC have been developed after taking into consideration the cybersecurity needs of CSPs and CSTs, and every CSP and CST must comply with all applicable controls.

5. Implementation and Compliance

To comply with item 3 of article 10 of NCA's mandate and as per the Royal Decree number 57231, all CSPs and CSTs within the scope of these controls must implement whatever necessary to ensure continuous compliance with the CCC according to the levels shown in Table (2) and Table (3) in section "Annex No. (A): Cloud Cybersecurity Controls Levels" in this document, taking into account the following two rules:

1. CST's controls in the CCC are an extension and complement to the controls in the ECC; therefore, the CSTs must ensure continuous compliance with the controls in both ECC and CCC.

2. CSP's controls in the CCC are an extension and complement to the controls in the ECC; therefore, the CSPs – within or outside the scope of the ECC- must ensure continuous compliance with the controls in both ECC and CCC.

NCA will give CSPs and CSTs within the scope of work a compliance period to comply with the CCC (taking into account CSPs and CSTs who move from outside the scope to within the scope of work) as deemed appropriate by NCA. Also, NCA evaluates CSPs and CSTs compliance with the

CCC in accordance with the mechanisms deemed appropriate by NCA; such as self-assessment of CSPs and CSTs, and/or external compliance assessment by NCA or designated third-parties.

6. Cloud Cybersecurity Controls Methodology and Mapping Annex

NCA developed cloud cybersecurity controls methodology and mapping annex document which is considered as a part of Cloud Cybersecurity Controls document. The cloud cybersecurity controls methodology and mapping annex document is constituted of the following:

Design principles of the CCC.

Relationship to other international standards.

Design methodology of the CCC.

Main domains and subdomains structure of the CCC.

Domains mapping to international standards.

Control mapping to international standards.

ECC/CCC subdomain mapping.

Control Applicability on different Cloud Service Models (IaaS, PaaS, and SaaS).

7. Update and Review

NCA will periodically review and update the CCC (in addition to any supplement documents related to the CCC) as per the cybersecurity requirements and related industry updates. NCA will communicate and publish the updated version of CCC for implementation and compliance.

Operational Technology Cybersecurity Controls

In continuation of its role in regulating and protecting the Kingdom's cyberspace, and in line with the Kingdom’s Vision 2030, NCA publishes the Operational Technology Cybersecurity Controls (OTCC-1:2022). These controls are aligned with related international cybersecurity standards, frameworks, controls, and best practices.

The controls aim to raise the cybersecurity level of OT systems in the Kingdom by setting the minimum cybersecurity requirements for organizations to protect their Industrial Control systems (ICS) from cyber threats that could result in negative impacts. These controls are an extension to the NCA’s Essential Cybersecurity Controls (ECC).

Critical Systems Cybersecurity Controls

Type of regulatory document: Policies and controls

The National Cybersecurity Authority “NCA” has developed the Critical Systems Cybersecurity Controls (CSCC – 1: 2019), as an extension and a complement to the Essential Cybersecurity Controls (ECC), to fit the cybersecurity needs for national critical systems. The Critical Systems

Cybersecurity Controls consist of 32 main controls and 73 sub controls, divided into four main domains:

- Cybersecurity Governance
- Cybersecurity Defense
- Cybersecurity Resilience
- Third-party and Cloud Computing Cybersecurity

Telework Cybersecurity Controls (TCC)

Type of regulatory document: Policies and controls

Based on the objectives of the National Cybersecurity Authority (NCA) strategy and in continuation of its role in regulating and protecting the Kingdom's cyberspace, NCA has issued the Telework Cybersecurity Controls (TCC) document. These controls were developed after reviewing many international cybersecurity standards, frameworks, controls and international practices in cybersecurity. The document aims to contribute to raising the level of cybersecurity at the national level by enabling the organization to perform its work remotely in a secure manner and adapt to the changes in the business environment and telework systems, and enhancing the organization’s cybersecurity capabilities and resilience against cyber threats when providing remote work. These controls are an extension to the Essential Cybersecurity Controls (ECC)

What is social media?

Social media encompasses all the platforms and apps that allow people, creators, and businesses to communicate with one another, create online communities, exchange ideas, and share content.

From Instagram and TikTok to YouTube and WhatsApp, the social media platforms that users have at their disposal are endless. While social media is mainly used by individual people, brands and creators can also use social media marketing to connect with their audience, build their brand, and sell their products or services.

Social media has completely revolutionized the way modern-day society communicates and shares ideas, information, and content. What really separates social media from other types of media is that it’s a two-way style of communication rather than a one-way communication style built to deliver information with no way to reply back, such as newspapers, radio, and television.

How does social media work?

Every social media platform works differently and has its own unique set of features, however

there are a few commonalities. Here are some of the most common features social media platforms share:

- Profile: Most social media platforms will have users create their own personal profile or a business profile, which is where they can upload a profile photo, add information in a bio, and create their unique account name.
- Sharing content: Each social media user has the ability to share content from their personal profile, but the type of content varies from platform to platform; for example, on Twitter and Facebook you can share text, photos, short videos, and more, while on TikTok you can only share pictures and videos.
- Direct messaging: A private form of communication between users on social media platforms; while some social media platforms have direct messaging as the main feature, like WhatsApp or WeChat, others have it as an additional feature, for example, Instagram Direct Messages or Facebook's Messenger.
- Algorithm: All social media platforms use an algorithm to determine which content to display to users, and in what order; most algorithms are designed to deliver the content a user is most likely to engage with, based on previous content they've interacted with.
- Feed and timelines: Most social media platforms aggregate all published posts from accounts you follow, suggested posts based on what you like, and relevant ads in a single feed or timeline.

What are some examples of social media platforms?

The major social media platforms (at the moment) are Instagram, Facebook, WhatsApp, TikTok, Twitter, LinkedIn, Pinterest, YouTube, and Snapchat, with Facebook being the largest social media platform at nearly 3 billion people using it monthly.

To make things easier, we researched the top social media platforms in 2023. Some will be familiar to you, while others might sound new. We recommend reading through that list to see what social media apps might work best for you and your brand. And remember, you don't have to be on every social media platform to have a successful brand.

What are the benefits of social media for personal use?

For many, social media is woven into the fabrics of everyday life. With 59% of the world's population using social media, it makes it an incredibly powerful tool for spreading ideas and communicating with one another; and it offers many benefits for social media users. Some of the benefits of social media use for personal purposes are:

- Build relationships: social media was born as a way for people to connect with one another, thus making it a great tool to foster new relationships and strengthen existing ones.

- Developing a personal voice: Your social media accounts can be an extension of your identity, which means social media can be used as a tool to express yourself, share your interests, and show your talents.
- Encourages discovery and education: Social media platforms offer enormous educational resources (like how-to YouTube videos and informative Tweet Threads), learning communities, and expert social media profiles.

What are the benefits of social media use for businesses and creators?

With 77 percent of people using social media to learn more about a product or brand, it's crucial for businesses and creators to have an active social media presence where they publish content regularly and consistently. Some of the benefits of social media use for business and creators are:

- Budget-friendly marketing strategy: Compared to other types of marketing strategies, social media marketing is one of the best and most affordable ways to get your products and services in front of a large audience
- Increased brand exposure: With almost 5 billion social media users around the globe, these platforms can give businesses the opportunity to reach new audiences and increase their brand exposure.
- Content, updates, and event sharing: social media is a natural and easy way for businesses to keep their audience in the loop on what's happening in their business, whether that be to promote their latest article, an upcoming event, or any other important updates (i.e. new closing hours, shipping delays, new teammates, etc.)
- Targeted marketing: Through social media advertising, such as Instagram Ads or Facebook Ads, you can run highly-targeted social media ads, which will help businesses to increase online sales and generate awareness.
- Customer engagement: The majority of people ages 18-54 see social media as an effective channel for customer service; and with many businesses not being super responsive on social media, this is an easy way to stand out from the crowd, impress your fans, and build a relationship.

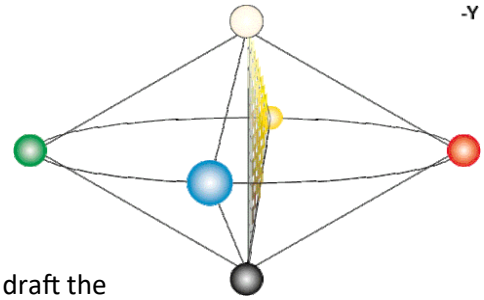
There are also a range of social media management tools that help businesses and creators to make social media work for them. For example, Buffer is a social media management tool that can help you achieve success with your social media marketing. Whether you want to build a brand or grow your business, we want to help you succeed. Sign up for our free plan or get started with a free trial.

How many people use social media?

As of January 2023, there are 4.76 billion active social media users around the globe, which means about 59% of the total global population uses social media. This number increased by 3% compared to the previous year.

Here are the top 6 social networking platforms of 2023, ranked by Monthly Active Users (MAUs):

1. Facebook: 2.96 billion MAUs
2. YouTube: 2.2 billion MAUs
3. WhatsApp: 2 billion MAUs
4. Instagram: 2 billion MAUs
5. WeChat: 1.26 billion MAUs
6. TikTok: 1 billion MAUs



Lesson2 : Standards: NCS, SCyWF

The National Cryptographic Standards (NCS)

Overview

The National Cybersecurity Authority (NCA) is mandated to draft the national cryptographic policies and standards, to ensure compliance with these standards and policies, and to review and update them periodically. The NCA has launched the National Cryptographic Standards (NCS) to meet the national need by specifying the minimum requirements necessary to provide the degree of protection required for national data, systems and networks using cryptographic mechanisms, for civilian and commercial purposes, based on global best practices, global standards and the national need in this field. The National Cryptographic Standards aim to define the minimum acceptable requirements for providing the degree of protection required for national data, systems and networks (that are used for civilian and commercial purposes) using cryptographic mechanisms, and to enhance national encryption uses to contribute to the protection of cyberspace at the national level.

The standards document defines two levels of strength and security for cryptographic systems and mechanisms, which are the MODERATE level and the ADVANCED level in order to ensure flexibility and efficiency in implementation. The document includes accepted symmetric and asymmetric primitives, symmetric and asymmetric schemes, some of the accepted common application protocols related to cryptography, Public Key Infrastructure (PKI) and Key Lifecycle Management (KLM). The document also presents appendices with topics of importance related to cryptographic operations such as: (Pseudo Random Number Generation (PRNG), Post-Quantum Cryptography and Side-Channel Attacks).

Each national entity is required to choose and implement the appropriate cryptographic standard level based on the nature and sensitivity of the data, systems and networks to be protected. Furthermore, other cybersecurity regulations, issued by the NCA, may mandate the use of a particular cryptographic standard level to protect data, systems and networks.

The Saudi Cybersecurity Workforce Framework (SCyWF)

Overview

The SCyWF categorizes cybersecurity work in Saudi Arabia, defines the job roles within each category and sets the requirements for each job role in terms of tasks, knowledge, skills and abilities.
The SCyWF aims to serve as a reference model and a guideline for preparing, developing, recruiting, promoting and managing the cybersecurity workforce. It provides a common lexicon that improves communication and content development for talent management activities. It also helps in mapping learning outcomes of education and training programs to the knowledge, skills and abilities required for different cybersecurity job roles.

The SCyWF has five categories, twelve specialty areas and forty job roles. These are defined in a brief description summarizing the work performed in that specific category, specialty area or job role. Each job role is associated with a set of tasks to be performed within that job role and a list of knowledge, skills and abilities required to perform those tasks.
Organizations in Saudi Arabia are recommended to adopt this framework so they can align their cybersecurity workforce structures and activities with the national frameworks and guidelines. The content of this framework will be reviewed and updated periodically.

Alignment guide for the Saudi cybersecurity workforce framework "SCyWF"

The alignment guide for the Saudi cybersecurity workforce framework "SCyWF" focuses on defining the alignment process of the existing cybersecurity job roles in Saudi Arabia organizations with the predefined job roles in "SCyWF" framework.
The "SCyWF" framework alignment mechanism consists of four steps:

Listing the job roles within "SCyWF" framework that exist at the organization according to the tasks assigned.

- Linking the listed job roles to the existing jobs at the organization.
- Handling special cases, such as two or more job roles within "SCyWF" framework can be mapped to one job at the organization.
- Document the alignment process.

Additionally, the alignment guide demonstrates a number of examples of mapping job titles in the organization with the relevant job roles in "SCyWF" framework.

Lesson3 : Guidelines: CGEC, CGESP, ECC Guidance

Guide to Essential Cybersecurity Controls (ECC) Implementation

Type of regulatory document: Guidelines and support tools

National Cybersecurity Authority (NCA) is the government entity in charge of cybersecurity in the Kingdom, and it serves as the national authority on its affairs. NCA is mandated to develop and update policies, governance mechanisms, frameworks, standards, controls and guidelines related to cybersecurity, share them with relevant entities and follow up on their compliance. The purpose of developing Guide to Essential Cybersecurity Controls (ECC) Implementation to enable the targeted entities in implementing ECC requirements that are needed for their compliance and identify relevant cybersecurity tools that are developed by NCA.

Cybersecurity Guidelines for e-Commerce

Type of regulatory document: Guidelines and support tools

The National Cybersecurity Authority (NCA) is mandated to develop and issue guidelines related to cybersecurity. Accordingly, in a joint effort with the Saudi E-Commerce Council, two cybersecurity guidelines documents were issued: the cybersecurity guidelines for e-commerce service providers and the cybersecurity guidelines for e-commerce consumers.

