



EUROPEAN CENTRAL BANK

EUROSYSTEM

Fundamentals of cybersecurity and the Cyber Resilience Oversight Expectations (CROE)

CEMLA

***Emran Islam &
Constantinos
Christoforides***

November 2019, Mexico

Agenda

1	Context, main definitions and the CROE
2	Governance and Continuous Evolution
3	Identification & Situational Awareness
4	Protection
5	Detection
6	Response and Recovery
7	Annexes

Main definitions of cyber...

➤ **Cyber**

“Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems”

Source: FSB Cyber Lexicon (adapted from CPMI-IOSCO Cyber Guidance)

➤ **Cyber security**

“Preservation of confidentiality, integrity and availability of information and/or information systems through the **cyber medium**. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved ”

Source: FSB Cyber Lexicon (adapted from ISO/IEC 27032:2012)

➤ **Cyber resilience**

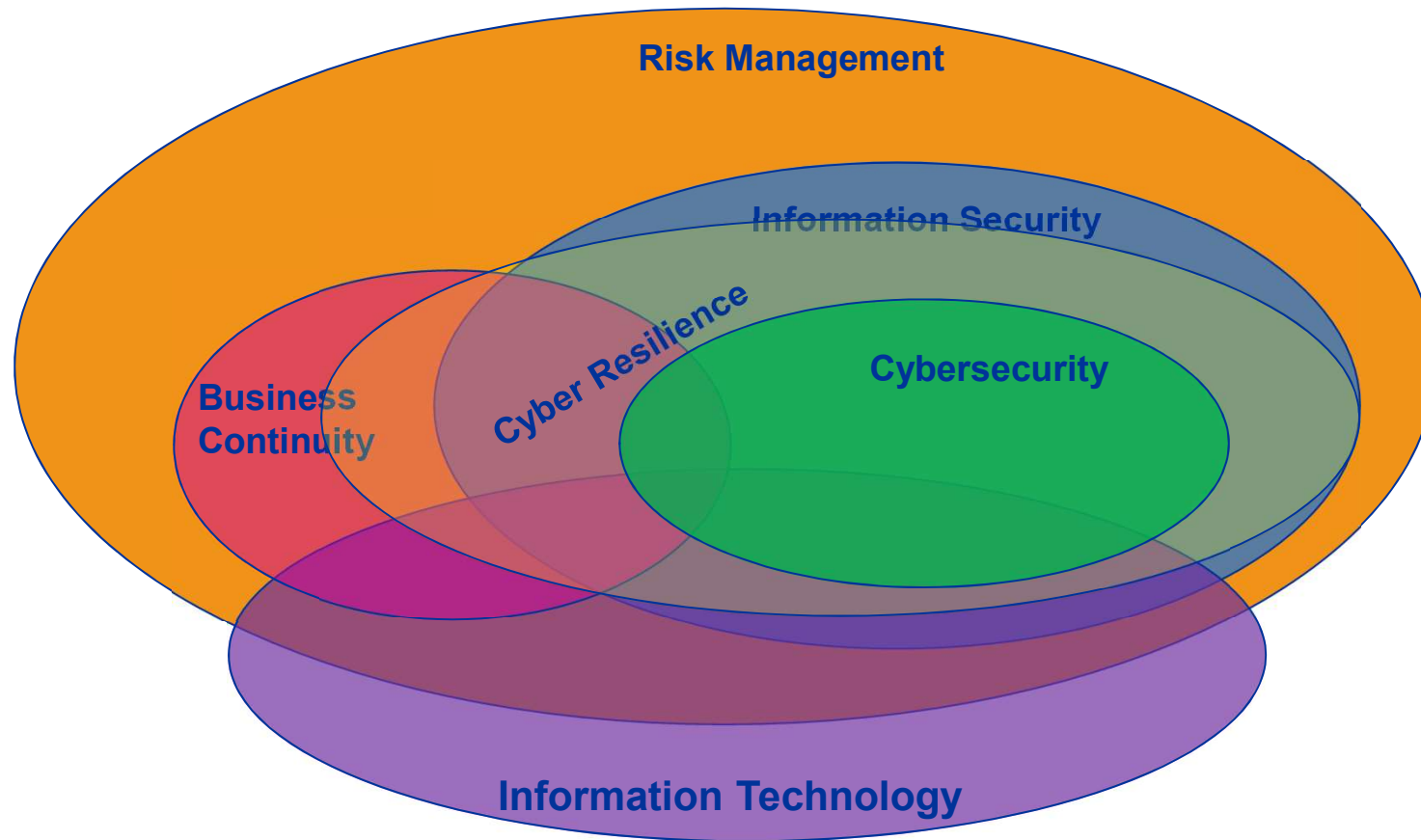
“The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents”

Source: FSB Cyber Lexicon (adapted from CPMI-IOSCO, NIST, and CERT glossary)

Strategic relevance of cyber threats

- **Characteristics of cyber threats**
 - Quickly **increasing** in **number**, **typology**, **persistence** and **complexity**
 - Can make **existent controls** and **business continuity measures** **ineffective**
 - Often occurring **immediately** after the **discovery** of a **vulnerability**
- **Characteristics and motivations of the attackers**
 - **Well organized** threat actors across **different countries**
 - Able to set **sophisticated attacks** difficult to detect
 - Disrupting organisations – loss of trust, credibility, business
 - Stealing funds
 - Obtaining sensitive information
- **Macro-vulnerabilities of the financial sector**
 - **Technological dependencies**
 - **Interconnections** and **mutual dependencies** → risk of quick distribution of threats from one entity to another
 - **Growing dependency** on TSP (Technical Service Providers)

A dynamic context where the scope of each activity continuously changes...



Do not stick to the definitions, but look at the purpose and at the rationale behind the security measures!

CPMI-IOSCO Guidance on Cyber Resilience for FMI

The Guidance is structured in chapters defining five main risk management categories and three general components that should be considered when talking about cyber resilience applied to FMI.

- Risk management categories are:
 - i. Governance
 - ii. Identification
 - iii. Protection
 - iv. Detection
 - v. Recovery
- General components are:
 - i. Test
 - ii. Situational awareness
 - iii. Learning and Evolution



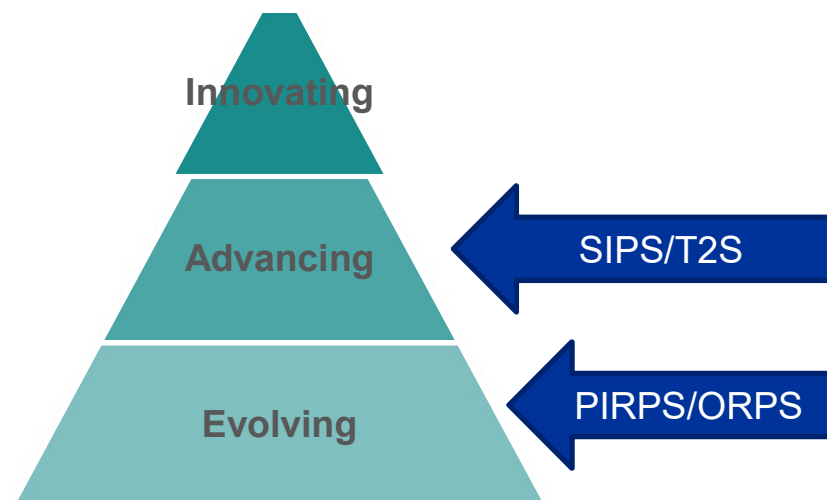
Cyber Resilience Oversight Expectations – December 2018

CROE – why?

- Sets up a more detailed elaboration of the CPMI-IOSCO Cyber Guidance to aid FMIs and overseers in implementing the Guidance and assessing the FMI's compliance against it
- Provides good practices which can be referred to when giving feedback to FMIs regarding assessments in the future
- Takes into consideration the industry best practices, already set out in different frameworks – e.g. *FFIEC Cybersecurity Assessment Tool*, *the NIST Cybersecurity Framework*, *ISF Standard of Good Practice*, *CobiT* and *ISO/IEC 27001*
- Provides the basis for overseers to work with FMIs over longer term to raise the FMI's maturity level
- Can be used as:
 - Assessment Methodology for overseers; and
 - Tool for self-assessments for FMIs.

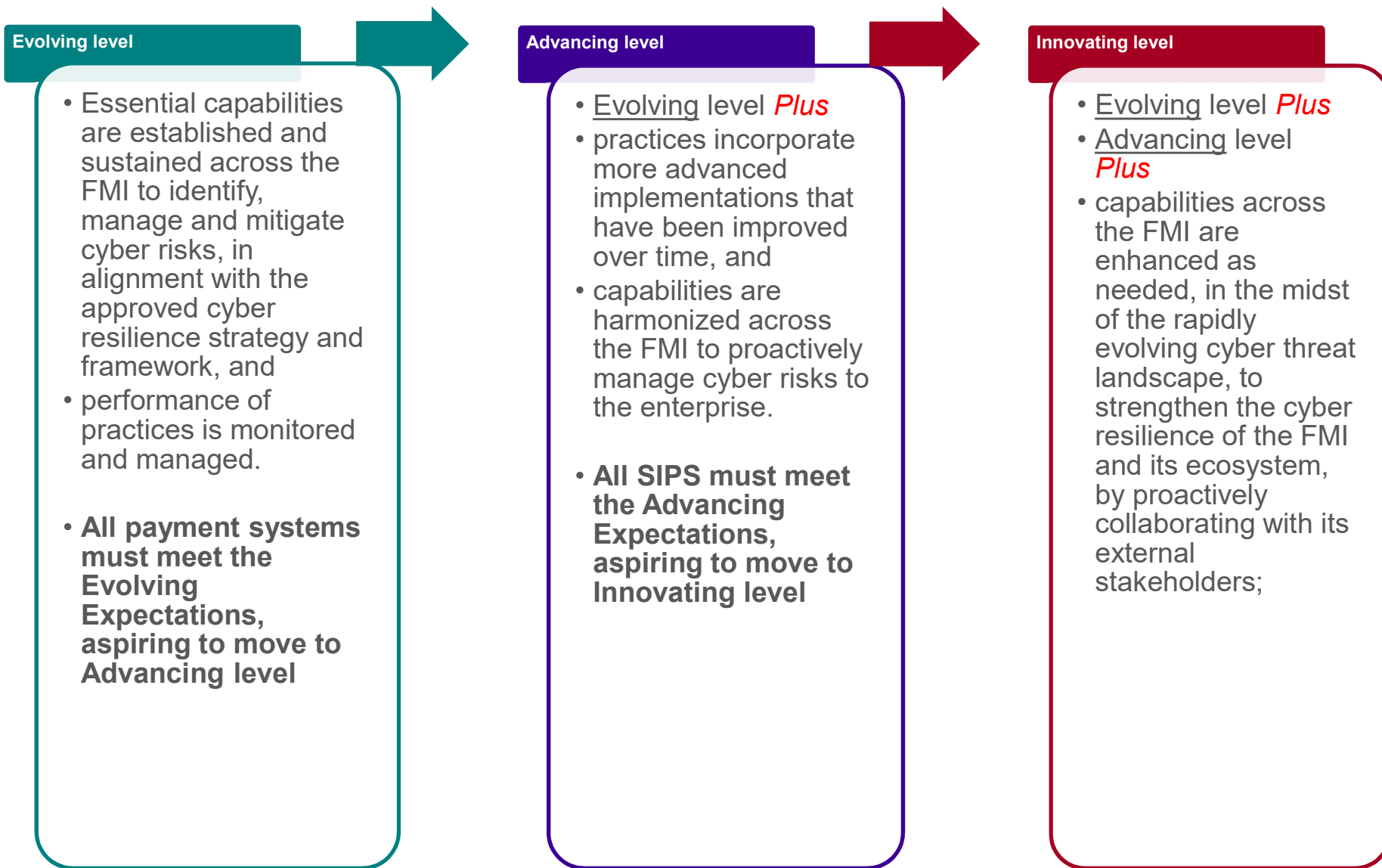
Levels of expectations: the three-level approach