The first document provides e-commerce service providers, including Small and Medium Enterprises (SMEs) and Small Office / Home Office (SoHo) sellers, with guidelines to protect their e-commerce data, devices and services. The second document provides guidelines to the consumers of e-commerce to help them get a secure shopping experience and to protect their devices, data and personal information during online transactions.

Lesson4 : Workshop Group Discussion

Group Discussion Workshop: An Exercise in Experiential Learning

Discussions are a valuable learning tool, but what are the keys to motivating students to participate, and keeping them engaged? This enquiry formed the basis for the workshop In-Class Group Discussion Could Be Engaging and Fun. The workshop was facilitated by Michael Lee, Instructor and Curriculum Coordinator in the Department of Occupational Science and Occupational Therapy. Michael's belief in the importance of experiential learning was evident in the way the workshop was structured and facilitated, with participants being encouraged to enrich the content by sharing their own experiences related to the topic.

The workshop attendees represented various UBC Faculties, including, Arts, Science, Medicine and Pharmaceutical Science. Michael began the workshop by asking the group – many of whom had used group discussions in the classroom – what they hoped to learn from the session. The responses focused on a number of areas, including how to make discussions fun, how to achieve consistent results, and what kinds of discussion strategies are recommended for higher education.

Ice Breaker

The first activity Michael had for the group was "Name Bingo", an ice breaker game to get people involved, and help them discover shared commonalities. Each participant was given a sheet listing nine different characteristics – for example, "Bikes to Work," "Is New to UBC," or "Teaches a Class of More than 100." The goal was to find a person in the group who was a match for each of the characteristics. The room soon became quite animated, with everyone up and circulating, asking questions of the other participants and exchanging information about themselves. "Bingo" was called as soon as the first person had completed the sheet.

Michael then moved on to the next part of the activity. Participants were asked to pair up with someone with whom they shared similar characteristics, and interview them for the purpose of introducing them to the group. The interview process revealed still more things the pairs had in common – whether in terms of their professional development, "we found we had taken similar career paths", or their personal lives, "we both love sushi!".

Group Discussions – The Pros and Cons

For the next activity, Michael divided the large group into two smaller groups, and asked them to discuss the pros and cons of small group discussions. Within their groups, participants shared thoughts and experiences related to the topic, and recorded their ideas on a flip chart. Michael circulated between the groups, supporting the discussions by validating insights, providing additional examples, and suggesting resources. At the end of the allotted time, all the attendees reassembled to report on the results.

On the "Pro" side, both groups agreed that in-class discussions increase the potential for individual participation. In a small group, everyone has a chance to speak – an important factor, in that people learn better when they are more involved. Students get to know one another more easily in a small group, and are more likely to express themselves. Students can also benefit from peer learning in small groups – communication between peers can help to simplify and clarify content, and allow students who have fallen behind to catch up. Another advantage of the group discussion format is that it allows for a longer exploration of a topic. The use of online discussion boards, moreover, can extend learning beyond the classroom.

In terms of the "Cons" or "Challenges" identified, some attendees felt that a lack of trust can be problematic in small group discussions. Students may not readily see the value of a group learning activity, and may be reluctant to accept the knowledge of their peers as valid. Group dynamics is another challenge: the effectiveness of a group discussion may vary, depending on the mix of individuals involved (introverts, extroverts). Similarly, differences in learning goals can affect the group discussion experience. For example, a student who is taking a course because it is required, rather than because it is a preferred choice, may be less motivated to participate. Group discussions can also present logistical problems for the facilitator – for example, the task of managing feedback effectively when a large number of groups are all reporting on the same topic.

Strategies for Promoting Participation and Engagement

Having examined some of the challenges, participants shared possible solutions, and strategies they have found effective in facilitating in-class group discussions:

1. **Create a climate for sharing**:
   Use an activity such as an ice breaker to allow participants to get to know one another, and to promote trust.

2. **Elicit a personal connection between the participants and the content**:
   Structure the discussion so that the topic resonates with the students' own lives.

3. **Have virtual group discussions, using social media/blogs/online discussion boards**:
   For example, assign students the task of blogging about a website they feel is related to the course or topic.

4. **Introduce accountability**:
   Incorporate group discussions into the marking structure by assigning a percentage of the grade for participation.

5. **Use peer evaluation**:
   Have the groups evaluate other members of their group for their degree of participation.

6. **Involve participants in the process**:
   For example, provide the topic, have each group formulate a question to be discussed, and then swap the questions between groups.

7. **Use e-learning tools**:
   When working with larger groups, consider using I Clickers for reporting activities.

8. **Employ the "Think-Pair-Share" strategy**:
   Allow students time to formulate and share ideas in pairs before presenting them to the group.

9. **Vary reporting methods**:
   For example, provide students with "Scratch and Win" cards (used in the Faculty of Applied Sciences), or conduct a group quiz which introduces the element of anticipation (groups or students are called upon randomly to answer questions).

Reflecting on How Group Discussions Wor

The final activity consisted of a reflection on the effectiveness of the day's group discussion exercise. Michael asked attendees to examine their experience in the group in terms of how ready people were to participate, what the dynamics had been, what had motivated people, and how the discussion progressed.

The participant responses highlighted some of the positive aspects of small group discussions, and provided some insights into how groups work. One participant acknowledged how the ice breaker game, at the beginning of the workshop, had increased the comfort level of the group, and made the discussion exercise more productive. Another participant noted the support she received from members of the group in response to sharing her difficulties using group discussions in her classroom. She felt validated by their understanding, and appreciated the strategies they recommended to ameliorate the problems. This experience made her aware that students who are reticent to participate could also benefit from group learning, if successfully engaged. She pointed out, however, that instructors need to be aware of the differing learning styles of their students. For example, some students might learn more successfully by participating via an online discussion board.

Workshop Mirrors the Process

By participating in the workshop, attendees were involved in an active learning exercise. Their own experience in the group discussion process mirrored that of their students.

The ice breaker at the beginning established personal connections between people, which were then extended to the group. By the time participants got together for the small group discussion exercise, a comfortable atmosphere for sharing had been created. Group members were motivated by their mutual interest in using the group discussion format as a teaching tool. They shared with their peers, learned from them, received validation, and were offered practical suggestions for making their group discussions more effective.

The role of the facilitator, as demonstrated by Michael during the workshop, was to assist in moving the discussion process forward.

Involvement of Participants is Key to Success

Throughout the workshop, Michael emphasized the fact that many of the challenges involved in facilitating small groups discussions can be overcome through engagement. There are numerous strategies, tools, and methods, including those contributed during the session, which can be employed to this end. As the participants learned through direct experience in the workshop, group discussions can indeed be stimulating, enjoyable, and productive.

Michael's final remarks served to summarize and reinforce the central message of the workshop, as well as to communicate his enthusiasm for the topic. "Make groups fun," he reminded the participants, and "keep the group engaged!"

Unit Three : SAMA

At the end of the unit, the trainee will be able to:

- Explains the cybersecurity framework

- Defines the mechanism of creative collaboration

- Explains the purpose of IT governance

- Explains how to deal with cyber-attacks and fraud

- Explains the methods used to prevent cyber attacks

Lesson1 : Cybersecurity Framework

What is a cybersecurity framework?

A cybersecurity framework is a set of guidelines that outlines standards to define the processes and procedures that an organization must take to assess, monitor, and mitigate cybersecurity risk. A cybersecurity framework provides a common language and set of standards for security leaders across countries and industries to understand their security postures and those of their vendors.

Seven common cybersecurity frameworks & standards

1. NIST Cybersecurity Framework
2. ISO 27001 and ISO 27002
3. SOC2
4. NERC-CIP
5. HIPAA
6. GDPR
7. FISMA

1. NIST Cybersecurity Framework 2.0

The NIST Cybersecurity Framework was established in response to an executive order by former President Obama - Improving Critical Infrastructure Cybersecurity - which called for greater collaboration between the public and private sector for identifying, assessing, and managing cyber risk.

While compliance is voluntary, NIST has become the gold standard for assessing cybersecurity maturity, identifying security gaps, and meeting cybersecurity regulations.

al profile; 2. gather needed information; 3. create the organizational profile; 4. analyze the gaps and create an action plan; 5. implement action plan and update profile

In 2024, NIST unveiled the Cybersecurity Framework 2.0 (CSF 2.0), marking its most significant update since the release of CSF 1.1 in 2018.

CSF 2.0 extends its reach beyond critical infrastructure cybersecurity, targeting a wider array of organizations including small schools, nonprofits, large agencies, and corporations, regardless of their cybersecurity expertise.

A notable addition in this update is the emphasis on cybersecurity governance, recognizing cybersecurity as a key component of enterprise risk management alongside financial and reputational risks.

The cybersecurity framework now encompasses six core functions — 1. Identify, 2. Protect, 3. Detect, 4. Respond, 5. Recover, and 6. Govern — providing a holistic approach to managing cybersecurity risk.

NIST has also introduced a suite of resources to facilitate the security framework's adoption. These include quick-start guides tailored for various audiences, success stories from organizations that have implemented the CSF, and a searchable catalog of informative references to align existing practices with the framework’s guidance.

Furthermore, the CSF 2.0 is designed to align with international standards, supporting global cybersecurity resilience efforts.

The journey from CSF 1.1 to CSF 2.0 represents NIST's commitment to evolving the security framework in response to the changing cybersecurity challenges and the needs of its users. Organizations are encouraged to customize the CSF to their specific contexts and share their experiences to benefit the broader community.

2. ISO 27001 and ISO 27002

Created by the International Organization for Standardization (ISO), ISO 27001 and ISO 27002 certifications are considered the international cybersecurity standard for validating a cybersecurity program — internally and across third parties.

With an ISO certification, companies can demonstrate to the board, customers, partners, and shareholders that they are doing the right things with cyber risk management.

Likewise, if a vendor is ISO 27001/2 certified, it’s a good indicator (although not the only one) that they have mature cybersecurity practices and controls in place.

The downside is that the process requires time and resources; organizations should only proceed if there is a true benefit, such as the ability to win new business. The certification is also a point-in-time exercise and could miss evolving risks that continuous monitoring can detect.

3. SOC2

Service Organization Control (SOC) Type 2 is a trust-based cybersecurity framework and auditing standard developed by the American Institute of Certified Public Accountants (AICPA) to help verify that vendors and partners are securely managing client data.

SOC2 specifies more than 60 compliance requirements and extensive auditing processes for third-party systems and controls. Audits can take a year to complete. At that point, a report is issued which attests to a vendors' cybersecurity posture.

Because of its comprehensiveness, SOC2 is one of the toughest security frameworks to implement — especially for organizations in the finance or banking sector who face a higher standard for compliance than other sectors.

Nevertheless, it's an important security framework that should be central to any third-party risk management program.

4. NERC-CIP

Introduced to mitigate the rise in attacks on U.S. critical infrastructure and growing third-party risk, the North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP) is a set of cybersecurity standards designed to help those in the utility and power sector reduce cyber risk and ensure the reliability of bulk electric systems.

The NERC-CIP security framework requires impacted organizations to identify and mitigate third-party cyber risks in their supply chain.

NERC-SIP stipulates a range of controls including categorizing systems and critical assets, training personnel, incident response and planning, recovery plans for critical cyber assets, vulnerability assessments, and more. Read more about effective strategies for achieving NERC-CIP compliance.

5. HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a cybersecurity framework that requires healthcare organizations to implement controls for securing and protecting the privacy of electronic health information.

Per HIPAA, in addition to demonstrating compliance against cyber risk best practices - such as training employees - companies in the sector must also conduct risk assessments to manage and identify emerging risk.

HIPAA compliance remains a keen challenge for healthcare organizations, as Bitsight research suggests.

6. GDPR

The General Data Protection Regulation (GDPR) was adopted in 2016 to strengthen data protection procedures and practices for citizens of the European Union (EU). The GDPR impacts all organizations that are established in the EU or any business that collects and stores the private data of EU citizens — including U.S. businesses.

The security framework includes 99 articles pertaining to a company's compliance responsibilities including a consumer's data access rights, data protection policies and procedures, data breach notification requirements (companies must notify their national regulator within 72 hours of breach discovery), and more.

Fines for non-compliance are high; up to €20,000,000 or 4% of global revenue, and the EU is not shy about enforcing them.

Read the Risk Managers Guide to the GDPR to learn more about developing a GDPR strategy and maintaining ongoing compliance.

7. FISMA

The Federal Information Security Management Act (FISMA) is a comprehensive cybersecurity framework that protects federal government information and systems against cyber threats.

FISMA also extends to third parties and vendors who work on behalf of federal agencies.

The FISMA security framework is aligned closely with NIST cybersecurity standards and requires agencies and third parties to maintain an inventory of their digital assets and identify any integrations between networks and systems.

Sensitive information must be categorized according to risk and security controls must meet minimum security standards as defined by FIPS and NIST 800 guidelines.

Impacted organizations must also conduct cybersecurity risk assessments, annual security reviews, and continuously monitor their IT infrastructure.

A cybersecurity framework can be a vital guidepost

Cybersecurity frameworks provide a useful (and often mandated) foundation for integrating cyber security risk management into your security performance management and third-party risk management strategy.

With a security framework as your guidepost, you'll gain vital insight into where your highest security risk is and feel confident communicating to the rest of the organization that you're committed to security excellence.

Lesson2 : Business Continuity

What Is Business Continuity?

Business continuity is an organization's ability to maintain or quickly resume acceptable levels of product or service delivery following a short-term event that disrupts normal operations. Examples of disruptions range from natural disasters to power outages.

Is business continuity the same as business resilience or disaster recovery?

Business continuity, disaster recovery, and business resilience are not the same, but they are related.