- Based on the *three level* approach;
- Each chapter is divided into the three levels of expectations;



- Applied in order to *adapt* to a changing cyber environment;
- FMIs are expected to *continuously evolve* on the cyber maturity scale;
- Provide an *insight* about the FMI's level of cyber resilience and what it needs to improve in terms of cyber expectations;
- Takes into account the *proportionality* principle (specific minimum requirements for SIPS/T2S, PIRPS, ORPS).

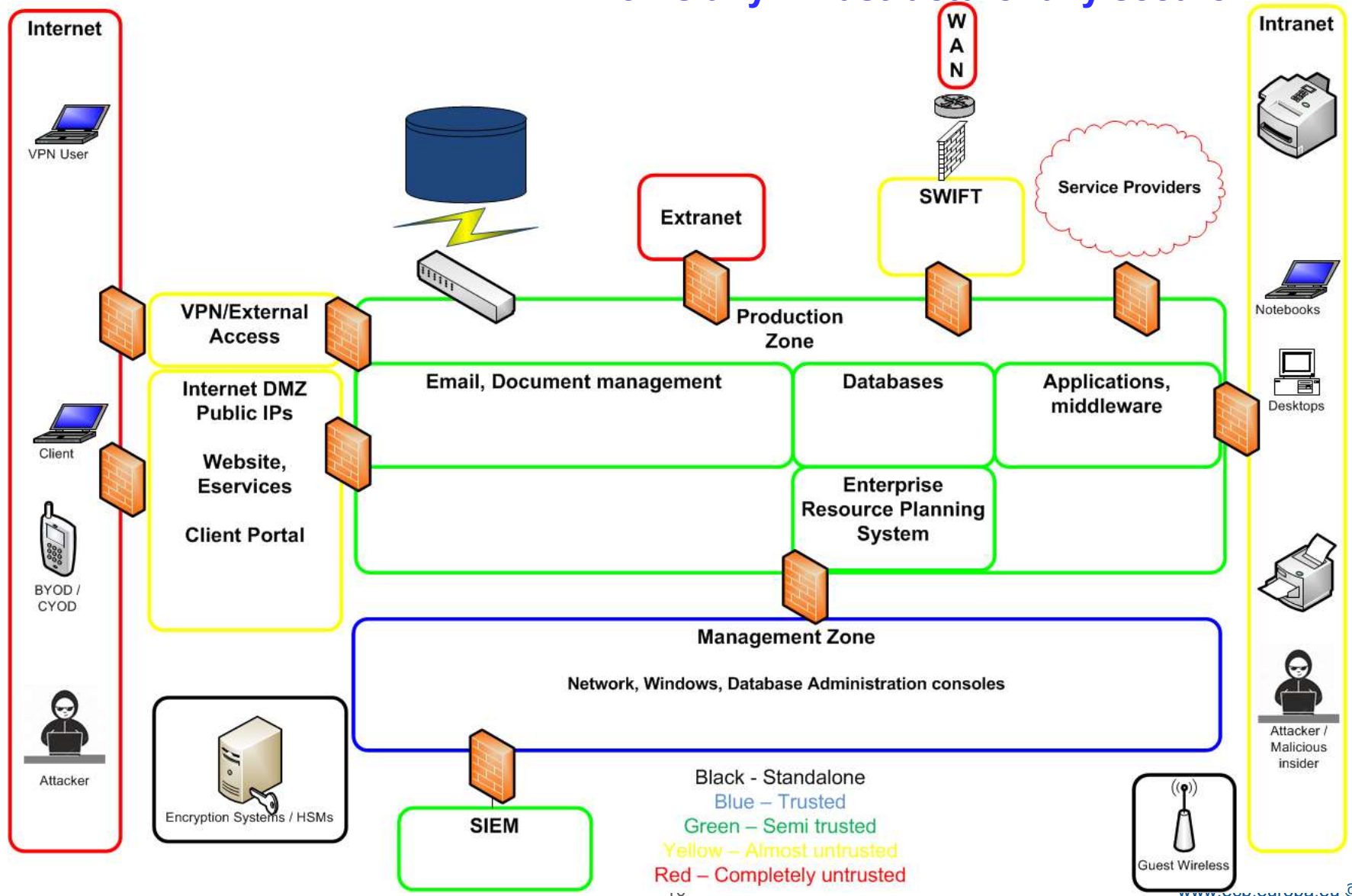
Levels of expectations: the three-level approach



Context: design of an FMI

FMI IT Infrastructure

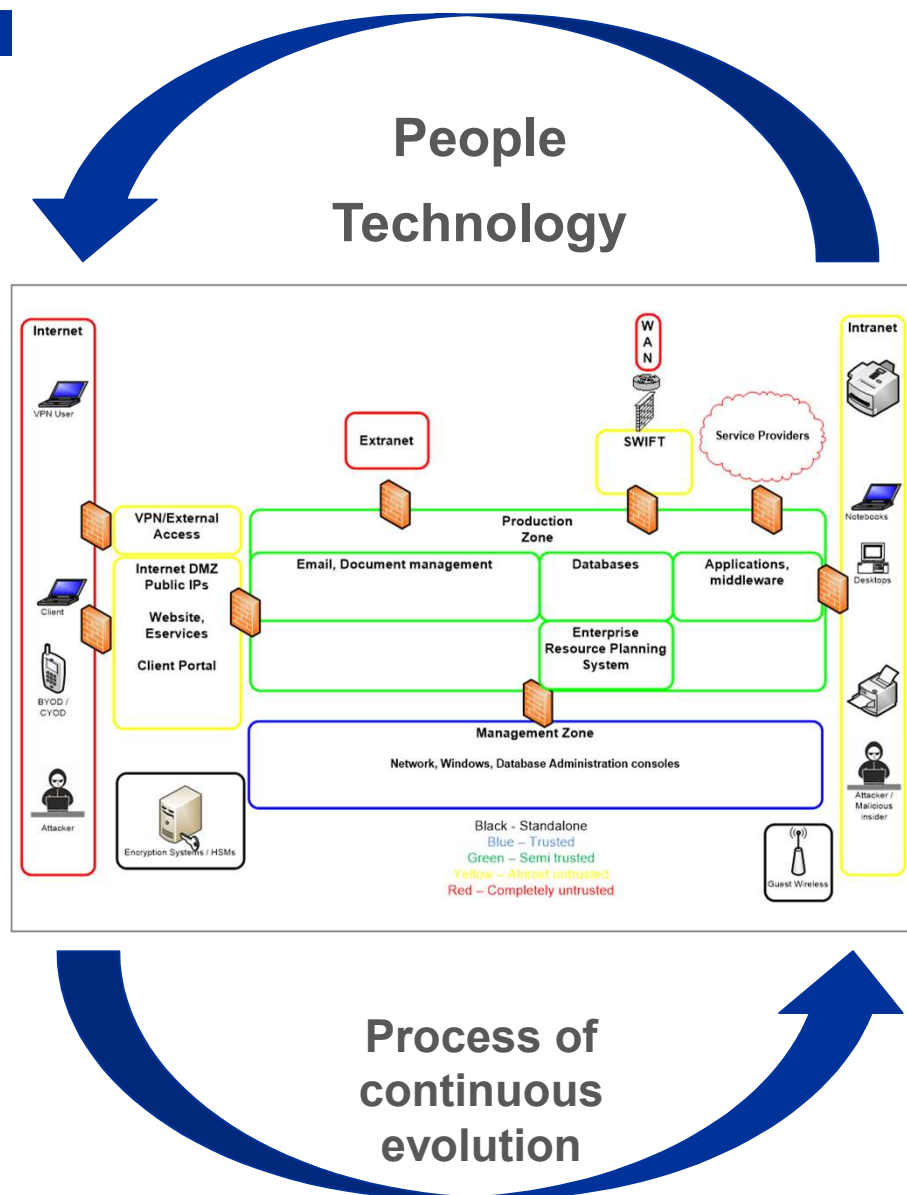
No technology is full-proof
nor is any infrastructure fully secure



Cyber Resilience in FMI

The CROE covers the following topics and how to use these domains to make the FMI resilient:

- i. Governance
- ii. Identification and Situational Awareness
- iii. Protection
- iv. Detection
- v. Response and Recovery
- vi. Testing



Agenda

1	Context, main definitions and the CROE
2	Governance and Continuous Evolution
3	Identification and Situational Awareness
4	Protection
5	Detection
6	Response and Recovery
7	Annexes

Information security / cyber resilience framework

Purpose

- The framework is developed to **describe how** the **objectives** and **targets** of the strategy shall be achieved systematically and how it will **continuously evolve**

What does it look like?

- Could be a myriad of **documents** depending on the size and scope of the FMI
- Includes policies, procedures, processes, workflows, forms etc.

Information security / cyber resilience framework

The framework should **cover** the key areas of:


- **Roles and Responsibilities** for Information Security/ Cyber Resilience
- **Identification** including asset classification and risk assessment
- **Protection** of information assets such as antimalware, encryption, segregation of duties, Privileged Identity management, Network Security, Change and patch management
- **Physical** Security controls
- **HR** security
- **3rd party security** management
- **Detection**, Logging and monitoring
- **Response** to a security incident, forensics and information sharing
- **Recovery** and Business continuity
- **Situational awareness** (Threat Intelligence)
- **Continuous evolution and metrics**
- **Information Risk Assessment**

Agenda

1	Context, main definitions and the CROE
2	Governance and Continuous Evolution
3	Identification and Situational Awareness
4	Protection
5	Detection
6	Response and Recovery
7	Annexes

What does the FMI know about its IT infrastructure?

The Information Security/ Cyber Security in a nutshell:

- 
1. In order to **protect** information assets you need to know what you have and where it is, catalogue it and keep it up to date.
 2. Then determine the **sensitivity / criticality** of these information assets both for existing IT systems and new ones.
 3. Then understand the **risks** to these assets based on the **threats** and **vulnerabilities**.
 4. **Implement** controls to mitigate risks (or perform other risk mitigation actions).
 5. **Re-evaluate** the risks after risk mitigation.

Conversely Step 1 is critical as you cannot safeguard what you do not know you have!

Information Asset Management in an FMI

Manual

- Done via excel or other form of register ☹️
- Must include details and serials to match
- Process required to update – resource intensive
- Maybe out of date/often inaccurate

Automated

- Done via the network discovery or via software (e.g. CMDB)
- Up to date, runs regularly
- Could have limited visibility with stand alone / isolated machines
- May lack details on underlying information to give a full picture
- Need to be augmented and managed also – no silver bullet

Hybrid

- Mix of manual and automated – usually the case in FMIs.

Risk Assessment

- A methodology for Information Risk Assessment (**IRM**), based on best practices must be adopted by the FMI in order to measure risks to the information assets.
- A systematic and periodic risk assessment process is **key** to identify the risks to the information assets by measuring the **business impact** in case **cyber threats materialise** in combination with the **threats and vulnerabilities** that exist.
- The risk assessment is undertaken in a **methodical** manner capable of producing **comparable** and **reproducible** results:
 - Identification of **mission critical** processes;
 - Identification of **associated information systems / asset**;
 - **Business impact analysis** for system / asset;
 - **Threats and vulnerabilities** analysis for each **system / asset**;
 - **Estimation of risk**;
 - **Risk mitigation measures** and **acceptance of residual risk**;

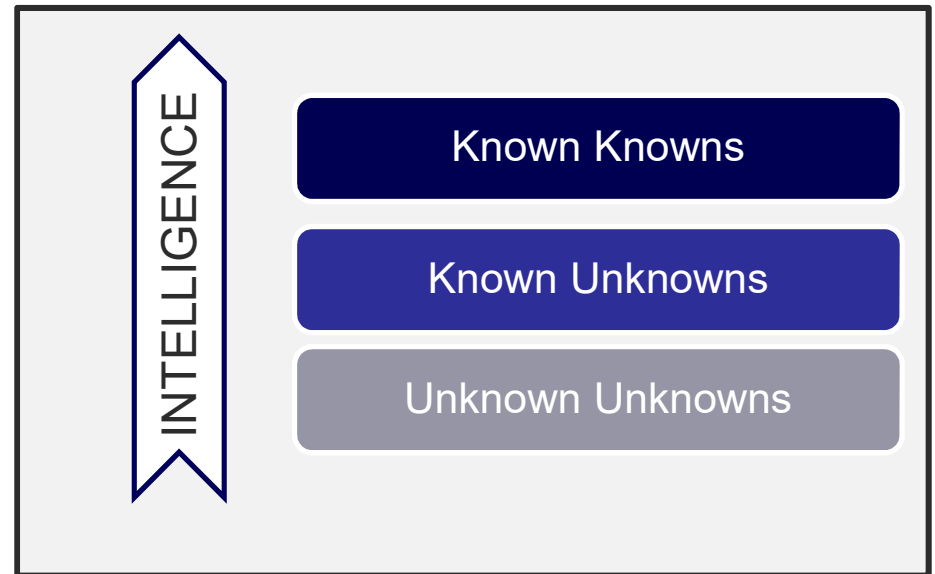
The importance of Threat Intelligence

- **Definition:**

Threat = Motivation of adversary combined with Capability of adversary

+

Intelligence = Any piece of information that can inform the decision making



- **The rationale:**

- *Know* your *enemy*
- Go *beyond the perimeter* of the organisation
- Go from *reactive* to *proactive* measures
- Allows FMIs to *prioritise* their *actions*

Threat Intelligence



- Usually a mix of **Commercial** and **Open source** Intelligence feeds.
- Use of **Indicators of Compromise (IoC)** and **Tactics, Techniques and Procedures (TTP)** to enhance the detection, e.g. SIEM solution, by being able to know how the FMI's adversaries attack.
- Use the adversaries TTPs to **plan** and **implement** better and more effective preventive controls.
- TI is **continuous** => threat levels, actors, techniques change.
- **Plugs in** with all **other Information Security / Cyber capabilities**, such as security testing providing value and guidance to perform more targeted testing such as **Red teaming**.

Information Sharing

- Share information regarding cyberattacks including **attackers' modus operandi, indicators of compromise, and threats and vulnerabilities**
- Levels of information sharing:
 - **Strategic** – Sharing information that helps organisations understand the type of threat they are defending against; the motivation and capability of the threat actor; and the potential impacts thereof
 - **Tactical** – Sharing information from direct adversary action inside your systems or from other sources that have the potential to immediately influence your tactical decisions
 - **Operational** – Sharing with participants network/technology service provider during an attack and vice versa
- FMI should share **timely information** (as an emergency process) to participants during and following a cyber attack to aid in the response, resumption and recovery of its own ecosystem.
- How is information shared? What are the **communication channels**?

Agenda

1	Context, main definitions and the CROE
2	Governance and Continuous Evolution
3	Identification and Situational Awareness
4	Protection
5	Detection
6	Response and Recovery
7	Annexes

Controls

Uniform control implementation and design offer:

- **Harmonised** approach to security controls
- Expandable and **scalable** controls
- Say the «**what**» and «**how**»
- Form the basis to create **security requirements** for new systems or changes to systems.
- Used to **benchmark controls** and enhance the overall posture
- Ensure security controls **comply** with any regulation or legal requirements

ISO 27001 and ISO 27002, NIST Framework, COBIT, ISF Standard of Good Practice for Information Security.....CSC Top 20, PCI-DSS, Australian Directorate Top 8

Identity lifecycle and management

- It refers to the creation, management, review and deletion of accounts
- Fundamental to manage identification, authentication, authorization and accountability

User Group → User	HR Dept → A. Waters
User → Roles	A. Waters → Recruitment_op, Payroll
Role → Permissions	Recruitment_op → Read, Write open vacancies → Create new vacancy

Permission (or privilege) → Operation (or action) on an object.

- Each user (human or technical) should exist as an identity in a system (individual-not shared) e.g. Document Management System, in the database or in any other repository has their own **access rights** which should be reviewed on a timely manner.
- In mature organizations identities are orchestrated by an **IAM (Identity and Access Management)** system or at the very least augmented via reporting tools.
- If no IAM system has been implemented there are separate islands of identities across systems with their own authorisation rules. This means systems are **handled independently. Resource intensive** and it almost always hails the **existence of security gaps.**

Information Repositories

- **Enterprise Content/Document Management System** –Contains documents which may include confidential information
- **Shared** folders, files and drives (contain reports)
- **Databases** (contain transactions/payments)
- **Cloud** platforms (share information with third parties)
- **Email** – an overlooked crucial information repository
- **End user repositories stored on clients** (workstations/ mobile devices)

Privileged Identity Management (PIM)

Everything in an FMI IT infrastructure from network equipment, clients, servers, operating systems, physical access systems, CCTV, telephony systems.... **have privileged accounts** (e.g. administrators), different from standard user accounts. Also technical accounts are used for intercommunication between systems (e.g. backups, updates):

- These accounts are the most sought after by attackers as they allow them to get access to **more systems** and/or to **escalate** their privileges.
- Some of these accounts possibly can access many machines e.g. IT Helpdesk, **Domain Controller Administrator**.
- PIM solutions are frequently used to **automate** these processes (ensure contingency arrangement), but have limitations and their setup is crucial for them to operate in a secure manner.
- If no automated solution exists, setting strong passwords frequently, assigning, revoking these accounts can be very labour intensive and is usually **troublesome**.

Attackers want to reach privileged accounts!

Identity attacks

- Social engineering (**Vishing, Phishing**) and keyloggers
- **Credential stuffing** – testing credentials from breaches linked to employees or clients in the FMI environment. Users may use the same passwords in their personal and professional lives.
- **Hash dump from system** – Once a system has been compromised like a user workstation the user can “dump” credentials. Note credentials of many users maybe found on even a client!
- **Sniffing credentials on network/ Man In the Middle** – once in the FMI infrastructure an attacker could impersonate another machine to obtain valid credentials or sniff them from any insecure/vulnerable protocols
- Taking advantage of **default username/passwords**.

Compromising identities is an essential part of a cyberattack

Identity attacks countermeasures

- **System Hardening** - System Configuration to make hacking systems more difficult and make the dumping of credentials less useful, more difficult to crack
- Proper **network security** to prevent attackers moving laterally
- Separation of **duties** of both users and systems to make credentials and systems captured by attackers less useful
- Privileged Identity Management solutions to **protect privileged accounts** as much as possible
- **Logging and Monitoring** of user logons, logoff, actions and correlations with other events.
- **Multi Factor Authentication** on critical systems/data/privileged accounts
- **Security Awareness** for all users.