- Business continuity is a process-driven approach to maintaining operations in the event of an unplanned disruption such as a cyber attack or natural disaster. Business continuity planning covers the entire business—processes, assets, workers, and more. It isn't focused solely on IT infrastructure and business systems.
- Business resilience encompasses crisis management and business continuity. It requires a response to all types of risk that an organization may face. An organization that is business resilient is essentially in a constant state of "expecting the unexpected." It means continuously preparing to meet disruptions head-on, including events of extended duration that may affect more than one facility or region.
- Disaster recovery focuses specifically on how to restore an enterprise's IT infrastructure and business systems following a disruption. It is considered an element of business continuity. A business continuity plan (BCP) might contain several disaster recovery plans, for example.

What is a business continuity strategy?

A business continuity strategy is a summary of the mitigation, crisis, and recovery plans to be implemented after a disruption to resume normal operations. "Business continuity strategy" is often used interchangeably with "business continuity plan." Both consider the broader goals, legal and regulatory requirements, personnel, and even the business's clients and partners.

What does a business continuity plan mitigate?

A relevant and well-tested BCP can help ease the negative impacts of an unexpected business disruption in many ways.

- Financial impact: Disruptions to product supply chains and critical services to customers can directly affect sales and revenue. Downtime caused by unplanned disruptions can also result in higher costs for a business as it looks to repair operations and mitigate previously unidentified threats.

- Reputation and brand impact: Failure to resume operations quickly and supply customers with the products or services they expect can prompt customer defections and tarnish the brand. Damage to reputation can in turn cause investors and capital sources to pull back funding, exacerbating the financial impact of a business disruption.
- Regulatory impact: Customers and vendors are likely to complain when businesses fail to respond appropriately to disruptions, which may result in regulatory scrutiny or even censure. In highly-regulated industries, such as energy and financial services, business continuity planning is mandatory to ensure regulatory compliance.

Business continuity planning activities

A well-crafted and tested BCP can go a long way toward helping a business recover swiftly from a disruption. These are key steps a business may want to take.

Identifying critical business areas and functions

Business continuity planning begins with identifying an organization's key business areas and the critical functions within those areas. A business needs to determine and document the acceptable downtime for each area and function considered vital to operations. Then a plan to restore operations can be established, documented, and communicated.

Analyzing risks, threats, and potential impacts

Creating appropriate response scenarios requires knowing what disruptions the business could experience. An upfront analysis of risks and threats is necessary in order to prepare contingency responses to events. Organizations can also conduct a back-end analysis after an event to gather metrics and assess lessons learned. This information can drive improvements in how the business responds to disruptions.

Outlining and assigning responsibilities

A BCP details which personnel will be responsible for implementing specific aspects of the plan. It also identifies key decision-makers and a chain of command. The plan should include alternative options in case primary personnel are incapacitated or unavailable to respond to the disruption.

Defining and documenting alternatives

A business continuity plan should define and document alternative communication strategies in case telephone services or the internet are down. Enterprises should also have alternatives for mission-critical spaces such as data centers or manufacturing facilities in case buildings are damaged.

Assessing the need for critical backups

Essential equipment may be damaged or unavailable during a disruptive event. A business should consider whether it has access to backup equipment and uninterruptible power supplies (UPS) during extended power outages. Business-critical data needs to be backed up regularly, and is mandatory in many regulated industries.

Testing, training, and communication

Business continuity plans need to be tested to ensure they will be effective. (Disaster recovery plans should be tested as well.) A best practice is to conduct a plan review at least quarterly with leadership and key team members who are responsible for executing the plan.

Many companies use role-playing sessions, simulations, and other types of exercises several times per year to test their BCPs. This approach helps to identify gaps, develop strategies for improvement, and determine if more resources are needed. Targeted staff training and communicating to the whole workforce the benefits of having a business continuity plan are also vital to its success.

Lesson3 : Ethical Red Teaming

Red teaming 101: An introduction to red teaming and how it improves your cyber security

Red teaming is an attack technique used in cyber security to test how an organization would respond to a genuine cyber-attack. It is done through an Ethical Hacking team or similar offensive security team.

The ‘red team’ that simulates the attack is often an independent cyber security provider, while the organization's defensive cyber security capability is known as the ‘blue team’. The blue team aren’t given warning of the exercise so that the organization receiving the red teaming gains a realistic measure of its ability to respond to a genuine cyber-attack.

In this post, the first in a short series on red teaming, we will look at how red teaming works and how it helps organizations understand the effectiveness of security controls when it comes to thwarting realistic attacks from common threat actors.

What is a Red Team?

A red team is a form of penetration test (pen test) that has a very different set of goals to the more traditional pen test. While a typical pen test focuses on finding vulnerabilities and potentially exploiting them within a predefined set of company systems, a red team is target-driven and seeks to gain access to predetermined objectives by exploiting relevant weaknesses anywhere within an organization. It does not seek to provide an exhaustive list of vulnerabilities present.

The value of a red team is in simulating how an organization could be targeted in a real world attack and testing how the blue team responds to such an attack. The tactics, techniques and procedures (TTPs) of a red team are modelled on real-world malicious threat actors, with the goal of highlighting gaps in the security response.

Unlike in a penetration test, the organization's security team is usually not made aware of the red team exercise. This serves to safely and realistically test an organization's capabilities to detect and respond to an attack. As the two teams get to work, the blue team has to respond to the evolving techniques of the red team and they in turn adapt to the blue team and attempt to evade the controls that are in place. It is through the teams learning about each other's tools and techniques that the organization can get most real-world value. An evolution of these techniques is to deliberately create a co-operative purple team, but that's the **topic for another article.**

How does a Red Team work?

Just as no two companies are identical, neither are two red teams; however, the standard attack path typically follows this chain:

Initial access ⇾ Persistence ⇾ Privilege escalation ⇾ Command and control ⇾ Objective ⇾ Exfiltration of data

The attack chain is often informed from a threat Intelligence report, identifying relevant threat actors which the red team should emulate, or from current trends seen in the wild (such as human-operated ransomware, campaigns), and through the company’s own assessment of its weaknesses. A particular threat actor could be simulated by using the techniques observed in the wild, targeting the same types of services. Alternatively, their behaviors could be used as a baseline and adjusted to better suit the specific target.

The final attack may look something like this:

- A list of company employee email addresses is obtained from social media and other open-source intelligence (OSINT) sources. A crafted phishing email is then sent to these addresses containing a lure and an attached document. When opened, this drops custom malware on the victims’ machines providing the red team with access to the corporate network.
- Obtaining persistence through exploiting common machine misconfigurations/outdated software and hiding the custom malware somewhere where it is unlikely to be noticed by the security operations center (SOC).
- Exploiting and mapping the network, escalating privileges where required to grant further access while evading detection.
- Identifying paths to predetermined objectives (e.g. a finance database) using privileged credentials to achieve those objectives.
- Exfiltration of data from the target network to demonstrate the ways an attacker could remove sensitive information.

At any point in the assessment, the blue team may detect the malicious activity and terminate access. For example, the phishing campaign may be identified by an attentive user and reported. In these situations, a red team can adopt a 'leg up' where the target provides an initial foothold on the network without the need for the phishing campaign.

While this approach may seem counterintuitive, it serves to provide a more complete picture of an organization's cyber security by allowing the red team to continue to the next step of the attack chain. An important philosophy in security is that you must assume controls will fail, and it is important to have layered security to mitigate and restrict the damage when they do. Many organizations unintentionally have an armadillo security model (hard on the outside, soft on the inside), and are shocked at the level of freedom an attacker has once any perimeter defenses are bypassed.

With a sufficiently sophisticated social engineering campaign, an attacker will eventually succeed in persuading an employee to execute malware. When the internal network is compromised, there needs to be protection in place to limit the access of the attacker and to minimize the impact of the breach. This is where the leg-up grants a more complete picture of the target's security. It shows what happens when individual protections fail and what the monitoring solution detects when attackers try to bypass them.

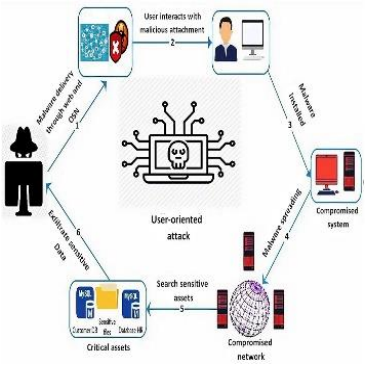
Red Team results

The test can last anywhere from weeks to months, but at the end the results are collated and a workshop is run with the blue team. The complexity of this workshop depends on the target. It can be:

- a high-level summary of where they performed well and where they can improve;
- a technical review of each attack and counterattack between the two teams; or,
- or a set up for a larger "find and fix" project the company wants to launch on the back of the red team.

Red teams offer a means of measuring response to specific scenarios as business operations change. For example, the 'unattended laptop' scenario which has changed, due to the dramatic shift to remote working in the pandemic, to a shared remote environment which has a different risk profile and possible attack paths. Red teams are ideal for companies that are keen to assess how good they are at preventing, detecting and responding to real world cyber-attacks.

Lesson4 : Cyber Threat Intelligence



Threat Intelligence

Our cyber threat intelligence team investigates and tracks cyber-attacks against organizations around the world. From this we build rich profiles of high-priority threat actor campaigns which we continuously update as new information is obtained. Our threat intelligence customers receive both technical data feeds and contextualized reports via a secure portal.

We also provide access to our technical experts, who can assist with investigating suspected cyber-attack activity. This spans the range of activities from deeply technical malware reverse-engineering to the broader understanding of socio-political situations and attribution analysis. Our threat intelligence services enable both enhanced threat detection and greater situational awareness.

In addition to regular reporting, our experts undertake bespoke assessments to understand how and why an organization might be attacked and who might be the perpetrators. This increases the value of penetration testing by ensuring it is conducted in accordance with the latest threat intelligence and is aligned to the business context. This intelligence led insight enables penetration testing services to be more targeted and focused in their approach

We are CREST and CBEST certified and provide threat intelligence services to regulated financial institutions, as well as broader industry and government.

Sign up to receive our summary Cyber Threat Bulletin updates of recent activity and emerging trends.

Penetration Testing

Penetration testing ensures that products, applications and networks are sufficiently robust to cope with cyber threats.

Prior to penetration testing being conducted, specific threat intelligence can be acquired to provide added insight into contemporary cyber risks. Penetration testing can then mimic the approaches that real, current threat actors can adopt in attacking the network; identifying relevant security weaknesses, vulnerabilities and possible attack vectors in the process.

These tests can be conducted so as to try and avoid detection wherever possible, emulating the approach a real attacker would take, identifying key security weaknesses and thus also testing the effectiveness of SOC and security monitoring capabilities: how soon do they detect an attack which is in progress and how do they respond?

This approach enables us to offer comprehensive and relevant recommendations which enable organizations to determine the best way to readjust or allocate resources to further enhance their protection and more effectively mitigate their cyber risk.

We are CREST certified and provide security testing services to government departments and to a wide range of industry sectors.

Emergency Response Services

When a successful cyber-attack impacts your network and business processes, we are here to support you. We offer a full range of expert emergency Cyber Incident Response services to enable you to act rapidly and effectively. We combine our technical skills with strategic guidance to make sure an organization makes the right decisions at the right times to limit the impact of these attacks.

Our expert incident response teams use world class and in-house developed tools to focus any incident investigation on uncovering the critical facts. If you have fallen victim to a targeted attack, our technology can be rapidly deployed to give unparalleled visibility of malicious behaviors.

If a breach of your security has already made the headlines or attracted regulator attention, then our team can help you move forward by managing internal and external stakeholders as well as the press.

We will respond within hours of a call to our 24/7 hotline for incidents around the world with remote support from one of our centers of excellence in the UK, US and Australia. We will also rapidly deploy to your site supported by BAE Systems offices and infrastructure around the globe.

We are CREST certified to provide cyber incident response services to government, critical national infrastructure and other operators of nationally significant networks.

Lesson5 : IT Governance

IT governance definition

IT governance is an element of corporate governance, aimed at improving the overall management of IT and deriving improved value from investment in information and technology.

IT governance frameworks enable organizations to manage their IT risks effectively and ensure that the activities associated with information and technology are aligned with their overall business objectives.

To understand how an organization's IT supports and enables the achievement of its strategies and objectives, read IT Governance – A Pocket Guide by Alan Calder.

Why is IT governance important?

IT governance enables an organization to :

- Demonstrate measurable results against broader business strategies and goals.
- Meet relevant legal and regulatory obligations, such as those set out in the GDPR (General Data Protection Regulation) or the Companies Act 2006.
- Assure stakeholders they can have confidence in your organization's IT services.
- Facilitate an increase in the return on IT investment; and
- Comply with certain corporate governance or public listing rules or requirements.

What is corporate governance ?

Corporate governance is *"a toolkit that enables management and the board to deal more effectively with the challenges of running a company. Corporate governance ensures that businesses have appropriate decision-making processes and controls in place so that the interests of all stakeholders are balanced."*- ICSA, The Governance Institute.

A robust corporate governance framework can help you meet the requirements of laws and regulations such as the DPA (Data Protection Act) 2018 and the GDPR.

For instance, the GDPR requires data controllers and processors to demonstrate their compliance with its requirements through certain documentation, including relevant logs, policies and procedures.

Harnessing the elements of IT governance will help you create and maintain appropriate policies and procedures to help meet your data privacy requirements.

Learn more about meeting your GDPR compliance obligations

IT governance frameworks, models and standards

ISO 38500 – The international IT governance standard

ISO/IEC 38500:2015 is the international standard for corporate governance of IT.

It sets out principles, definitions and a high-level framework that organisations of all types and sizes can use to better align their use of IT with organisational decisions and meet their legal, regulatory and ethical obligations.