Information classification

- Primary process to **protect** data to guarantee confidentiality, integrity, and availability whether it is at rest or in motion.
- Criteria for classification: **sensitivity**, **lifetime**, disclosure damage, modification damage, ...
- Useful to prioritize the risk and to define the access rules, authorization levels, and security controls
- **Main aspects :**
 - Identification of the **owner** and of the main **roles and responsibilities**
 - **Labeling** resources → classifying and declassifying
 - **Documenting** the classification
 - **Definition** of **security requirements** for both data at rest, in use, and in transit
 - **Implementation** of **controls** and security **measures** (e.g. encryption, watermark, Data Loss Prevention systems, back up) for both data at rest and in transit
 - **Training** of the users
 - **Data retention** and **disposal**

Information classification

Common technologies and controls to aid:

- **Data Loss Prevention System (DLP)** - System that monitors and protects data in use, data in transit and data at rest, with the aim to identify and prevent any unauthorised use and transmission of sensitive information (data exfiltration).
- **Digital Rights Management** – Originally was meant to protect copyrighted material but is now used to technically enforce data classification but in a different manner than above. E.g. you can send a DRM protected file via email externally but it will be encrypted and made unreadable.
- **Watermark** - cryptographic technique able to embed the sensitivity classification in a document, in a way that can be detected by DLP, too. Usually a watermark is not perceivable, and can be placed in a digital file (digital watermark).
- **USB/Removable media control** – disabling the use of USB, CD/DVDs and other ports with very specific exceptions.
- **Application Control** – allowing only the use of specific software throughout the infrastructure (deters many malware).
- **Browsing and Email control** – Restricting where users can go on the Web and who they can receive emails from or send to.

Data – at rest and in transit

- **Data at Rest**

- *How encryption is applied to:*

- *Documents*
 - *Databases*
 - *Email messages*
 - *Backups*
 - *Workstation/ mobile devices*
 - *User credential storage*
 - *Storage/USB*

- **Data in transit**

- *How encryption is applied to:*

- *Email messages*
 - *Remote access sessions*
 - *Helpdesk/ Administrative remote management*
 - *Web services internal and external*
 - *Wireless network*
 - *Web and wired network*



Implementation / Key / Certificate management is crucial! Who is responsible and how are they protected?

HR resources security policies

- Humans are often the weakest link in a security chain.
- HR security should be embedded in **every stage** of the **employment life cycle**:
- **Before hiring new staff:**
 - Carry out **security (white record) check**, **credit** and **reference check** with different levels of depth depending on the specific tasks and responsibilities
 - Clearly state **job responsibilities**
 - **Grant** the necessary **access rights**, based on the principles of **need to know**, **least privilege**, and **segregation of duties**
- **During employment:**
 - Apply **job rotation** and **mandatory vacations**
 - **Periodically review access rights** and change them in a timely manner if needed (preferably in automated way)
 - Require participation in **security awareness and training sessions**
 - **Redo pre-employment checks**

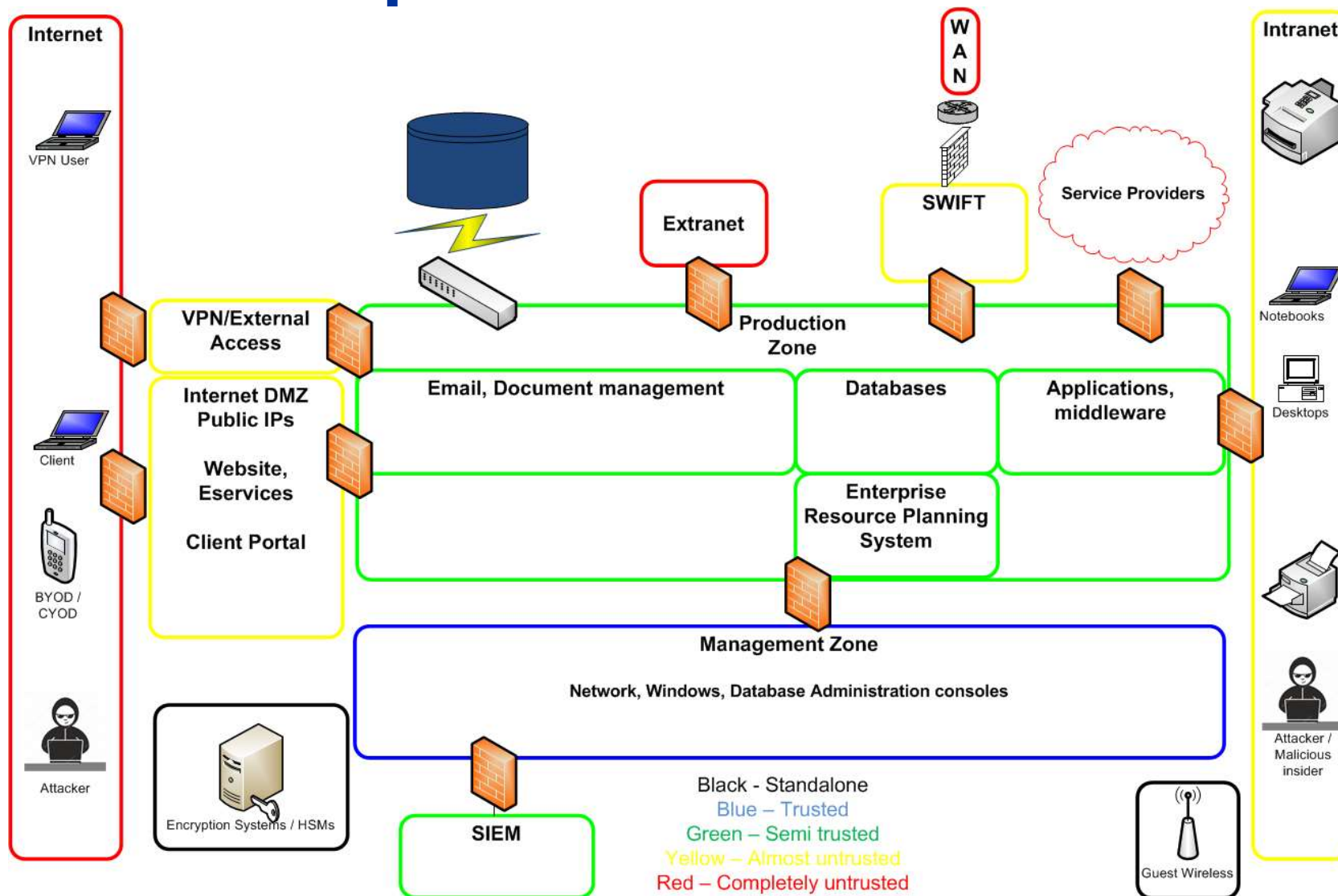
HR resources security policies

- **At the termination of the employment contract:**
 - **Revoke** in a timely manner accounts and access rights
 - **Ensure** return of information assets devices
 - Put in place **specific security procedures** in case of forced termination by the FMI, in order to minimize any risk

Overall Culture

- **Promote** a security culture within the FMI: employees should understand they play a relevant role in guaranteeing security, and that they could be also the weakest point. The Board should promote the security culture in the organisation.
- **Establish** a security awareness programme: the FMI should introduce mandatory training and awareness sessions for all employees or for specific user groups, based on their specific task and responsibilities. Exercises (e.g. phishing tests) or ad hoc workshops should also be also organised.

Practical example on the FMI IT architecture



Databases in an FMI

- Operationally very **significant**
- Contain **transactions, payments, customers information**, etc.
- **Multiple technologies** may be used for various databases.
- Should **not** be **accessed directly** – only via application.....
- **Sensitive data** usually encrypted
- Apart from security, database structure **optimisation, capacity** and **performance** are **critical** for an FMI to operate its database without problems

Database Security (DB) in an FMI

- **Encryption**

- Sensitive data is **encrypted** either in **columns or tables**
- Alternatively the **whole database** may be encrypted
- Even DB Administrators cannot “see” this data
- **Encryption key** is stored in another location-wallet but is accessible under circumstances. → An attacker who hacks the DB may not see the data, but if an account of a privileged application user is hacked the attackers would obtain access.

- **DB Firewall**

- The DB Firewall controls **who can access** the DB and how as well as **detects attacks** from queries and stopping them
- Without a DB Firewall a user could in theory access the DB and perform queries.
- It is not uncommon to have users that access the DB directly and they must be controlled and monitored
- All user actions are **logged** and sent to a centralised solution for correlation

Web application servers in an FMI

- Web application and application servers are needed to **provide a way** in which **users interact** with the structured data (=database).
- Could be that an application has both a **separate web application and application server** but it is also likely that only an application server is needed.
- Applications if vulnerable could be **compromised** to infect users and to capture credentials from them.

Web application security: web application firewall (WAF), proper configuration, securely coded web application (testing!)



It is possible to attack and get information from the database via the application/web application. Whatever is input in the application is then conveyed to execution in the database

Network Security

- **Attacks from external network**
 - Direct attacks via the **Internet**
 - Attacks against **external facing web services** e.g. payment gateway, customer portal etc.
- **Attacks between internal machines**
 - **Forbidden or suspicious communication** between machines especially between network segments (Pivoting-lateral movement of active attackers)
 - **Hacked machines**
 - **Unauthorised (remote) administrative activity**

Moving within the network is an essential part of a cyberattack

Remember! It is important to have in place:

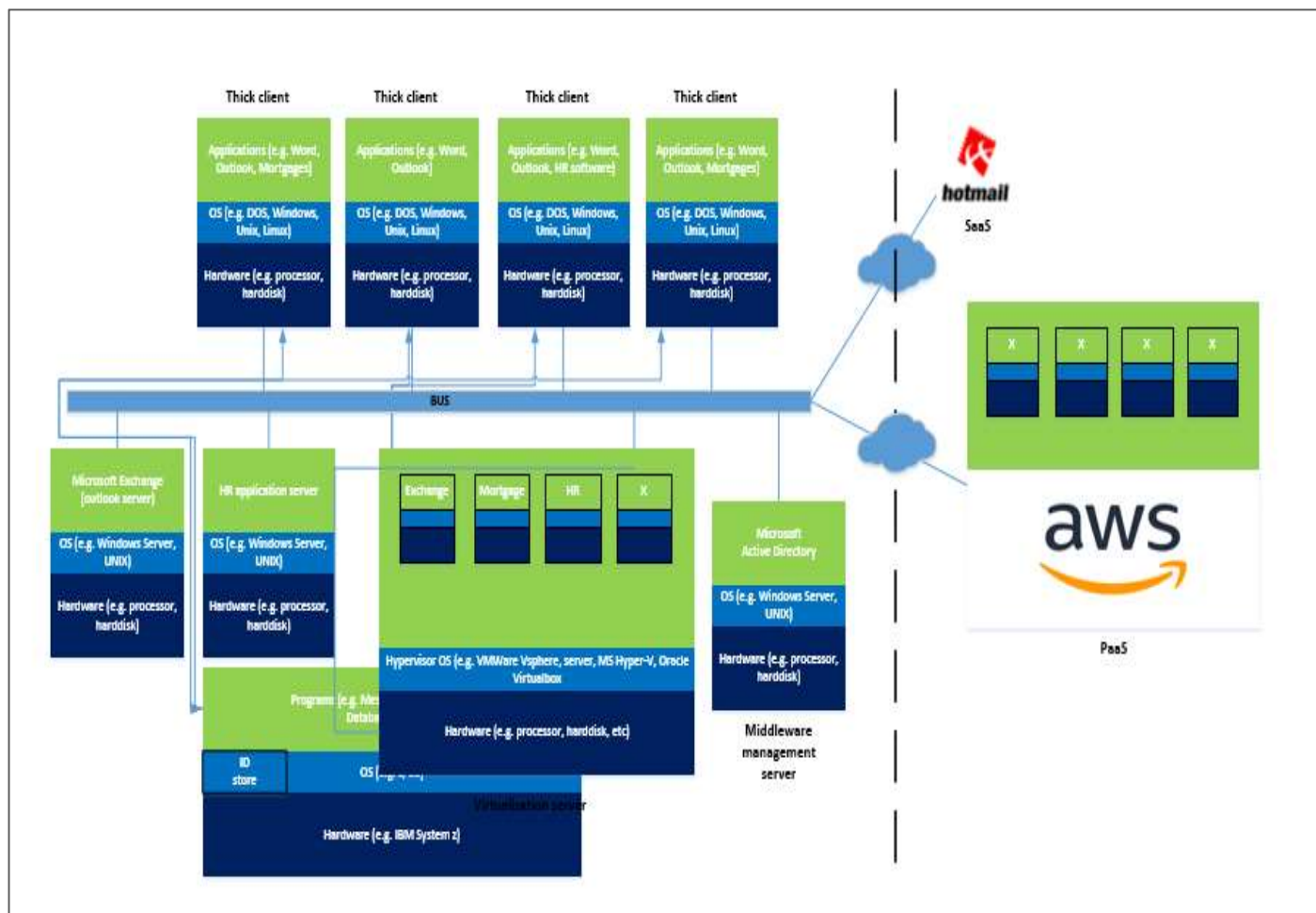
- Machine **authentication** to prevent unauthorised machines
- Proper **procedures** to **authorise new machines on network** and to **decommission** existing ones.
- Properly configured firewalls, IPS and other security devices.

General Client and Server Protection

- **Clients → Workstations, Mobile Devices**
 - Hardening/Group Policy from Domain Controller if Windows
 - Non admin rights to users
 - Central management/patching
 - Antivirus, antimalware - endpoint protection
 - Intrusion prevention system
 - File Integrity Monitoring
 - Removable media restrictions
 - Browsing and email control
 - Logging and Monitoring
- **Servers → Database, Application, Web, Management duties or Utilities**
 - Hardening/Group Policy from Domain Controller if Windows
 - Antivirus, antimalware - endpoint protection
 - Intrusion prevention system
 - File Integrity Monitoring
 - Removable media restrictions
 - Logging and Monitoring
 - Central management/patching

Protection – Network & IT infrastructure

Technologies – the complex reality



Cloud Services

VoIP - Voice over IP

Video Conference equipment

Storage Area Network (SAN) and fibre channel switches

Virtual containers

Decentralised Databases

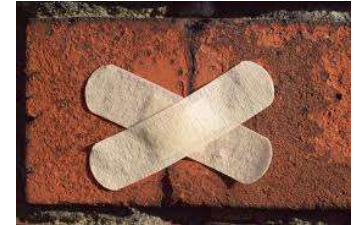
AS400 Nonstop servers

Hardware Security Modules

Change Management

- Change management is deeply connected to the **asset management** process and to the **identification** of the most critical assets. To this regard, it is crucial to have **criteria** to prioritise changes (and to be able to perform emergency changes)
- Changes to system configurations should be strictly **controlled** and **monitored**, to avoid harmful effects in terms of confidentiality, integrity, and availability
- Changes should be **properly documented and communicated to the organisation** → failing to document changes can cause only trouble to the organisation
- There should also be the possibility of **rolling back unsuccessful** changes
- **Different** procedures/processes could exist for various systems, types of changes etc.

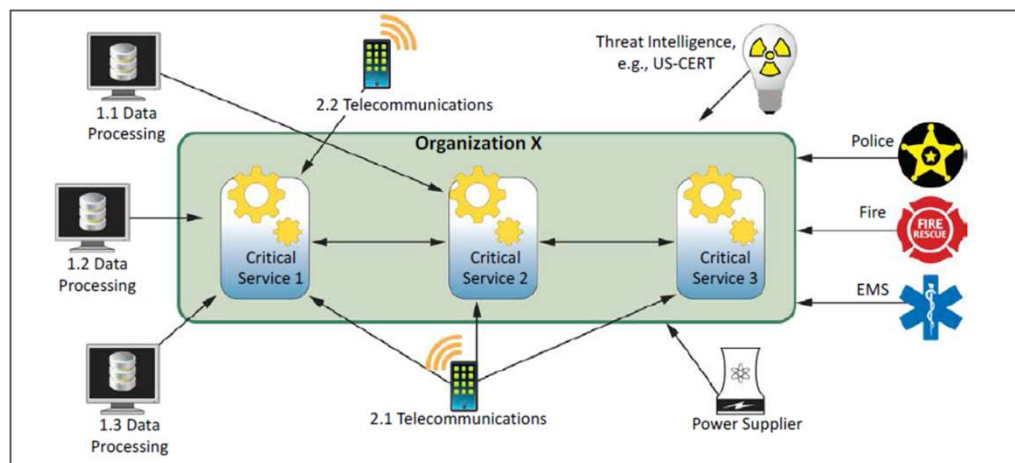
Patch management



Main **aspects** to be considered in a patch management process:

- **Severity** of the vulnerability → Priority for patching
- **Timing** for installing the patch
- Patching **configuration**:
 - **Automated , centralised, decentralised**
- **Dependencies** on other patches
- **Testing** of the impacts of patches (i.e. downgrade of system performances)
→ preferable to test patches on isolated systems
- **Approval** process
- **Roll back process** in case of failure
- **Critical** to prevent/detect cyberattacks
- System **downtime**, lack of **testing** systems and **resource intensiveness**
are a big issue.

Third Party Risks



Lowering of control

Loss of knowledge in the organization

Dependence on the service provider

Long and complex outsourcing chains

Legal and Compliance

Conflict of interest

Dependence on internet access

Operational

Reputational (Data leakage)

Vendor lock-in

Concentration on a few service providers

Physical controls

- Adequate physical controls should be applied to protect office premises, data centers, sensitive areas (e.g. technical rooms with network devices/cabling..).
- Examples:
 - Access controls (reception, badges, locks, security guard, intrusion alarms...);
 - Smoke detectors, fire extinguishing systems;
 - UPS;
 - Air conditioning;
 - Water flood detectors;
 - ...
- Physical security controls should be periodically reviewed/audited:
 - Users with access rights to data rooms /sensitive areas;
 - Data center certifications (e.g. Tier, ISO27001, ISAE 3402 type II,...)



Agenda

1	Context, main definitions and the CROE
2	Governance and Continuous Evolution
3	Identification and Situational Awareness
4	Protection
5	Detection
6	Response and Recovery
7	Annexes

Security Incident

- **Multiple ways** of detection of a security incident exist:
 - **Event** with operational impact such as an outage
 - **Security** event investigation
 - **Human** observance
 - **Processes**, such as reconciliation
 - **Threat intelligence** – Indicators of Compromise (IOCs)
 - **Third Party** notifications
 - **Machine Learning** systems / Anomaly detection → got very advanced recently
 - **Deception** Technology → creation of fake targets
- Focus should be on:
 - **Training** and empowering staff to **report** anything suspicious.
 - Building the **technical capabilities** to **log** and **monitor** systems for potential security incidents.

Logging and Monitoring

- Logging is the process to **capture** details related to **events** and **activities** occurring on a system → *who did what, when, where and how*
- The object is to **track** and **record** all the activities, to provide **accountability, detect anomalies, incident management, response, and investigations**
- Logs come from firewalls, IDS, IPS, routers, servers, domain controllers, applications, devices,...
- Logs must be **protected** to guarantee **integrity** and **availability**



- Due to the high volumes and different types of logs, the log analysis is generally supported by specific **systems**, able also to normalize and correlate different information → **Security Information and Event Management (SIEM)**
– **Splunk, Arcsight, Q Radar** etc.

Logging and monitoring in an FMI - SIEM

Security Incident Event Management (SIEM) is able to **gather**, monitor, **manage**, and **correlate logs** in real time, in order to **detect anomalous behaviour** in the organization's technology infrastructure (devices, network, applications, etc).

- **Critical** components and IT infrastructure should be **logged** at the level of Operating System, Application, Database, network devices, security devices, IDS/IPS, firewall, antivirus, document management system, etc.
- Any **missing logs** is **missing visibility** from a cyberattack
- Logs must be **properly configured** for each and every to ensure they are capturing the necessary information but not capturing “noise” that will lead to false positives
- The logs need to be **protected** from deletion or modification from administrators but also be available for a significant amount of time to aid in investigations. The logs could also be **digitally signed** to enable use as presentation of evidence in court if need be
- Logs are useless without **security intelligence**, **business parameters** and **correlation** → we are talking about millions of lines!