Buy a copy of ISO/IEC 38500:2015

As well as ISO 38500, there are numerous widely recognised, vendor-neutral frameworks that organizations can use to implement an IT governance programme.

Each has its own IT governance strengths – for instance, COBIT focuses more on process management and ITIL on service management – but you might benefit from an integrated approach, using parts of several frameworks to deliver the results you need.

Follow the links below to find out more about each framework.

ITIL – IT service management

Widely adopted around the world, ITIL is a framework for ITSM (IT service management). Its latest iteration, ITIL 4, was launched in February 2019.

ITIL is supported by ISO/IEC 20000-1:2018 – the international standard for ITSM against which organisations can achieve independent certification.

Learn more about ITIL

Browse ITIL products

COBIT

COBIT (Control Objectives for Information and Related Technology) is an internationally recognised IT governance control framework that helps organisations meet business challenges in regulatory compliance, risk management and aligning IT strategy with organisational goals.

COBIT 2019, the latest iteration of the framework, was released in November 2018. It builds on COBIT 5, introducing new concepts and addressing the latest developments affecting enterprise IT.

Learn more about COBIT

Browse COBIT products

Calder-Moir IT Governance Framework

This framework provides structured guidance on how to approach IT governance. It can help benchmark the balance and effectiveness of IT governance practices within an organisation.

The IT Governance Control Framework Implementation Toolkit provides practical assistance and guidance for practitioners and board members tackling the subject.

Learn more about the Calder-Moir IT Governance Framework

The five domains of IT governance

The IT Governance Institute (a division of ISACA) breaks down IT governance into five domains:

1. Value delivery
2. Strategic alignment
3. Performance management
4. Resource management
5. Risk management

Other IT governance frameworks and models to consider

In addition to the frameworks listed above, there are several other models and frameworks you should consider for effective IT governance:

- King reports of corporate governance (versions I to IV).
- ISO/IEC 31000:2018 (risk management).
- ISO/IEC 27001:2013 (information security).
- Business continuity management and disaster recovery.
- Knowledge management, including intellectual capital.
- Programmed management and project governance, including PRINCE2® and PMBOK®.

IT governance auditing

As IT governance plays a curtail role in strategic performance, internal auditors are expected to include it in their audit plans.

Learn more about IT governance auditing

How to establish an IT governance framework

The challenge for many organizations is to establish a coordinated, integrated framework that draws on best-practice IT governance frameworks.

We offer a wide range of products and services, including books, toolkits and training courses, to support your organization's compliance with these frameworks. Browse our bestselling IT governance products and services below.

Lesson6 : Fraud

Internal organizational fraud

Sometimes called “occupational fraud,” this is when an employee, manager or executive of an organization deceives the organization itself. Think embezzlement, cheating on taxes, and lying to investors and shareholders.

External organizational fraud

This includes fraud committed against an organization from the outside, such as vendors who lie about the work they did, demand bribes from employees and rig costs. But customers sometimes defraud organizations, such as when they submit bad checks or try to return knock-off or stolen products. And increasingly, technology threatens organizations with theft of intellectual property or customer information.

Lesson7 : Workshop Group Discussion

What Is Fraud?

It's both simpler and more complicated than you think.

Fraud 101: What is Fraud

Defining Fraud

Why Do People Commit Fraud?

The Fraud Tree

Categories of Fraud

What Is Fraud, Anyway?

"Fraud" is any activity that relies on deception in order to achieve a gain. Fraud becomes a crime when it is a "knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment" (Black's Law Dictionary). In other words, if you lie in order to deprive a person or organization of their money or property, you're committing fraud.

Why Do People Commit Fraud?

The most widely accepted explanation for why some people commit fraud is known as the Fraud Triangle. The Fraud Triangle was developed by Dr. Donald Cressey, a criminologist whose research on embezzlers produced the term "trust violators."

The Fraud Triangle hypothesizes that if all three components are present

unshakeable financial need, perceived opportunity and rationalization — a person is highly likely to pursue fraudulent activities. As Dr. Cressey

explains in the *Fraud Examiners Manual*:

When the trust violators were asked to explain why they refrained from violation of other positions of trust they might have held at previous times, or why they had not violated the subject position at an earlier time, those who had an opinion expressed the equivalent of one or more of the following quotations: (a) 'There was no need for it like there was this time.' (b) 'The idea never entered my head.' (c) 'I thought it was dishonest then, but this time it did not seem dishonest at first.'

Helpful Resources

Fraud Resources

Tools & Guides

Reports & Statistics

Fraud Risk Tools

Videos

Podcasts

Become an ACFE Member

When you join the ACFE, you join a global community of experts who are uncovering and preventing fraud across every industry.

The Fraud Triangle

This short explainer video highlights how the Fraud Triangle is used to explain the reasons why people commit fraud:

The Fraud Tree

Occupational fraud contains a wide variety of specific schemes — each of which with its own tactics and goals. That's why we created the Fraud Tree, which classifies every type of occupational fraud.

Fraud Tree

Categories of Fraud

Unfortunately, fraud is so common that it can be categorized in countless ways.
But fundamentally, every type of fraud is either organizational or individual. Let's look at some key characteristics of each.

Against individuals

This is when a single person is targeted by a fraudster — including identity theft, phishing scams and "advance-fee" schemes. Perhaps one of the most noteworthy and devastating individual frauds is the Ponzi scheme.

Group Discussion Workshop: An Exercise in Experiential Learning

By Jill Pittendrigh on April 10, 2012

Discussions are a valuable learning tool, but what are the keys to motivating students to participate, and keeping them engaged? This enquiry formed the basis for the workshop In-Class Group Discussion Could Be Engaging and Fun. The workshop was facilitated by Michael Lee, Instructor and Curriculum Coordinator in the Department of Occupational Science and Occupational Therapy. Michael's belief in the importance of experiential learning was evident in the way the workshop was structured and facilitated, with participants being encouraged to enrich the content by sharing their own experiences related to the topic.

The workshop attendees represented various UBC Faculties, including, Arts, Science, Medicine and Pharmaceutical Science. Michael began the workshop by asking the group – many of whom had used group discussions in the classroom – what they hoped to learn from the session. The responses focused on a number of areas, including how to make discussions fun, how to achieve

consistent results, and what kinds of discussion strategies are recommended for higher education.

Ice Breaker

The first activity Michael had for the group was “Name Bingo”, an ice breaker game to get people involved, and help them discover shared commonalities. Each participant was given a sheet listing nine different characteristics – for example, “Bikes to Work,” “Is New to UBC,” or “Teaches a Class of More than 100.” The goal was to find a person in the group who was a match for each of the characteristics. The room soon became quite animated, with everyone up and circulating, asking questions of the other participants and exchanging information about themselves. “Bingo” was called as soon as the first person had completed the sheet.

Michael then moved on to the next part of the activity. Participants were asked to pair up with someone with whom they shared similar characteristics, and interview them for the purpose of introducing them to the group. The interview process revealed still more things the pairs had in common – whether in terms of their professional development, “we found we had taken similar career paths”, or their personal lives, “we both love sushi!”.

Group Discussions – The Pros and Cons

For the next activity, Michael divided the large group into two smaller groups, and asked them to discuss the pros and cons of small group discussions. Within their groups, participants shared thoughts and experiences related to the topic, and recorded their ideas on a flip chart. Michael circulated between the groups, supporting the discussions by validating insights, providing additional examples, and suggesting resources. At the end of the allotted time, all the attendees reassembled to report on the results.

On the “Pro” side, both groups agreed that in-class discussions increase the potential for individual participation. In a small group, everyone has a chance to speak – an important factor, in that people learn better when they are more involved. Students get to know one another more easily in a small group, and are more likely to express themselves. Students can also benefit from peer learning in small groups – communication between peers can help to simplify and clarify content, and allow students who have fallen behind to catch up. Another advantage of the group discussion format is that it allows for a longer exploration of a topic. The use of online discussion boards, moreover, can extend learning beyond the classroom.

In terms of the “Cons” or “Challenges” identified, some attendees felt that a lack of trust can be problematic in small group discussions. Students may not readily see the value of a group learning activity, and may be reluctant to accept the knowledge of their peers as valid. Group dynamics is another challenge: the effectiveness of a group discussion may vary, depending on the mix of individuals involved (introverts, extroverts). Similarly, differences in learning goals can affect the group discussion experience. For example, a student who is taking a course because it is required, rather than because it is a preferred choice, may be less motivated to participate. Group discussions can also present logistical problems for the facilitator – for example, the task of managing feedback effectively when a large number of groups are all reporting on the same topic.

Strategies for Promoting Participation and Engagement

Having examined some of the challenges, participants shared possible solutions, and strategies they have found effective in facilitating in-class group discussions:

Create a climate for sharing:
Use an activity such as an ice breaker to allow participants to get to know one another, and to promote trust.

1. Elicit a personal connection between the participants and the content:
Structure the discussion so that the topic resonates with the students' own lives.

2. Have virtual group discussions, using social media/blogs/online discussion boards:
For example, assign students the task of blogging about a website they feel is related to the course or topic.

3. Introduce accountability:
Incorporate group discussions into the marking structure by assigning a percentage of the grade for participation.

4. Use peer evaluation:
Have the groups evaluate other members of their group for their degree of participation.

5. Involve participants in the process:
For example, provide the topic, have each group formulate a question to be discussed, and then swap the questions between groups.

6. Use e-learning tools:
When working with larger groups, consider using **I Clickers** for reporting activities.

7. Employ the "Think-Pair-Share" strategy:
Allow students time to formulate and share ideas in pairs before presenting them to the group.

8. Vary reporting methods:
For example, provide students with "Scratch and Win" cards (used in the Faculty of Applied Sciences), or conduct a group quiz which introduces the element of anticipation (groups or students are called upon randomly to answer questions).

Reflecting on How Group Discussions Work

The final activity consisted of a reflection on the effectiveness of the day's group discussion exercise. Michael asked attendees to examine their experience in the group in terms of how ready people were to participate, what the dynamics had been, what had motivated people, and how the discussion progressed.

The participant responses highlighted some of the positive aspects of small group discussions, and provided some insights into how groups work. One participant acknowledged how the ice breaker game, at the beginning of the workshop, had increased the comfort level of the group, and made the discussion exercise more productive. Another participant noted the support she received from members of the group in response to sharing her difficulties using group

discussions in her classroom. She felt validated by their understanding, and appreciated the strategies they recommended to ameliorate the problems. This experience made her aware that students who are reticent to participate could also benefit from group learning, if successfully engaged. She pointed out, however, that instructors need to be aware of the differing learning styles of their students. For example, some students might learn more successfully by participating via an online discussion board.

Workshop Mirrors the Process

By participating in the workshop, attendees were involved in an active learning exercise. Their own experience in the group discussion process mirrored that of their students.

The ice breaker at the beginning established personal connections between people, which were then extended to the group. By the time participants got together for the small group discussion exercise, a comfortable atmosphere for sharing had been created. Group members were motivated by their mutual interest in using the group discussion format as a teaching tool. They shared with their peers, learned from them, received validation, and were offered practical suggestions for making their group discussions more effective.

The role of the facilitator, as demonstrated by Michael during the workshop, was to assist in moving the discussion process forward.

Involvement of Participants is Key to Success

Throughout the workshop, Michael emphasized the fact that many of the challenges involved in facilitating small groups discussions can be overcome through engagement. There are numerous strategies, tools, and methods, including those contributed during the session, which can be employed to this end. As the participants learned through direct experience in the workshop, group discussions can indeed be stimulating, enjoyable, and productive.

Michael’s final remarks served to summarize and reinforce the central message of the workshop, as well as to communicate his enthusiasm for the topic. “Make groups fun,” he reminded the participants, and “keep the group engaged!”

Unit Four : SDAIA

At the end of the unit, the trainee will be able to:

- Learn about international protection of cybersecurity

- Learn about the law on the protection of personal data

- Explain the methods used to protect data

- Learn about Interpol's efforts in protecting cybersecurity

Lesson1 : PDPL

Personal Data Protection Law (PDPL)

Article 1

For the purpose of implementing this Law, the following terms shall have the meanings assigned thereto, unless the context requires otherwise:
1-Law: The Personal Data Protection Law.
2-Regulations: The Implementing Regulations of the Law.
3-Competent Authority: The authority to be determined by a resolution of the Council of Ministers.
4-Personal Data: Any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature.
5-Processing: Any operation carried out on Personal Data by any means, whether manual or automated, including collecting, recording, saving, indexing, organizing, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing and destroying data.
6-Collection: The collection of Personal Data by Controller in accordance with the provisions of this Law, either from the Data Subject directly, a representative of the Data Subject, any legal guardian over the Data Subject or any other party.
7-Destruction: Any action taken on Personal Data that makes it unreadable and irretrievable, or impossible to identify the related Data Subject.
8-Disclosure: Enabling any person - other than the Controller or the Processor, as the case may be - to access, collect or use personal data by any means and for any purpose.
9-Transfer: The transfer of Personal Data from one place to another for Processing.
10-Publishing: Transmitting or making available any Personal Data using any written, audio or visual means.
11-Sensitive Data: Personal Data revealing racial or ethnic origin, or religious, intellectual or political belief, data relating to security criminal convictions and offenses, biometric or Genetic Data for the purpose of identifying the person, Health Data, and data that indicates

that one or both of the individual's parents are unknown.
12-Genetic Data: Any Personal Data related to the hereditary or acquired characteristics of a natural person that uniquely identifies the physiological or health characteristics of that person, and derived from biological sample analysis of that person, such as DNA or any other testing that leads to generating Genetic Data.
13-Health Data: Any Personal Data related to an individual's health condition, whether their physical, mental or psychological conditions, or related to Health Services received by that individual.
14-Health Services: Services related to the health of an individual, including preventive, curative, rehabilitative and hospitalizing services, as well as the provision of medications.
15-Credit Data: Any Personal Data related to an individual's request for, or obtaining of, financing from a financing entity, whether for a personal or family purpose, including any data relating to that individual's ability to obtain and repay debts, and the credit history of that person.
16-Data Subject: The individual to whom the Personal Data relate.
17-Public Entity: Any ministry, department, public institution or public authority, any independent public entity in the Kingdom, or any affiliated entity therewith.
18-Controller: Any Public Entity, natural person or private legal person that specifies the purpose and manner of Processing Personal Data, whether the data is processed by that Controller or by the Processor.
19-Processor: Any Public Entity, natural person or private legal person that processes Personal Data for the benefit and on behalf of the Controller.