Logging and monitoring in an FMI – SIEM

- **What** correlation rules are in place? **How** are they updated, based on what criteria? How **frequently**?
- A SIEM constantly generates security alerts to be investigated and analysed by security **analysts** independent from operations.
- Events must be timely **analysed** and recognised either as an incident or as false positive etc.
- These **parameters** used to generate alert must be **revaluated** and **changed** in a controlled and authorised manner.
- Designating an alert as **false positive** must be **controlled**.
- SIEM upon deployment **will** generate a lot of **false positives** and there is an effort from analysts to constantly fine tune and maximise the efficiency of the logging and monitoring effort.

ALL ALERTS ARE POTENTIAL SECURITY INCIDENTS

Agenda

1	Context, main definitions and the CROE
2	Governance and Continuous Evolution
3	Identification and Situational Awareness
4	Protection
5	Detection
6	Response and Recovery
7	Annexes

Incident Response in an FMI

- It is a documented **policy statement**, with a generic procedure and **specific** plans in case of specific cyberattacks (e.g. ransomware, exfiltration, integrity breach)
- Incident **log** must exist (and not empty)
- **Technical Response**
 - Who? What? How? When?
 - Main elements:
 - Forensic capability and associated processes
 - Contagion strategies and desktop walkthroughs of the plans
 - Ensured readiness and availability of the technical teams
- **Business Side**
 - Tight integration with CRISIS Management and Business Continuity
 - Incident Response Team: Who does what, how, by when and who leads?
 - Has Incident Response Team been trained and do they test their readiness regularly?

TESTING!

Incident Response in an FMI

- FMI employees as well as third parties, insourced employees must be able to **report** security incidents, it is **not only** the Security Operation Centre's job to detect incidents and incidents (e.g. an employee stealing confidential information from a printer is not something a SOC would detect).
- Forensics which also include **malware analysis** are in-house in large FMIs and could be integrated with SOC (creating a SOC-Computer Emergency Response Team (CERT)) and outsourced in smaller FMIs (but with specific response times in contract).

Crisis Management

- **Operational incidents, security incidents**, as well as other events (e.g. damaging the reputation of the organisation) must interface with and trigger CRISIS Management.
- It is important to understand that an event such as a core system downtime would be treated as an **operational incident**, would be investigated to determine it is not a security incident, and also trigger a **CRISIS management** response as clients are affected.
- Main actions:
 - Informing all relevant authorities and communicating with stakeholders
 - Issuing press releases
 - Investigating the problem and determining the most prudent course of action
 - Approving initiation of recovery activities
 - In general steering the FMI in a way to minimise risk in light of the incident that occurred.
- For this to be effective the proper people (seniority and skill) must be **trained** and be involved as well as routinely test their readiness.

Recovery

Overlaps with traditional Disaster Recovery Planning and Business Continuity Planning of the FMI, the FMI must also be ready to **recover** its operations in case of cyberattack and test such plausible scenarios (e.g. a cyberattack compromises the network and customer data of the production systems)

- How **resilient** are the systems underpinning critical operations?
- Are the **backups** kept in a way to be safeguarded from a cyberattack? How quickly can the business data be restored?
- Can the FMI **restore** the latest trusted software from offline golden copies? And can it do it fast enough if there are hundreds of machines?
- How long would it take to **recover** software and data and be ready to continue operations?
- How is the **Ecosystem** involved.

This is an iterative process and a never ending one. There are always more scenarios and a higher degree of resilience plus faster recovery to be accomplished.

Recovery

- Identifying critical operations and setting correct **Recovery Time Objectives** and **Recovery Point Objectives** is key. It is also crucial that the correct IT infrastructure and other necessary components (could be individuals, third parties) that underpin the critical operations be correctly accounted.
- There should be a link from the IRM assessment of a system and its recovery capability. The higher the criticality from an availability perspective the faster a system should recover.
- FMs usually **have multiple sites** with IT infrastructure using technologies such as optical fibres to facilitate communications and Storage Area Networks (SANs) to replicate data. In case of cyberattack this leads to increased propagation and means FMs must be ready to operate in a world where these sites have been compromised.
- Scenarios for designing and testing recovery (from a cyber perspective) should also be based on **Threat Intelligence** information. Of course recovery under other scenarios such as terrorism, strikes, pandemics, natural disasters, region unavailability, civil unrest/war should be evaluated and tested.

Conclusion - Key messages

- To reach and evolve to high levels of cyber resilience:
 - A **continuous monitoring of new trends in cyber attacks** and **update of defence mechanisms** are key
 - Focus not only **technology**, but consider also **processes** and **people**
 - Design, test, implement and update both **preventive, detective** and **reactive** controls.
- Do **not forget 4** crucial elements as:
 - **The establishment of a proper governance**
 - **The identification and prioritization of risks**
 - **Use of an established framework**
 - **The risk stemming from third parties and new technologies must be identified and managed**



Annex – Cyber Resilience Indicators, case studies and further information on CROE

CROE Assessment process

- The operator writes a self-assessment up to the required level of expectation.
- If the expectation is „advancing“ the self-assessment must cover all elements in „evolving“ and „advancing“
 - An FMI can – if it wants to – also write a self-assessment for the level beyond the expected level;
 - An FMI can use the ***meet or explain principle*** if it does not meet an expectation, but feels that it achieves the intended outcome through another means;
- Operator submits self-assessment including background documentation
- Overseers assesses the materials:
 - Does the FMI meet the expectations?
 - If not, is the explanation provided sufficient?
- Overseer/operator meetings are held to discuss the material and agree on action plans to improve the system (if required)
- The overseer drafts a short CROE report which includes the weaknesses identified and recommendations for improvements
- The report is shared with the operator

Governance

- **Cyber governance** refers to the arrangements an FMI has put in place to establish, implement and review its approach to managing cyber risks. Effective cyber governance should start with a clear and comprehensive cyber resilience framework, guided by a cyber resilience strategy.
- In ***Evolving***, focus is on establishing a Board-approved Cyber Resilience Strategy and Framework, with strong involvement of the Board and senior management, with adequate skills, accountability and the right culture.
- In ***Advancing***, focus is on using maturity models and defining relevant metrics to assess and measure the adequacy and effectiveness of and adherence to its cyber resilience framework through independent compliance programmes and audits carried out by qualified staff on a regular basis.
- In ***Innovating***, focus is on establishing the appropriate structures, processes and relationships with the key stakeholders in the ecosystem to continuously and proactively enhance the ecosystem's cyber resilience and promote financial stability objectives as a whole.

Cyber resilience strategy and framework

- Strategy: High level document, declaring the FMI's commitment and tangible milestones in delivering its cyber resilience objectives.
- Its purpose is to show that the highest governance body of the FMI acknowledges the importance of cyber resilience, integrates it into its broader strategic objectives, encompasses it into all aspects of the business, has established appropriate governance and is monitoring progress.
- ***As part of the CROE assessment, overseers should request a copy of the FMI's cyber resilience strategy and framework, as approved by the Board.***
- ***When reviewing the strategy and framework, the overseers should discuss what process the FMI went through to develop it and which stakeholders they consulted (internal and external)***

Key considerations that should be addressed within the cyber resilience strategy

- The importance of cyber resilience to the FMI and its key stakeholders
- The role of the FMI's internal and external stakeholders in ensuring cyber resilience of the FMI
- The FMI's vision and mission in relation to cyber resilience.
- The cyber resilience objectives that the FMI will work towards, which should include ensuring the ongoing efficiency, effectiveness and economic viability of its services to its users and maintaining and promoting its ability to anticipate, withstand, contain and recover from attacks.
- The FMI's cyber risk appetite, to ensure that it remains consistent with the enterprise risk tolerance, as well as with the overall business objectives and corporate strategy.
- Clear and credible maturity targets and a roadmap or implementation plan with change delivery and planning of capabilities relating to people, processes and technology at pace with threats and proportionate to the FMI's size and criticality. The strategy should clearly set out how this roadmap or implementation plan will be delivered and how the Board should track and monitor delivery.
- The high-level scope of technology and assets covered by the Strategy and subsequent Framework.
- The governance necessary to enable cyber resilience to be designed, transitioned, operated and improved.
- How cyber resilience initiatives will be delivered, managed and funded, including the budgeting process and organisational capabilities.
- How cyber resilience will be integrated into all aspects of the business, which includes people, processes, technology and new business initiatives.

Cyber Resilience Framework

- **Cyber Resilience Framework: *Consists of the policies, procedures and controls an FMI has established to identify, protect, detect, respond to and recover from the plausible sources of cyber risks it faces.***
- The Framework could be comprised of a number of different documents: includes policies, procedures, processes, workflows, etc.
- The Framework should cover the following key areas:
 - Identification including asset classification and risk
 - Protection
 - Change and patch management
 - Logical and physical controls
 - HR security
 - 3rd party security management
 - Detection
 - Security incident and forensics
 - Response and Recovery
 - Testing
 - Situational awareness
 - Learning and Evolving

Board responsibility

- **The FMI's Board approves the cyber strategy and framework; sets the risk tolerance; and oversees the implementation of the framework.**
- The Board and senior management must have the adequate level of skills, knowledge and experience to discharge its responsibilities with regards to cyber resilience.
- Overseers should query:
 - What does the Board know or do on cyber resilience?
 - Is it discussed regularly? (standard agenda item)
 - Do they decide on initiatives and programs and assign them high priority?
 - Are they trained and regularly updated on the latest developments in the field relating to cyber resilience?
 - Are they briefed on incidents and the lessons learned?
 - Do they keep up to date on the status of the FMI's cyber posture using dashboards and metrics?
 - Are they regularly assessed themselves on their roles, responsibilities and understanding of cyber?

Senior management (CISO) responsibility

- The FMI should delegate responsibility and accountability for the implementing the cyber resilience strategy and framework to a senior executive (e.g. CISO) – should be independent, skilled and have adequate resources.
- Overseers should query:
 - Who is responsible for cyber resilience?
 - What experience does this person have on cyber?
 - What responsibilities / power does this person have for cyber?
 - What level / seniority is this person at? Where does this person sit in the organogram – e.g. second line of defence?
 - Where and how often does this person get information from, to monitor strategy and framework implementation?
 - Who does this person report to?