Article 2

1-The Law applies to any Processing of Personal Data related to individuals that takes place in the Kingdom by any means, including the Processing of Personal Data related to individuals residing in the Kingdom by any means from any party outside the Kingdom. This includes the data of the deceased if it would lead to them or a member of their family being identified specifically.
2-The scope of applying the Law excludes the individual's Personal Data Processing for purposes that do not go beyond personal or family use, as long as the Data Subject did not publish or disclose it to others. The Regulations shall define personal and family use provided in this Paragraph.

Article 3

The provisions and procedures stated in this Law shall not prejudice any provision that grants a right to the Data Subject or confers better protection to Personal Data pursuant to any other law or an international agreement to which the Kingdom is a party.

Article 4

Data Subject shall have the following rights pursuant to this Law and as set out in the Regulations:
1-The right to be informed about the legal basis and the purpose of the Collection of their Personal Data.
2-The right to access their Personal Data held by the Controller, in accordance with the rules and procedures set out in the Regulations, and without prejudice to the provisions of Article (9) of this Law.
3-The right to request obtaining their Personal Data held by the Controller in a readable and clear format, in accordance with the controls and procedures specified by the Regulations.
4-The right to request correcting, completing, or updating their Personal Data held by the Controller.
5-The right to request a Destruction of their Personal Data held by the Controller when such Personal Data is no longer needed by Data Subject, without prejudice to the provisions of Article (18) of this Law.

Article 5

1-Except for the cases stated in this Law, neither Personal Data may be processed nor the purpose of Personal Data Processing may be changed without the consent of the Data Subject. The Regulations Shall set out the conditions of the consent, the cases in which the consent must be explicit, and the terms and conditions related to obtaining the consent of the legal guardian if the Data Subject fully or partially lacks legal capacity.
2-In all cases, Data Subject may withdraw the consent mentioned in Paragraph (1) of this Article at any time; the Regulations determines the necessary controls for such case.

Article 6

In the following cases, Processing of Personal Data shall not be subject to the consent referred to in Paragraph (1) of Article (5) herein:
1-If the Processing serves actual interests of the Data Subject, but communicating with the Data Subject is impossible or difficult.
2-If the Processing is pursuant to another law or in implementation of a previous agreement to which the Data Subject is a party.
3-If the Controller is a Public Entity and the Processing is required for security purposes or to satisfy judicial requirements.

4-If the Processing is necessary for the purpose of legitimate interest of the Controller, without prejudice to the rights and interests of the Data Subject, and provided that no Sensitive Data is to be processed. Related provisions and controls are set out in the Regulations.

Article 7

The consent referred to in paragraph (1) of Article (5) of this Law may not form a condition of providing a service or a benefit, unless such service or benefit is directly related to the Processing of Personal Data for which the consent is given.

Article 8

Subject to the provisions of this Law and the Regulations regarding the Disclosure of Personal Data, the Controller shall only select Processors providing the necessary guarantees to implement the provisions of this Law and the Regulations. The Controller shall also monitor the compliance of said Processors with the provisions of this Law and the Regulations. This shall not prejudice the Controller's responsibilities towards the Data Subject or the Competent Authority as the case may be. The Regulations shall set out the provisions necessary in this regard, including provisions related to any subsequent contracts conducted by the Processor.

Article 9

1-The Controller may set time frames for exercising the right to access Personal Data stated in Paragraph (2) of Article (4) herein as stipulated in the Regulations. The Controller may limit the exercise of this right in the following cases:
a) If this is necessary to protect the Data Subject or other parties from any harm, according to the provisions set forth the Regulations.
b) If the Controller is a Public Entity and the restriction is required for security purposes, required by another law, or required to fulfill judicial requirements.
2-The Controller shall prevent the Data Subject from accessing Personal Data in any of the situations stated in Paragraphs (1, 2, 3, 4, 5) and (6) of Article (16) herein.

Article 10

The Controller may only collect Personal Data directly from the Data Subject and may only process Personal Data for the purposes for which they have been collected. However, the Controller may collect Personal Data from a source other that the Data Subject and may process Personal Data for purposes other than the ones for which they have been collected in the following situations:
1- The Data Subject gives their consent in accordance with the provisions of this Law.
2- Personal Data is publicly available or was collected from a publicly available source.

3- The Controller is a Public Entity, and the Collection or Processing of the Personal Data is required for public interest or security purposes, or to implement another law, or to fulfill judicial requirements.
4- Complying with this may harm the Data Subject or affect their vital interests
5- Personal Data Collection or Processing is necessary to protect public health, public safety, or to protect the life or health of specific individuals.
6- Personal Data is not to be recorded or stored in a form that makes it possible to directly or indirectly identify the Data Subject.
7- Personal Data Collection is necessary to achieve legitimate interests of the Controller, without prejudice to the rights and interests of the Data Subject, and provided that no Sensitive Data is to be processed.
The Regulations shall set out the provisions, controls and procedures related to what is stated in paragraphs (2) to (7) of this Article.

Article 11

Action is achieved shall be
avoided. The Regulations shall set out the necessary controls in this regard.
4- If the Personal Data collected is no longer necessary for the purpo -1The purpose for which Personal Data is collected shall be directly related to the

Controller's purposes, and shall not contravene any legal provisions.
2- The methods and means of Personal Data Collection shall not conflict with any legal provisions, shall be appropriate for the circumstances of the Data Subject, shall be direct, clear and secure, and shall not involve any deception, misleading or extortion.
3- The content of the Personal Data shall be appropriate and limited to the minimum amount necessary to achieve the purpose of the Collection. Content that may lead to

specifically identifying Data Subject once the purpose of Collese for which it has been collected, the Controller shall, without undue delay, cease their Collection and destroy previously collected Personal Data.

Article 12

The Controller shall use a privacy policy and make it available to Data Subjects for their information prior to collecting their Personal Data. The policy shall specify the purpose of Collection, Personal Data to be collected, the means used for Collection, Processing, storage and Destruction, and information about the Data Subject rights and how to exercise such rights.

Article 13

When collecting Personal Data directly from the Data Subject, the Controller shall take appropriate measures to inform the Data Subject of the following upon Collection:
1- The legal basis for collecting their Personal Data.

2- The purpose of the Collection, and shall specify the Personal Data whose Collection is mandatory and the Personal Data whose Collection is optional. The Data Subject shall be informed that the Personal Data will not be subsequently processed in a manner inconsistent with the Collection purpose or in cases other than those stated in Article (10) of this Law.
3- Unless the Collection is for security purposes, the identity of the person collecting the Personal Data and the address of its representative, if necessary.
4- The entities to which the Personal Data will be disclosed, the capacity of such entities, and whether the Personal Data will be transferred, disclosed or processed outside the Kingdom.
5- The potential consequences and risks that may result from not collecting the Personal Data.
6- The rights of the Data Subject pursuant to Article (4) herein.
7- Such other elements as set out in the Regulations based on the nature of the activity done by the Controller.

Article 14

The Controller may not process Personal Data without taking sufficient steps to verify the Personal Data accuracy, completeness, timeliness and relevance to the purpose for which it is collected in accordance with the provisions of the Law.

Article 15

The Controller may not Disclose Personal Data except in the following situations:
1- Data Subject consents to the Disclosure in accordance with the provisions of the Law.
2- Personal Data has been collected from a publicly available source.
3- The entity requesting Disclosure is a Public Entity, and the Collection or Processing of the Personal Data is required for public interest or security purposes, or to implement another law, to fulfill judicial requirements.
4- The Disclosure is necessary to protect public health, public safety, or to protect the lives or health of specific individuals.
5- The Disclosure will only involve subsequent Processing in a form that makes it impossible to directly or indirectly identify the Data Subject.
6- The Disclosure is necessary to achieve legitimate interests of the Controller, without prejudice to the rights and interests of the Data Subject, and provided that no Sensitive Data is to be processed.
The Regulations shall set out the provisions, controls and procedures related to what is stated in paragraphs (2) to (6) of this Article.

Article 16

The Controller shall not disclose Personal Data in the situations stated in Paragraphs (1, 2, 5) and (6) of Article (15) if the Disclosure:
1- Represents a threat to security, harms the reputation of the Kingdom, or conflicts with the interests of the Kingdom.
2- Affects the Kingdom's relations with any other state.
3- Prevents the detection of a crime, affects the rights of an accused to a fair trial, or affects the integrity of existing criminal procedures.
4- Compromises the safety of an individual.
5- Results in violating the privacy of an individual other than the Data Subject, as set out in the Regulations.
6- Conflicts with the interests of a person that fully or partially lacks legal capacity.
7- Violates legally established professional obligations.
8- Involves a violation of an obligation, procedure, or judicial decision.
9- Exposes the identity of a confidential source of information in a manner detrimental to the public interest.

Article 17

1- If Personal Data is corrected, completed or updated, the Controller shall notify such amendment to all the other entities to which such Personal Data has been transferred and make the amendment available to such entities.
2- The Regulations shall set out the time frames for correction and updating of

Personal Data, types of correction, and the procedures required to avoid the consequences of Processing incorrect, inaccurate or outdated Personal Data.

Article 18

1- The Controller shall, without undue delay, Destroy the Personal Data when no longer necessary for the purpose for which they were collected. However, the Controller may retain data after the purpose of the Collection ceases to exist; provided that it does not contain anything that may lead to specifically identifying Data Subject pursuant to the controls stipulated in the Regulations.

2- In the following cases, the Controller shall retain the Personal Data after the purpose of the Collection ceases to exist:

a) If there is a legal basis for retaining the Personal Data for a specific period, in which case the Personal Data shall be destroyed upon the lapse of that period or when the purpose of the Collection is satisfied, whichever longer.

b) If the Personal Data is closely related to a case under consideration before a judicial authority and the retention of the Personal Data is required for that purpose, in which case the Personal Data shall be destroyed once the judicial procedures are concluded.

Article 19

The Controller shall implement all the necessary organizational, administrative and technical measures to protect Personal Data, including during the Transfer of Personal Data, in accordance with the provisions and controls set out in the Regulations.

Article 20

1- The Controller shall notify the Competent Authority upon knowing of any breach, damage, or illegal access to personal data, in accordance with the Regulations.

2- The Controller shall notify the Data Subject of any breach, damage or illegal access to their Personal Data that would cause damage to their data or cause prejudice to their rights and interests, in accordance with the Regulations.

Article 21

The Controller shall respond to the requests of the Data Subject pertaining to their rights under this Law within such period and in such method as set out in the Regulations.

Article 22

The Controller shall conduct an impact assessment of Personal Data Processing in relation to any product or service, based on the nature of the activity carried out by the Controller, in accordance with the relevant provisions of the Regulations.

Article 23

Without prejudice to this Law, the Regulations shall set out additional controls and procedures for the Processing of Health Data in a manner that ensures the privacy of the Data Subject and protects their rights under this Law. Such additional controls and procedures shall include the following:

1- Restricting the right to access Health Data, including medical files, to the minimum number of employees or workers and only to the extent necessary to provide the required Health Services.

2- Restricting Health Data Processing procedures and operations to the minimum

extent possible of employees and workers as necessary to provide Health Services or offer health insurance programs.

Article 24

Article 25

With the exception of the awareness-raising materials sent by Public Entities, Controller may not use personal means of communication, including the post and email, of the Data Subject to send advertising or awareness-raising materials, unless:

1- Obtaining the prior consent of the targeted recipient for such materials.

2- The sender of the material shall provide a clear mechanism, as set out in the Regulations, that enables the targeted recipient to reWithout prejudice to this Law, the Regulations shall set out additional controls and

procedures for the Processing of Credit Data in a manner that ensures the privacy of the Data Subject and protects their rights under this Law and the Credit Information Law. Such controls and procedures shall include the following:

1- Implementing appropriate measures to verify that the Data Subject has given their explicit consent to the Collection of the Personal Data, changing the purpose of the Collection, or Disclosure or Publishing of the Personal Data in accordance with the provisions of this Law and the Credit Information Law.

2- Requiring that the Data Subject be notified when a request for Disclosure of their Credit Data is received from any entity.

quest stopping receiving such
materials if they desire so.

3- The Regulations shall set out the provisions concerning the aforementioned advertising and awareness-raising materials, as well as the conditions and situations concerning the consent of the recipient to receive aforementioned materials.

Article 26

With the exception of Sensitive Data, Personal Data may be processed for marketing purposes, if it is collected directly from the Data Subject and their consent is given in accordance with the provisions of Law; the Regulations shall set out the controls in such regard.

Article 27

Personal data may be collected or processed for scientific, research, or statistical purposes without the consent of the Data Subject in the following situations:

1-If it does not specifically identify the Data Subject.

2-If evidence of the Data Subject’s identity will be destroyed during the Processing and prior to Disclosure of such data to any other entity, if it is not Sensitive Data.

Lesson2 : Data Classification

What is Data Classification?

What is Data Classification?

With organizations expected to handle massive amounts of data over the course of everyday operations, it can become a major challenge to locate information quickly and to ensure that no sensitive or otherwise valuable data is left vulnerable.
A key part of maintaining visibility and control over this information is data classification.

Data classification is the continuous practice of tagging and organizing data into pre-defined categories, making it easier to locate and retrieve but also enforcing secure access for authorized users. In this introductory data classification guide, we will look at how the practice is essential for good data management, along with why it should be a critical component of your data security strategy.

Why Data Classification is Important for Cybersecurity

Why classify data? In addition to making information easier to locate, it comprises an essential element in cybersecurity best practices. One of the greatest benefits of data classification is that you can tag progressively more sensitive types of data and use the categories to determine automated security responses to attempts to access, transmit or copy data.

Depending upon the level of risk, this may involve restricting access or simply auditing an interaction so it is available for future review. By ensuring that security teams know where to find sensitive information and by putting rules in place about who is allowed to access it, you can prevent or contain data breaches and keep unauthorized users away from resources they shouldn't have. Proper data classification practices are necessary for maintaining a strong security posture.

Types of Data Classification

There are three primary types of data classification, each of which carries its own pros and cons, and different data classification solutions may focus on different approaches. Which approach you primarily use will depend upon factors such as the size of your organization, the training level of your users or the proportion of your data that would be considered sensitive.

- **Content-based classification:** This is the practice of examining files and searching for sensitive information inside them. This can be helpful if you have a problem of information that is not for public consumption hiding in seemingly innocuous file types. But you also run the risk of generating false positives that waste employee time.
- **Context-based classification:** Instead of examining file contents directly, this approach primarily looks at the metadata associated with files to find clues indicating that data inside is sensitive. This may include identifying the location where a file is saved, which user created it or which application the file is built for. This approach works well when

your user base is well trained and you already have a degree of control over your sensitive data.

- **User-based classification:** This puts the burden upon users to comb through files and categorize them. While at its best this approach can significantly cut down on false positives, it relies upon having not only a highly trained user base but also the time to manually classify data. That means that it is typically only suitable for a leaner organization or a smaller dataset.

Data Sensitivity Levels

Most organizations distinguish among three levels of data risk, although your own needs might lead you to use a different number. It is important to note that these risk levels are not synonymous with data categories. In this list we will look at the three main risk levels and which data categories tend to correspond to each level; however, a category such as Personally Identifiable Information (PII) may fall anywhere on the risk spectrum from low to high, depending upon the company mission and what type of information is being gathered.

- **Low risk:** This data is safe for public consumption and does not need present a danger if it leaks. This tends to also mean that it is either easy to replace if it goes missing or not important to the organization's operations. Some internal information may present a lower risk if its release would not present a competitive edge or damage an organization's reputation.
- **Moderate risk:** This data is usually intended for internal consumption and should not be released to public view, but it does not present a major threat to the organization's mission if leaked. This might include company records with no potential reputational risk but that might be difficult to replace if lost. Some organizations will use different categories for basic internal data and confidential information.
- **High risk:** Any data that has a direct bearing on organizational operations will fall under this level of risk. This includes proprietary information such as trade secrets. Data with a high risk level should have access tightly controlled and may beneficially be stored in an encrypted format.

Data Classification Best Practices

Getting the most out of data classification requires taking proactive measures in several areas. These include:

- **Identification** – Find where your sensitive data resides, including cloud repositories and physical hard drives, and take any necessary immediate steps to secure them with encryption, physical access controls, etc.
- **Organization** – Come up with the scheme that you will use to organize data into categories. Don't get overly elaborate; the fewer categories you use, the more effective your classification activities will be.

- **Training** – Empower employees to take a role in tagging data and placing it in the proper place based on its category. The more people who have a role in the process, the more stringent your training needs to be to make sure that human error doesn't compromise your efforts.
- **Compliance** – Go to the effort of understanding the applicable data security and data privacy regulations for your operations, along with the penalties for noncompliance. See below for more about regulatory compliance.
- **Solutions** – Locate the data classification solution that best suits your organization. In many cases it can be best to utilize a comprehensive data security platform that can assist with data discovery, classification and prioritization instead of patching together different solutions from various vendors.

Data Classification and Data Security Compliance

If your organization has a global footprint, there are likely multiple regulations dictating how you are expected to care for your data. Take time to understand the requirements of applicable regulations, which may include GDPR, HIPAA or PCI DSS. Especially when it comes to PII and Personal Health Information (PHI), your data classification practices should be drawn up in line with pertinent regulations. These will often impact where sensitive data is stored and how quickly it can be retrieved on demand. A good data classification solution can help you to anticipate your regulatory needs and respond quickly to audits and information requests.

Forcepoint Data Classification

You can increase the accuracy and efficiency of your data classification practices with Forcepoint Data Classification powered by Getvisibility. This solution leverages Machine Learning (ML) and Artificial Intelligence (AI) to more accurately classify unstructured data, all while covering the broadest range of data types in the industry. You can increase the increase the speed and efficiency of data classification to reduce false positives and spend more time on legitimate data security incidents.

And when you integrate Forcepoint Data Classification with Forcepoint Data Loss Prevention (DLP), you can select the requirements and criteria for data classification to easily deploy Forcepoint Data Classification into Forcepoint DLP and Forcepoint ONE integrated DLP policies

Lesson3 : Data Sharing

What is data sharing?

Data sharing is the ability to make the same data available to one or many consumers. The ever-growing amount of data has become a strategic asset for any company. Sharing data — within business units as well as consuming data from external sources - is an enabling technology for new

business opportunities. Sharing data allows you to collaborate with partners, establish new partnerships, and generate new revenue streams with data monetization.

What are the types of data sharing?

There are many different types of data sharing, including sharing within an organization and sharing outside of an organization, one-on-one sharing, sharing with multiple recipients, public sharing, and private sharing. Companies may use public or private data marketplaces to enhance their data sharing and collaboration as well as privacy-safe data clean rooms for sensitive data, such as personally identifiable information (PII).

What are the challenges of data sharing?

Data sharing is essential to modern businesses, but it can be challenging. One of the most critical of these challenges is security. Sharing only the right data with the right people within the right context requires strategic policies, effective tools and intentional processes that are consistently followed. Data governance — ensuring that data is used in compliance with specific regulations — is another challenge. In addition, technical and structural data management issues such as managing multiple systems and legacy or proprietary solutions can place roadblocks in the way of efficient and effective data sharing.

What are the benefits of data sharing in an organization?

Data sharing is crucial for the evolution of the data-driven business model. Gartner predicts that by 2024, organizations that promote data sharing will outperform their peers on most business value metrics. Data sharing eliminates data silos, resulting in greater efficiency and transparency and increased collaboration within an organization, as well as with partners. Data sharing also provides organizations with new and faster time to insights that help improve performance. Finally, data sharing provides possibilities for revenue streams by enabling an organization to offer new data products or services.

Traditional data sharing technologies

Legacy technologies such as SFTP (secure file transfer protocol), email, or APIs (application programming interface) allow the implementation of vendor-agnostic homegrown solutions that will work both on-premises and on clouds. However, they are often costly to manage and maintain and are increasingly difficult to secure and govern as modern data requirements have evolved. Using these solutions can make data sharing complex and time-consuming, and they don't scale to accommodate large datasets.

Cloud object storage is a good fit for the cloud because its scalability supports unlimited data growth. It's widely available, cheap, and reliable, but there are downsides. For example, recipients must be on the same cloud to access the data, and security and governance processes can be complicated. In addition, sharing large volumes of data via cloud storage is time-consuming, cumbersome and nearly impossible to scale.

Commercial/closed source data sharing offerings

Data sharing solutions are baked into vendor products such as Oracle, Amazon Redshift or Snowflake. These solutions are convenient to use within a product and allow users to share data easily with anyone who uses the same platform. However, users can't share data with users of competing solutions and vendors often limit scalability. With these solutions, data must be loaded onto the platform, which requires extract, transform and load (ETL) and creates data copies. All these restrictions create complexity, version control issues and higher costs for sharing data with recipients on different cloud platforms.

Open source, modern data sharing solutions

In today's reality of sometimes complex infrastructures with multiple platforms, having an open source data sharing solution can offer valuable flexibility. Open source-based solutions eliminate the lock-in of vendor products and bring a number of additional benefits such as community-developed integrations with popular, open source data processing frameworks. Open protocols also allow the easy integration of commercial clients, such as BI tools.

Data marketplaces

Data marketplaces enable data sharing and data monetization, and they are important tools in data sharing and collaboration. Marketplaces can take different forms, including:

- Internal data marketplaces for data sharing within a company
- Private data marketplaces for data sharing with trusted partners
- Public data marketplaces that connect data providers and consumers

Public data marketplaces offer participants the opportunity to buy and sell data and related services in a secure environment offering high quality and consistency directly from the data providers. Companies may use marketplaces to acquire third-party data to enrich their existing data, or offer and monetize new data products and services.

Data clean rooms

Data clean rooms allow businesses to easily collaborate in a secure, governed environment with customers and partners on any cloud in a privacy-safe way. Within a data clean room, multiple participants can join their first-party data and perform analysis on the data without the risk of exposing their data to other participants. Participants have full control of their data and can decide which participants can perform analysis on their data without exposing any sensitive data such as PII.

Delta Sharing

Delta Sharing is the world's first open protocol for secure data sharing, making it simple for organizations to share data with other organizations regardless of which computing platforms they use.

- **Share live data directly —** Easily share existing, live data in your Delta Lake without copying it to another system.

- **Supports diverse clients —** Data recipients can directly connect to Delta Shares from pandas, Apache Spark™, Rust and other systems without having to first deploy a specific compute platform. Reduce the friction to get your data to your users.
- **Security and governance —** Delta Sharing allows you to easily govern, track and audit data access.
- **Scalability -** Share large-scale datasets reliably and efficiently by leveraging cloud storage systems like S3, ADLS and GCS.

Delta Sharing on Databricks

Databricks natively integrates with Delta Sharing in Unity Catalog, providing a streamlined experience for sharing data both within and across organizations. Recipients don't have to be on the Databricks platform, on the same cloud, or on a cloud at all.

Delta Sharing delivers several key benefits, including:

- Open cross-platform sharing
- Live data sharing without replication
- Centralized governance
- The ability to share data products, including AI models, dashboards, and notebooks, with greater flexibility
- Lower cost
- Reduced time to value

Delta Sharing is an open ecosystem of open source and commercial partners that continues to grow. Databricks has recently expanded Delta Sharing partnerships to include Cloudflare, Dell, Oracle and Twilio.

Lesson4 : Workshop Group Discussion

Group Discussion Workshop: An Exercise in Experiential Learning

Discussions are a valuable learning tool, but what are the keys to motivating students to participate, and keeping them engaged? This enquiry formed the basis for the workshop *In-Class Group Discussion Could Be Engaging and Fun*. The workshop was facilitated by Michael Lee, Instructor and Curriculum Coordinator in the Department of Occupational Science and Occupational Therapy. Michael's belief in the importance of experiential learning was evident in the way the workshop was structured and facilitated, with participants being encouraged to enrich the content by sharing their own experiences related to the topic.

The workshop attendees represented various UBC Faculties, including, Arts, Science, Medicine and Pharmaceutical Science. Michael began the workshop by asking the group – many of whom had used group discussions in the classroom – what they hoped to learn from the session. The responses focused on a number of areas, including how to make discussions fun, how to achieve

consistent results, and what kinds of discussion strategies are recommended for higher education.

Ice Breaker

The first activity Michael had for the group was “Name Bingo”, an ice breaker game to get people involved, and help them discover shared commonalities. Each participant was given a sheet listing nine different characteristics – for example, “Bikes to Work,” “Is New to UBC,” or “Teaches a Class of More than 100.” The goal was to find a person in the group who was a match for each of the characteristics. The room soon became quite animated, with everyone up and circulating, asking questions of the other participants and exchanging information about themselves. “Bingo” was called as soon as the first person had completed the sheet.

Michael then moved on to the next part of the activity. Participants were asked to pair up with someone with whom they shared similar characteristics, and interview them for the purpose of introducing them to the group. The interview process revealed still more things the pairs had in common – whether in terms of their professional development, “we found we had taken similar career paths”, or their personal lives, “we both love sushi!”.

Group Discussions – The Pros and Cons

For the next activity, Michael divided the large group into two smaller groups, and asked them to discuss the pros and cons of small group discussions. Within their groups, participants shared thoughts and experiences related to the topic, and recorded their ideas on a flip chart. Michael circulated between the groups, supporting the discussions by validating insights, providing additional examples, and suggesting resources. At the end of the allotted time, all the attendees reassembled to report on the results.

On the “Pro” side, both groups agreed that in-class discussions increase the potential for individual participation. In a small group, everyone has a chance to speak – an important factor, in that people learn better when they are more involved. Students get to know one another more easily in a small group, and are more likely to express themselves. Students can also benefit from peer learning in small groups – communication between peers can help to simplify and clarify content, and allow students who have fallen behind to catch up. Another advantage of the group discussion format is that it allows for a longer exploration of a topic. The use of online discussion boards, moreover, can extend learning beyond the classroom.

In terms of the “Cons” or “Challenges” identified, some attendees felt that a lack of trust can be problematic in small group discussions. Students may not readily see the value of a group learning activity, and may be reluctant to accept the knowledge of their peers as valid. Group dynamics is another challenge: the effectiveness of a group discussion may vary, depending on the mix of individuals involved (introverts, extroverts). Similarly, differences in learning goals can affect the group discussion experience. For example, a student who is taking a course because it is required, rather than because it is a preferred choice, may be less motivated to participate. Group discussions can also present logistical problems for the facilitator – for example, the task of managing feedback effectively when a large number of groups are all reporting on the same topic.