Culture and skills

- **The FMI should cultivate a strong level of awareness within the FMI with regards to cyber resilience; ensure a continuous training programme is in place; identify the competencies, skills and resources required to deliver the cyber programme and invest accordingly.**
- In general:
 - Culture is difficult to define but can be felt within an institution.
 - Do people wear tags in premises?
 - Are there cybersecurity posters in premises?
 - Do people lock their screens and clear their desks before going for a break?
 - Is security part of their annual performance reviews or compliance framework?
 - Has the FMI established a competency skills framework for Information Security/Cyber capabilities?
 - Does management seem to actively participate in security initiatives?
 - Is there a comprehensive training programme in place? What types of solutions do they use to deliver training?

Governance indicators

- **Board level Information Security/Cyber**
 - What information do they get?
 - How often?
- **CISO**
 - What powers does the person have?
 - Independence?
 - Experience?
 - Reporting?
 - Escalations?
 - Results?
- **Cyber Resilience Strategy**
 - When was it reviewed? What does it cover?
- **Cyber Resilience Framework**
 - When was it reviewed? What does it cover?
 - How detailed is it?
- **Cyber Resilience Culture and Skills**
 - Is there a skills competency matrix?
 - Are there training programmes and metrics to measure performance?
 - Are there company slogans and initiatives?

Brainstorming questions: Governance

Your FMI has recently appointed a CISO, which is the first time they have such a role in their organisation. As the overseer, what is the first thing you would want to see from the CISO? What would your primary concerns be?

The CISO has decided to report to the Board on its cyber resilience programme. As an overseer, you ask to see an example of what is being reported to the Board. What would you expect to be reported?

As an overseer, how would you evaluate whether the Board is knowledgeable about and challenging on cyber resilience?

Identification

- In **Identification**, the FMI should identify its critical functions and the processes and information assets supporting those critical functions and any interconnections to be able to effectively direct its protection, detection and response and recovery efforts/investments to those assets to strengthen its overall cyber resilience posture.
- In **Evolving**, is on identifying, documenting and conducting risk assessments, on a regular basis, of all the critical functions, key roles, processes, information assets, third-party service providers and interconnections to determine, classify and document their level of criticality. This implies having different inventories, which need to be updated regularly and the need to conduct risk assessments.
- In **Advancing**, focus is on using more automated and centralized tools (e.g. a centralised asset inventory management [AIM] tool and/or a centralised identity and access management [IAM] tool) that facilitate the update of the information and its analysis.
- In **Innovating**, the FMI's focus is on having a more proactive approach regarding risks, using the information of the automated tools to anticipate risks and work actively with its ecosystem. This may involve identifying common vulnerabilities and threats.

High level Identification process: asset inventory

1. In order to protect your assets, you need to know what you have and where it is;
2. Then you need to determine the sensitivity / criticality of these assets;
3. Then you need to understand the risks to these assets;
4. Then you need to implement controls to mitigate risks to these assets.

Step 1 is critical as you cannot safeguard what you do not know you have!

Actions for the overseers - Identification

1. Ask for the **risk assessment** conducted by the FMI to identify critical functions, processes, and information assets supporting them (I1), and any interconnections (I2).
2. Ask for the **inventory of information assets** (I8) (definition in glossary), which should include: hardware, software and data, i.e. the information used by the FMI to conduct its critical functions, where it is stored, and the software used. This inventory should include: owner of the asset (I3), its criticality (I4), interconnections of the assets (internal or external) (I3), update policy (who and frequency) (I6, I11).
3. Ask for the **map of network resources** (I5, I10) to know the interdependencies.
4. Ask for the **access rights** inventory or accounts inventory (I7, I9).

Cyber Resilience Indicators

- **Information Asset Inventory**

- *How is the **FMI** conducting it (**AIM**)? What details are included?*
- *How does the FMI ensure that **non electronic/offline assets** are documented?*
- *Is there a **process/metric** to ensure it is accurate and up to date?*
- *Are **interdependencies/ interconnections** mapped?*

- **Risk**

- *What **methodology** was selected and why?*
- *How **often** are the assessments conducted?*
- *Does the FMI use a **tool** and incorporate other metrics and information?*
- *What happens to **accepted** risks? How are they monitored?*
- *In an **assessment** does the action seem to justify residual risk?*

- **Threat Intelligence**

- *How is it performed?*
- *Where does the FMI get **feeds** from?*
- *What does the FMI do with the feeds?*
- *What are its plans to **maximise** the use of TI in its **security framework**?*

Cyber Resilience Indicators

- **Information Sharing**

- *Has it been setup?*
- *What kind of **information sharing** is taking place? With whom? How often?*
- *How is information **shared**?*
- *Is there an **emergency process** to share information during an incident to the relevant parties?*
- *Is this sharing in the **incident response process**?*

Brainstorming question: Identification

Your FMI has approached you as the overseer to ask whether they should invest in a centralised asset inventory management [AIM] tool and a centralised identity and access management [IAM] tool. They are concerned about the cost implications and they want your view. What would you say?

Protection

What to protect?

- All entities critical to the FMI's material operations: key roles, processes, systems, inf. assets, interconnections, TP-services → "Identification"

Protect in what regard?

- Confidentiality, Integrity, Availability (CIA)

Protect in what state?

- At rest, in transit, in use (data)
- Before, during, after employment (access)

When to include protection?

- During operation, during design

How to protect?

- Defence-in-depth → multiple, compl. meas.



<https://de.freeimages.com/photo/red-onion-1328914>, 24.04.2019

www.ecb.europa.eu ©

Protection

Protective measures:

- **Physical:** e.g. perimeter security, phys. access control
- **Logical / technical:** e.g. log. access control, firewalls, AV, encryption, VPN, IDS/IPS, proxy
- **Structural:** e.g. network separation, DMZ, Bastion/Jump server

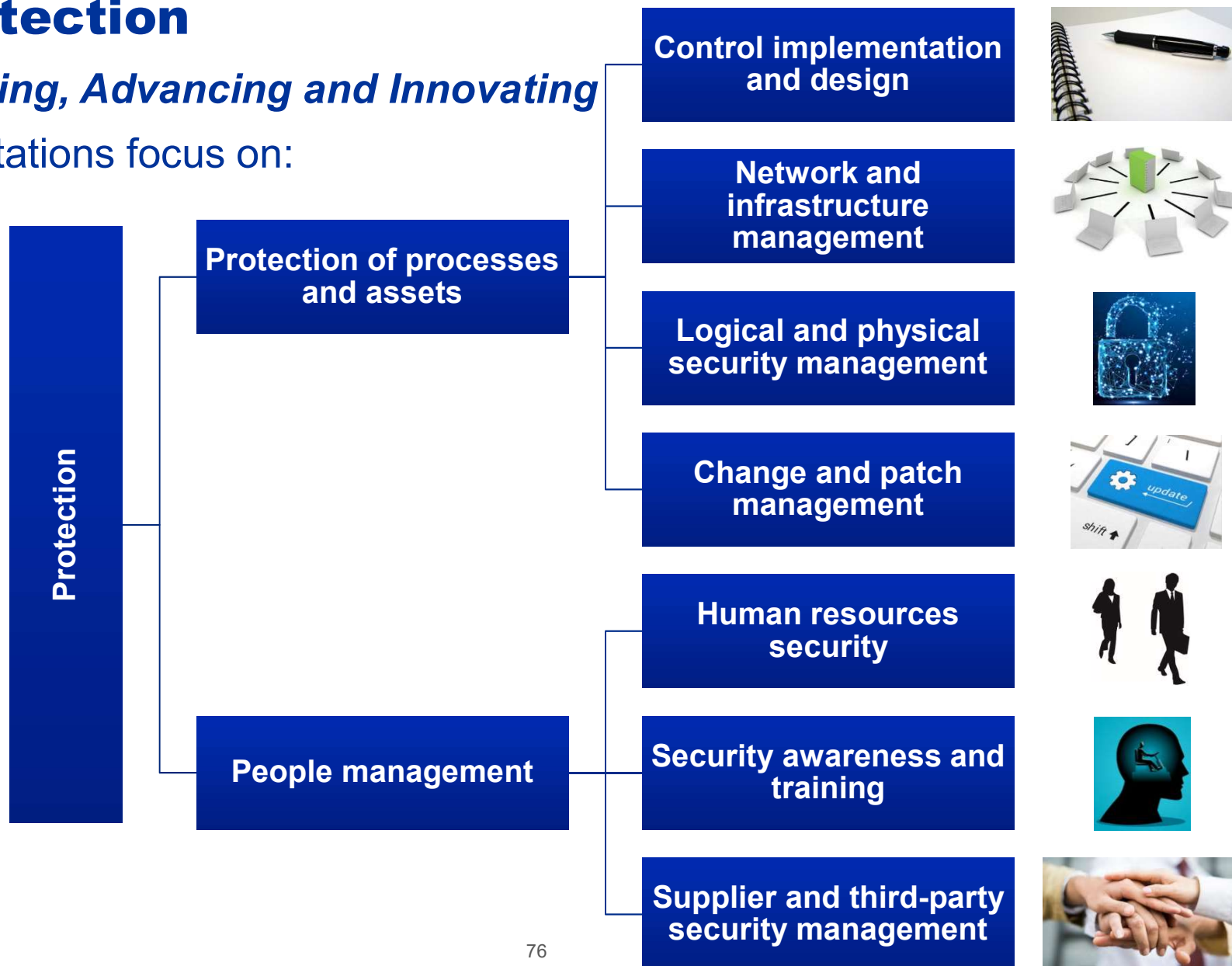
• **Organizational:** e.g. four-eye-principle, patch management rules, contractual arrangements with third parties

- **Awareness:** e.g. sensitization, anti social-engineering competencies, secure password usage



7) Protection

- Evolving, Advancing and Innovating* expectations focus on:



Protection questions

- Control implementation and design:
 - Are security controls designed and implemented successfully based on risk facing the FMI?
 - Do these controls cover physical security and people security aspects?
 - Are these controls regularly reviewed?
 - Is an information security management system (ISMS) implemented? Is it based on any well-recognised international standard? Which one?
 - Is cyber risk management in place at each stage of the system development life cycle (SDLC)?
- Network and infrastructure management:
 - How is the network protected?
 - Are baseline system and security configurations established and documented?
 - Is IT infrastructure adequately separated with different security levels and controls implemented?
 - How are non-controlled devices prevented from connecting to the internal network?