Strategies for Promoting Participation and Engagement

Having examined some of the challenges, participants shared possible solutions, and strategies they have found effective in facilitating in-class group discussions:

1. Create a climate for sharing:
   Use an activity such as an ice breaker to allow participants to get to know one another, and to promote trust.

2. Elicit a personal connection between the participants and the content:
   Structure the discussion so that the topic resonates with the students' own lives.

3. Have virtual group discussions, using social media/blogs/online discussion boards:
   For example, assign students the task of blogging about a website they feel is related to the course or topic.

4. Introduce accountability:
   Incorporate group discussions into the marking structure by assigning a percentage of the grade for participation.

5. Use peer evaluation:
   Have the groups evaluate other members of their group for their degree of participation.

6. Involve participants in the process:
   For example, provide the topic, have each group formulate a question to be discussed, and then swap the questions between groups.

7. Use e-learning tools:
   When working with larger groups, consider using iClickers for reporting activities.

8. Employ the "Think-Pair-Share" strategy:
   Allow students time to formulate and share ideas in pairs before presenting them to the group.

9. Vary reporting methods:
   For example, provide students with "Scratch and Win" cards (used in the Faculty of Applied Sciences), or conduct a group quiz which introduces the element of anticipation (groups or students are called upon randomly to answer questions).

Reflecting on How Group Discussions Work

The final activity consisted of a reflection on the effectiveness of the day's group discussion exercise. Michael asked attendees to examine their experience in the group in terms of how ready people were to participate, what the dynamics had been, what had motivated people, and how the discussion progressed.

The participant responses highlighted some of the positive aspects of small group discussions, and provided some insights into how groups work. One participant acknowledged how the ice

breaker game, at the beginning of the workshop, had increased the comfort level of the group, and made the discussion exercise more productive. Another participant noted the support she received from members of the group in response to sharing her difficulties using group discussions in her classroom. She felt validated by their understanding, and appreciated the strategies they recommended to ameliorate the problems. This experience made her aware that students who are reticent to participate could also benefit from group learning, if successfully engaged. She pointed out, however, that instructors need to be aware of the differing learning styles of their students. For example, some students might learn more successfully by participating via an online discussion board.

Workshop Mirrors the Process

By participating in the workshop, attendees were involved in an active learning exercise. Their own experience in the group discussion process mirrored that of their students.

The ice breaker at the beginning established personal connections between people, which were then extended to the group. By the time participants got together for the small group discussion exercise, a comfortable atmosphere for sharing had been created. Group members were motivated by their mutual interest in using the group discussion format as a teaching tool. They shared with their peers, learned from them, received validation, and were offered practical suggestions for making their group discussions more effective.

The role of the facilitator, as demonstrated by Michael during the workshop, was to assist in moving the discussion process forward.

Involvement of Participants is Key to Success

Throughout the workshop, Michael emphasized the fact that many of the challenges involved in facilitating small groups discussions can be overcome through engagement. There are numerous strategies, tools, and methods, including those contributed during the session, which can be employed to this end. As the participants learned through direct experience in the workshop, group discussions can indeed be stimulating, enjoyable, and productive.

Michael's final remarks served to summarize and reinforce the central message of the workshop, as well as to communicate his enthusiasm for the topic. "Make groups fun," he reminded the participants, and "keep the group engaged!"

Unit Five : Mapping with international standards

At the end of the unit, the trainee will be able to:

- Explains the technical principles of dealing with information systems

- Learns the rules for the safe use of information systems in institutions

- Learns how to draw maps according to international standards

- Shows the extent of the danger of attacks directed at information systems

Lesson1 : Mapping with international standards

International Mapping Standards Updated for Planets throughout Solar System

The internationally agreed upon standards for mapping planets and objects other than Earth throughout the solar system have been updated in a new report led by the U.S. Geological Survey. These standards include definitions of the latitude and longitude systems and body size and shape for all mapped objects.

The new parameters can be universally used by planetary science researchers to assign geographic position information to their data sets, allowing them to be registered and compared at known levels of accuracy and precision.

“These new standards ensure that anyone around the world, including individual scientists, instrument teams, spacecraft missions and space agencies, can make maps and geographically register information that can be compared and used interchangeably,” said Brent Archinal, a USGS scientist and the lead author of the study. “The recommended parameters will also allow for accurate and safe navigation of spacecraft near solar system bodies.”

Archinal is the chair of the Working Group for Cartographic Coordinates and Rotational Elements, the international group of scientists who have been given the responsibility by the International Astronomical Union to define the rotational elements of the planets, satellites, asteroids and comets of the solar system on a systematic basis. The WGCCRE issues a report approximately every three years that describes the most up-to-date recommendations for the latitude and longitude and rotational elements of all planetary bodies. The current report consolidates recommendations made at the 2015 meeting of the IAU.

These new parameters have provided a significant improvement to the coordinates on Mars. The previous model recommended by the working group had an error level of many tens of meters over 20-30 years, while the new model has a level of error at the 10-meter level over such periods. The new standards also provide a more accurate definition of the zero degrees longitude, or the prime meridian location, of Mars.

The USGS Astrogeology Science Center in Flagstaff, Arizona, has a long history of assisting the IAU with planetary cartography, as well as planetary nomenclature. The USGS Astrogeology Science Center is a national resource for the integration of planetary geoscience, cartography

and remote sensing. The center was established in 1963 to provide lunar geologic mapping for NASA and assist in training astronauts destined for the moon. Throughout the years, the USGS has participated in processing and analyzing data from numerous missions to planetary bodies in our solar system, and collaborates with the planning and operation of space exploration missions.

Get Our News

These items are in the RSS feed format (Really Simple Syndication) based on categories such as topics, locations, and more. You can install and RSS reader browser extension, software, or use a third-party service to receive immediate news updates depending on the feed that you have added. If you click the feed links below, they may look strange because they are simply XML code. An RSS reader can easily read this code and push out a notification to you when something new is posted to our site.

Unit Six : Assessment and Audit

At the end of the unit, the trainee will be able to:

- Shows how to evaluate and refine data
- Explains how to develop measures for key performance indicators
- Learns the rules for developing and building a work plan
- Explains the technical principles for dealing with and auditing data

Lesson1 : Assessment and Audit

What is the Difference Between Assessment and Audit?

What is the difference between assessment and audit when it comes to security in the IT industry? In an era where cybersecurity threats are constantly evolving, organizations need to have a robust security posture to protect sensitive data and maintain the trust of their customers and stakeholders.

Assessments and audits are critical tools in this endeavor, providing organizations with a comprehensive view of their security posture and helping them identify potential vulnerabilities and risks. While assessments and audits are often used interchangeably, the two have some key differences. Want to know what they are? Read on!

What is the difference between assessment and audit?

An assessment is an internal evaluation of an organization's security posture. In contrast, an audit is an external evaluation of an organization's compliance with specific external standards or regulations.

Assessment

Assessments aim to identify **potential security weaknesses** and evaluate the effectiveness of existing security controls. There are different types, such as vulnerability assessments, risk assessments, and penetration testing.

Audit

Audits, on the other hand, are typically performed to verify **compliance with specific standards or regulations**, such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), or the General Data Protection Regulation (GDPR). They typically involve a detailed review of policies, procedures, and controls to ensure they meet the relevant standard or regulation requirements.

Assessment vs. audit

The key differences between assessment and audit are the following:

1. Internal security teams or third-party consultants often conduct assessments. In contrast, audits are typically conducted by certified external auditors who are trained to follow a specific set of standards or guidelines.

2. The primary objective of an assessment is to evaluate an organization's security controls and identify potential risks and vulnerabilities. At the same time, an audit measures how well an organization meets a set of external standards.

3. Assessments are usually conducted more frequently to ensure that security controls remain effective, while audits are typically conducted annually or on a specific schedule.

4. Assessments are often more flexible regarding scope and methodology, while audits are typically more rigid and follow specific standards or guidelines.

Why are assessments and audits important?

Assessments and audits are essential to maintaining a strong security posture in the IT industry. They help organizations identify security risks, prioritize remediation efforts, and demonstrate compliance with regulatory requirements. The following are some reasons why assessments and audits are critical.

1. Identify security risks

Assessments and audits provide organizations with a comprehensive view of their security posture, enabling them to **identify potential security risks and vulnerabilities**. By conducting them, organizations can identify gaps in their security controls and proactively address them before attackers can exploit them. Assessments and audits may also uncover hidden security risks that have yet to be apparent through regular security monitoring.

2. Prioritize remediation efforts

Assessments and audits help organizations **prioritize remediation** by identifying the most critical security risks and vulnerabilities. They enable organizations to allocate resources effectively and focus on first addressing the most significant risks. With them, organizations can manage all security risks promptly and effectively.

3. Demonstrate compliance with regulatory requirements

Assessments and audits are also critical for demonstrating **compliance with regulatory requirements**. Many industries, including healthcare, financial services, and government, are subject to strict regulations requiring organizations to implement specific security controls and demonstrate that they meet regulatory requirements. Failure to comply with these regulations can result in significant fines and damage an organization's reputation.

3 key types of assessments

There are various **types of assessments** that organizations can perform to evaluate their security posture and identify potential vulnerabilities, but three of them are the most popular.

Vulnerability assessments

A **vulnerability assessment** aims to identify vulnerabilities and weaknesses in an organization's IT infrastructure, applications, and systems before attackers can exploit them. This assessment is typically performed using automated tools that scan the network for vulnerabilities and identify potential security risks.

Risk assessments

A **risk assessment** evaluates the potential impact of security risks on an organization's business operations. It considers the likelihood of a security incident occurring and the potential impact on the organization's assets, reputation, and finances. They can help organizations prioritize security efforts and allocate resources more effectively.

Penetration testing

Penetration testing, or "pen testing," involves simulating an attack on an organization's systems to identify potential vulnerabilities and weaknesses. This assessment is typically performed by a skilled, ethical hacker who attempts to exploit vulnerabilities in the organization's systems and applications. It can help organizations identify weaknesses that automated tools may not detect.

3 key types of audits

Organizations may be required to undergo various **types of audits**, depending on their business operations and the regulatory environment in which they operate. The following are three of the most common ones.

PCI DSS Audits

The Payment Card Industry Data Security Standard is a set of security standards designed to protect the confidentiality and integrity of payment card data. Organizations that process, transmit, or store payment card data must comply with it.

HIPAA Audits

The Health Insurance Portability and Accountability Act is a set of privacy and security regulations designed to protect the confidentiality of protected health information (PHI). Organizations that handle PHI, including healthcare providers, health plans, and business associates, must comply with it.

GDPR Audits

The General Data Protection Regulation is a set of privacy regulations designed to protect the privacy rights of individuals within the European Union (EU). Organizations that process the personal data of EU residents must comply with it.

Key takeaways

Assessments and audits are critical to maintaining a strong security posture in the IT industry. Organizations can help:

- Identify security risks and vulnerabilities.
- Prioritize remediation efforts.
- Demonstrate compliance with regulatory requirements.

The various assessments and audits available provide organizations with multiple tools to evaluate their security posture, from vulnerability assessments to penetration testing and compliance audits. The benefits of a strong security posture far outweighs the costs, making them a worthwhile investment for any organization operating in the IT industry.

Lesson2 : Developing metrics and KPIs

7 Key Steps to Develop Effective Performance Metrics

Performance metrics are valuable for monitoring, analysis, and collaboration. In turn, businesses can monitor operations, optimize processes, and finetune and execute strategy.

Astute businesses also see performance indicators as roadmaps for their employees. Effective performance measures guide focus and ensure employees are not working at cross purposes.

Many businesses, however, struggle to choose effective performance measures despite the numerous benefits.

Some challenges include wrong design, lack of top-level commitment, no linkage between metrics and processes or goals, only measuring what's easy, no accountability or authority, and a poor performance management culture.

In this article, we enumerate the steps you can adopt to develop effective metrics and avoid the challenges above.

We also discuss the importance of performance measures and the core principles for originating them.

Step 1: Create a key performance indicators (KPI) team

In his book, "Performance Dashboards: Measuring, Monitoring, and Managing Your Business, Second Edition," Wayne Eckerson explains that companies need to create a KPI team to choose effective performance metrics.

The team should consist of members with performance management process experience. Other skills needed in the group include:

- Group facilitation

- Measurement methodology
- Data pipeline and analysis, especially with context on the company's existing data architecture
- Organizational unit's processes knowledge

The tasks of this team are in six folds:

Gathering requirements

All performance measures must serve a purpose. The KPI team must identify the consequences of adopting a particular metric.

For example, what would happen if you tied a performance bonus to the number of accounts opened or tied a doctor's performance to the number of patients they saw?

The doctors may start offering subpar care to patients to see more patients in a day.

That's where gathering requirements come in. The process helps forestall adopting metrics with dire consequences. Gathering requirements involve:

- Asking what the short and long-term strategic objectives are. This stage includes interviewing all key stakeholders to understand the "why." What is each metric supposed to achieve? To plan, learn, predict, forecast?
- Learning which department, processes, or groups are affected by this metric?
- Knowing the best way to measure this metric
- Identifying the appropriate time frame

Prioritizing performance measures

The "gathering requirement" stage will likely throw up many meaningful measures.

However, the team will need to choose measures most likely to move the needle towards meeting your strategic objectives.

Validating performance measures

The KPI team also tracks these measures to ensure they're achieving the "why" identified in Step 1.

It may not necessarily be the performance measure but how it is evaluated. So, the team needs to review how it's measured and correct it accordingly.

If the metric is totally off base, it is more prudent to pivot to a new metric completely.

Standardizing metrics across the organization

Standardizing metrics ensures all departments track and report information uniformly. It means that there's a clear definition for each adopted measure by your organization.

Otherwise, many departments or employees may provide their definition of a metric and fly with it. It also helps when the KPI team creates a reference document for each adopted measure.

Setting realistic targets

The KPI team must set targets based on the business context. For example, say the industry benchmark for a metric is 50%.

It is not advisable to set the same benchmark if the department is starting from 0%.

The KPI team must consider previous performance, budget, department dependencies, and other factors.

You may also like: How to Set KPI Targets that Drive Business Growth

Getting buy-in from individuals

The KPI team must also ensure individuals whose performance will be evaluated buy into the measures. The individuals must know what they'll be judged on, why, and other details like timeframe.

Step 2: Start with your mission, goals, and objectives

Nicholas Fisher, in the article "Performance Measurement: Issues, Approaches, and Opportunities," published in the Harvard Data Science Review, opined that:

"It is clearly of interest to individuals, enterprises, and governments to have sensible (quantitative) targets and sound ways of assessing progress toward these targets."

Performance measures must always stem from your company's goals, targets, and objectives. That way, you can develop metrics that fit all your business dimensions, including finances, people, customers, internal processes, compliance, and innovation or growth.

Aligning performance measures to objectives will ensure everyone uses the same data points and metrics and is focused on the same strategy.

You can thus more easily assess if you're on track to achieving your goals.

These quantitative measures should then be translated into business unit goals and cascaded into individual actions.

Step 3: Choose your measures carefully

After the end of the review period, a marketing director did an attribution analysis and found that the company made $10 million from 100 conversions. The marketing department spent $5 million during the review period.

From the marketing director's perspective, the 100 conversions happened based on marketing activities carried out by their team. As such, the cost per conversion is $50,000 ($5 million/100).

But the real question is: Would some of this conversion have happened irrespective of what the marketing department did?

Most likely, yes! From word of mouth to non-marketing factors, certain drivers other than marketing can lead to a conversion.

This means the cost per conversion rate calculated above is misleading if marketing doesn't account for all the conversions.

Avoiding faulty conclusions

Rather than use attribution, it's more valuable and accurate to use incrementality.

Avinash Kaushik defines incrementality as "the conversions that would not have occurred without various marketing tactics." It's a better approach to measuring marketing impact than attribution.

On further prompting from the financial director, the marketing director returned to the drawing board. After painstaking effort, the marketing director found that marketing only contributed to 27 of the 100 conversions. Ouch!

This new revelation means that the cost per conversion jumped to $185,185 ($ 5 million/27). That is more than the $50,000 per conversion rate from the initial approach.

While the final measure does not put the marketing team in a shining light, it's more useful than a misleading metric.

The marketing team can review patterns and what worked to bring 27 conversions. By repeating what works, the team can eventually increase incremental conversions.

Additionally, using the incrementality approach clearly showed there was a large chunk of wasted marketing budget that could be better channeled.

Case study culled from The Marketing Analytics Intersect by Avinash Kaushik.

Lessons learned

The lessons from the above case study to adopt include:

- Developing metrics that paint the full picture
- You can only improve performance by adopting the best practices when using certain measures. The cost per conversion in the case study above is the same but with different outcomes. The incremental approach was more valuable.
- Tracking effective performance measures takes effort. Don't choose the easy metrics but those that can improve specific business processes. Don't prioritize Net Promoter Score over a more robust market research process into what makes your customers tick.
- Every performance measure you adopt has consequences and will lead to behavioral changes.

- Measure impact and value, not activity.

Step 4: Develop a measurement plan

Think of a measurement plan as your strategy for ensuring the accurate and timely tracking of your chosen metrics. It's a roadmap to determine the kind of data you need and the sources of those data points.

It can also involve detailing the kind of dashboards required and how employees need to produce certain reports.

Let's say one of the data points you need requires customer feedback. Your measurement plan must answer questions like:

What's the best approach? Do you need to create a survey? What's the ideal sample size? What's the best delivery method? Do we need to pay for software? If so, which is the best fit for our needs?

You may also like: How to Track Performance Metrics (Beginner's Guide)

Step 5: Create a quality and accurate data pipeline

Any insight or performance measure is only as good as the quality of the data that produced them. You can have the right metric, but poor data can truncate your progress and provide misleading results.

You cannot develop effective performance measures without quality and accurate data.

You must review your data architecture and systems, including third-party providers, for accuracy, recency, ownership, and reliability.

You must also collect business performance data that your team can use to derive the measures. Consequently, you may need to find new data sources.

You may also like: 5 Tips for Holistic Performance Data Integration (Explained!)

Step 6: Assign ownership and authority

The next step is to delegate the responsibility of delivering the target to a primary entity. They would be held accountable for both success and failure.

They are the go-to person when you need information on the progress (or lack of it) of the measurable components of a set goal.

It's one thing to be responsible for something, but another reality entirely when you're empowered to do that thing. Suffice it to say that many organizations get it wrong in not delegating authority appropriately.

If the entity in charge of a performance measure needs certain resources, would they be able to get it without delay?

Delegating both responsibility and authority is especially essential when the actualization of reaching performance measure targets depends on multiple individuals and business units.

Step 7: Review and refresh

This step helps you track progress to ensure all measures are still relevant to your business goals and objectives. Note that this is not the step to evaluate if you're meeting your targets. Your focus is on their relevance and implementation.

You may pivot your business offerings and thus render certain metrics useless or less important than before.

In other instances, you may need to add some measures because of compliance and external factors.

Ultimately, the goal is to review and evaluate the efficacy of each measure and if you should continue with them.

Principles for developing effective metrics

Two key principles for developing effective metrics are:

Stakeholder analysis

Stakeholder analysis is a simple concept of identifying all entities with a vested interest in a project and what "quality" means to them.

While there are other key stakeholders like shareholders, the board of directors, and employees, your number one stakeholder should always be the customer.

The Tribus Paradigm

The Tribus Paradigm captures four critical elements:

- Your customers must always be the starting point of picking performance measures.
- The concept of "quality" must be understood from the customer's perspective, and subsequent measurement of outcomes for the customer must be based on this definition.
- That good quality is predicated on process improvement. For example, you can only reduce your cost per conversion by improving the process of identifying your target audience and designing quality marketing campaigns.
- Identifying leading indicators and predictors of the outcome you identified above.

Why are performance metrics important?

Performance measures serve three core purposes, according to Nicholas Fisher:

A concise overview of the health of the enterprise

Performance measures taken together should provide a snapshot of your organization's health. There are little to no surprises that can derail your operations.

From the board room to individuals, everyone in the organization must be able to answer these three questions confidently:

- "Where are we now?" - Present performance
- "Where are we heading?" - Business targets and objectives
- "Where do we need to focus our attention?" - Strategic analysis

Effective performance measures help you gain context at the full system level, not just locally. Metrics linked to the entire system can provide a bigger-picture view and lead to optimal decisions.

Decision makers can then leverage this health-check information to make timely and data-driven effective decisions like allocation of resources and hiring and firing choices.

A quantitative basis for selecting continuous improvement priorities

In the mid-1980s, AT&T ran a monthly customer satisfaction survey, similar to Net Promoter Score, that always returned at least 95% satisfaction.

Surprisingly, though, the company lost 6% market share during the same period despite the high satisfaction reported by its customers. The value of the lost market share was $3.6 billion.

The question is: Why did AT&T lose market share if their customers were satisfied with their products?

The answer to that question is that it turned out that the satisfaction score did not take a system's view and did not provide areas for continuous improvement priorities.

Customers may have been satisfied with the product, but the survey failed to capture areas where the team could do better or get what customers wanted.

Perhaps support service was poor, or customers wanted more on their package. And as soon as another company filled this void, the customers jumped ship.

Effective performance measures dig deeper and help unearth growth opportunities, as shown in our attribution and incremental case study above.

Alignment of the efforts of the people with the mission of the enterprise

We've extensively emphasized the importance of aligning performance measures to your business goals and objectives. That's because 100% alignment ensures everyone is focused on the same strategy.

Alignment also fosters collaboration between managers and staff and better coordination among departments.

Other than serving as a tool for strategic alignment, performance measures are also a tool for communicating strategy.

When you adopt clear, simple, and specific measures, your employees know what direction the company is going.

You may also like: 5 Tips for Aligning Performance Metrics with Strategic Objectives

Takeaway: The power of business survival lies in the quality of performance measures

Performance measures are critical to a business's survival odds. Many companies went bankrupt due to poor monitoring and not knowing what was going on.

By adopting the seven steps above, you can avoid major consequences like bankruptcy and minor ones like poor customer satisfaction.

Overall, developing systems and bigger-picture metrics will provide you with insights into your business health status, identify improvement areas, and align the efforts of your staff with your organization's objectives.

Do you want to seamlessly track, cascade, and monitor performance measures in your company? Start an interactive demo and see how Kippy can help.

Lesson3 : Developing and building action plan

1.3 Developing an action plan

Developing an action plan means turning ideas raised during strategic planning or evaluation into reality. It means identifying the steps that need to be taken to achieve the resource center's aims. The resource center officer and their manager or supervisor should develop the action plan, in consultation with members of the resource center advisory committee and/or other users.

It is useful to have action plans for each area of the resource center's work, such as:

- fundraising
- selecting and ordering materials
- organizing materials
- computerization
- providing information services
- promoting the resource center
- networking and cooperation.

How to develop an action plan

An action plan consists of seven steps: setting objectives, assessing the objectives, identifying action required to meet the objectives, working out how to evaluate the activity, agreeing a time-frame for action, identifying resources (human, financial and technical), finalizing the plan, and evaluating the results.

1. Set objectives

You need to identify clear objectives that will guide your work to achieve the resource center's aims. Objectives need to be achievable - do not be over-ambitious. They need to be measurable (for example, a certain number of activities carried out within a certain period), so that you can know whether you have achieved them.

Ask yourself:

- What do we want to achieve?
- *Example of an aim:* To disseminate information that will improve local health workers' knowledge of local health problems.
- *Example of an objective:* To produce and distribute an information pack on malaria diagnosis and management to all health clinics in the district within the next three months.

2. Assess the objectives

Assessment helps to determine whether or not the objective is appropriate. It may result in confirming the objective, abandoning it or revising it. Ask yourself:

- Is the objective compatible with the resource center's aims and objectives?
- Are the necessary resources (funds, equipment, staff) available to reach this objective? If not, are they obtainable?
- What problems might arise in working to achieve this objective?
- *Example of resources needed to carry out the objective:* staff time, relevant materials in the resource center or obtainable from elsewhere, stationery, photocopier, postage.
- *Example of revised objective:* To produce and distribute an information pack on malaria diagnosis and management to 20 health clinics and training institutions within the next six months.

3. Identify action required to achieve the objective

A series of tasks needs to be identified for the objectives to be achieved. List these as steps.

Ask yourself:

- What tasks are necessary, in what order, to meet the objective
- *Example:*

1. Plan the content of the information pack and decide how to distribute the packs, in consultation with other staff and users.

2. Calculate costs and staff time, and make sure that funds and time are available.
3. Allocate responsibilities.
4. Gather information for the pack (search resource center, contact other organizations).
5. Request permission from publishers to photocopy material.
6. Photocopy material and prepare packs.
7. Distribute packs.

4. Work out how to evaluate the activity

Plans for finding out how far the activity has achieved its objectives need to be built into the action plan. Ask yourself:

- How will we know whether we have achieved our objectives
- *Example:*
    - Contact five clinics to see whether they have received the packs.
    - Include an evaluation form in the pack, asking health workers whether the information has improved their knowledge, how they have used the information, and how future packs could be improved. Assess the feedback from the forms.

Then incorporate plans for evaluation into your action plan.

- *Example* (showing plans for evaluation in *bold italics*):

1. Plan the content of the information pack, *including evaluation forms*, and decide how to distribute the packs, in consultation with other staff and users.
2. Calculate costs and staff time, and make sure that funds and time are available.
3. Allocate responsibilities.
4. Gather information for the pack (search resource center, contact other organizations).
5. Request permission from publishers to photocopy material.
6. *Prepare evaluation forms.*
7. Photocopy material, prepare packs.
8. Distribute packs.
9. *Contact clinics to see if they have received packs.*
10. *Revise plans for distributing packs if they have not reached some clinics.*
11. *Assess the feedback from the evaluation forms and use it to plan future work.*

5. Agree a time frame

As you identify each task, work out how long it will take and when it needs to be done. This will help you to see whether your action plan is on schedule or whether you need to modify the schedule.
Ask yourself:

- What is the actual time required for each individual task? (Be careful not to under-estimate)
- When will each step be completed?
  Example: Total of 18 days over a three-month period

6. Assess the action plan

Ask yourself:

- How will you know whether the individual tasks have been achieved?
- Have you allowed for possible interruptions?
- Have you tried to do too much or too little?

An action plan must be realistic if it is to work. It is easy to over-estimate what you can do, leading to disappointment and failure. *For example*:

1. Leaflets that you had planned to include in the pack may have run out and need to be reprinted. Can you substitute something else, or will you need to arrange for them to be reprinted before you can finish preparing the packs?
2. The member of staff preparing the pack will take annual leave for six weeks during the period in which the pack was planned to be prepared. Can you re-schedule the work, or can someone else, do it?

7. Finalize the action plan

Revise the action plan. Obtain feedback and comments from colleagues, and revise it again if necessary.