Protection questions

- Logical and physical security management:
 - Are there any processes to manage the creation, modification or deletion of user access rights (physical and logical)?
 - Are there any procedures that address user accounts management in accordance with a role-based access control (RBAC)?
 - Are there any specific procedures to allocate privileged access on a need-to-use or an event-by-event basis? How is it organized?
 - Are there any controls implemented to prevent unauthorised privilege escalation?
 - How is data protected (at rest, in transit, in use)?
- Change and patch management:
 - Are there any policies, procedures and controls in place for change management?
 - Is there a patch management policy?
 - How are changes tested?
 - Is there any procedure or fall-back in case of unsuccessful change or patch implementation?



Protection questions

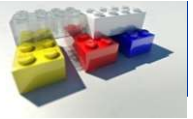
- Human resources security:
 - What is the process for on-boarding new staff?
 - What is the process for employment termination, i.e. off-boarding?
 - Is there any procedure for granting or revoking access to systems when an employee is changing responsibilities?
- Security awareness and training:
 - Are there any security awareness trainings organized for the employees and/or contractors? How often?
 - Are these trainings properly customised to help employees understand their roles and responsibilities in protecting the FMI's assets?
 - How does the FMI validate the effectiveness of its trainings?
- Supplier and third-party security management:
 - How often are third-party risk assessments carried out? Which tools are used?
 - Are there any security controls implemented that detect and prevent intrusions from third-party connections?



Cyber Resilience Indicators

- **Security Control Framework**

- *When was it reviewed? What does it cover? (It should cover what a standard like ISO27002 etc)*
- *How detailed is it? Does it contain all the **necessary policies, procedures, processes, guidelines**?*
- ***Regulatory / Legal requirements** included?*
- *Does it cover new **technologies**?*
- *Are there limits to the **scope** covered?*
- *Is it aligned with the **business objectives** and how is this ensured?*



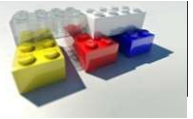
Cyber Resilience Indicators

- *Proper user registration/registration(and timely) procedures?*
- *Proper user access granting/revocation of roles/rights procedures with clear authorisation?*
- *Procedure to review access rights of users in a routine and meaningful manner?*
- *Are there defined roles with **controlled changes of permissions for Information Repositories and critical systems**?*
- *Controlled and defined use of technical accounts (non human) via procedures/automated systems?*
- *Any results on testing regarding **Identity and Access Management**?*
- *Controlled and defined use of **privileged accounts** via procedures/automated systems?*
- *Proper password and account lockout configuration?*
- *Single Sign On, IAM are clear sings of mature identity and access management, How are they used and configured? If not what procedures exist to fulfil the same control objective*



Cyber Resilience Indicators

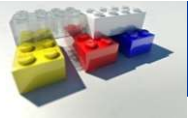
- **Data Loss Protection/ Digital Rights Management** configured and aligned with Information/Data Classification scheme?
- **File/folder encryption / Document management system encryption** via aligned with the aforementioned classification?
- **Port restrictions** (such as USB) with procedure for exceptions?
- **Email and browsing** controls?
- What network controls are in place?



Cyber Resilience Indicators

- **Data at Rest**
 - *How encryption is applied to:*
 - Documents
 - Databases
 - Email messages
 - Backups
 - Workstation/ mobile devices
 - User credential storage
- **Data in transit**
 - *How encryption is applied to:*
 - Email messages
 - Remote access sessions
 - Helpdesk/ Administrative remote management
 - Web services internal and external

➡ Implementation / Key management is crucial! Who is responsible and how are they protected?



HR Security in an FMI - indicators

- **Employment**

- *Processes and checks prior to employment like credit checks, criminal record, reference checking?*
- *Processes and checks during employment like credit checks, criminal record, and providing “whistle blowing” capabilities (for insider threats)?*
- *Procedure for employee termination with checklists?*

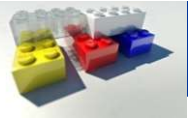
- **Security awareness and training**

- *Organised Training Programme/Plan approved by management?*
- *Plan covering also external parties and insourced employees?*
- *Plan also covering special groups like system admins, employees with access to sensitive information and senior management / board?*
- *Conduct social engineering and phishing tests and use results to educate staff?*



Cyber Resilience Indicators

- *High level **network diagram** and detailed segment diagrams? Updated?*
- ***Intrusion Detection/ Prevention Systems (IDS/ IPS)** configured, tested and updated?*
- ***Firewalls and IDS/IPS** in place between boundaries like untrusted and trusted areas and between critical machines and users?*
- *Proper network **segmentation**?*
- ***Firewall rule review**? How often? Who?*
- *Proper firewall and network device **control and authorisation**?*
- *Proper firewall and network device **patching**?*
- *Has the **network segmentation and controls** been tested?*
- ***Web Application Firewall** to protect web applications especially from external users and internally for high criticality web applications?*
- *Web application firewall regularly tested and updated?*
- ***Machine authentication** on network?*
- *Procedures for new machines on the network and removal of existing ones?*
- *How do machines get their IP? DHCP, Static? Network Access Control?*
- *Plan to deal with **unauthorised machines** connected to the network?*



Cyber Resilience Indicators

- ***Configuration standards** for all off the shelf technologies including Hypervisor and virtualised software as well as virtual networking equipment?*
- *Patching of the **virtual** infrastructure, how does it happen? When?*
- *Risk assessment on **virtualisation or other new technologies** and taking account of virtualisation in the risk assessments of virtualised systems ?*
- ***Database Firewall** correctly, tested, configured and access rights reviewed?*
- *IT Staff trained in the technologies they administrate?*
- *IT Staff adequately staffed?*
- *Reliance on third parties for system administration?*



Cyber Resilience Indicators

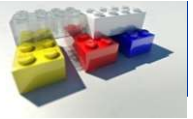
- *Is there a policy on **change management**? Is there a procedure on change management? **Scope**?*
- *Is there a policy on **patch management**? Is there a **procedure** on patch management? What triggers a patch procedure? **Scope**?*
- *Are their rollback procedures?*
- *What testing occurs for changes to systems to make sure loss of Confidentiality, Integrity, and Availability does not ensue?*
- *What security testing occurs for changes to systems?*
- *How are changes/patches tested when there is **no test environment**?*
- *How are changes **approved**?*
- *How are patches **approved**?*
- *How **frequently** are patches deployed on **workstations**? What is patched on **workstations**? **Operating Systems**? **BIOS**? **Applications**?*
- *How frequently are patches deployed on **servers**? **DBs**?*
- *How frequently are patches deployed on **network and security infrastructure**?*
- *How is the frequency of patching determined?*
- *What happened with systems that **cannot be patched**? **EOL**?*
- *Is there an **emergency patching process** / **Change management**?*
- *% of systems where application inventory is updated*
- *% of patched systems (manually, via semi automated or fully automated patching procedures)*



Cyber Resilience Indicators

• Third Party Risk

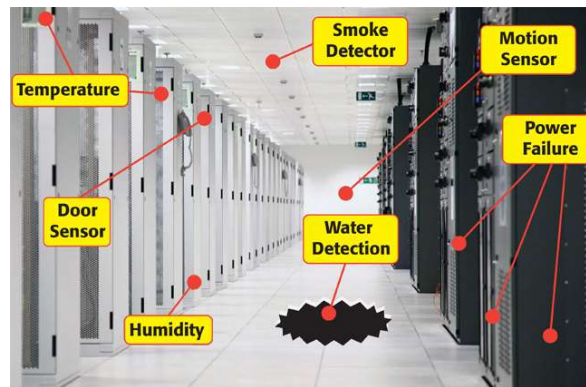
- *Is there a policy on how to perform **outsourcing** to third parties?*
- *Is there a procedure on how to get such an **outsourced** activity approved?*
- *What has been **outsourced**? Is there a list? Who is **responsible** for each agreement/ outsourcing activity?*
- *How is it ensured that these **third parties comply with security requirements** and other **compliance requirements** of the FMI?*
- *Does **security testing** also cover critical third parties?*
- *How has **risk been assessed** for these third parties? Is it repeated in a systematic manner?*
- *Are there clauses for compliance in the contract with other **regulations/laws with penalties**?*
- *Is there a **right to audit** or other way to get assurance? What are the results of these audits?*
- *How do these third parties integrate into the **information security processes** (e.g. incident management)?*
- *How does the FMI deal with **non compliances** or security issues stemming from the third parties?*
- *Is there an **exit strategy**?*



Cyber Resilience Indicators

• Physical Security Management

- *Is there a policy on **physical and environmental security**?*
- *Is there proper **access control** for high sensitivity information assets?*
- *Are **access rights** reviewed?*
- *Is there **CCTV** in the entry points of data centres and in areas of high sensitivity information assets?*
- *Are there proper **environmental conditions** for data centres and media **storage** rooms?*
- *Are physical controls tested? Are the tests used to improve the physical security of these assets?*
- *How is **physical** media destroyed? What **policies/procedures** are in place?*



Brainstorming question: Protection

Your FMI has decided to expand its business by providing a new payment service, requiring new infrastructure, which they are aiming to build over the next year. As an overseer, tasked with assessing this proposal, what would you expect to see from the FMI? What questions would you ask? What areas would you investigate?

Detection

- In **Detection**, FMIs should be able to recognise signs of a potential cyber incident, or detect that an actual breach has taken place. Early detection provides an FMI with useful lead time to mount appropriate countermeasures against a potential breach, and allows proactive containment of actual breaches.
- In **Evolving**, focus is on developing detection capabilities to monitor (e.g. network traffic, system activities, user activity, connections, external service providers, devices and software) and detect anomalous activities and events. Such capabilities have to be periodically reviewed, tested and updated appropriately by appropriately trained staff.
- In **Advancing**, focus is on developing and implementing automated mechanisms (e.g. a security information and event management (SIEM) system) and/or a process to collect, centralise and correlate event information from multiple sources and log analysis to continuously monitor the IT environment (e.g. via a Security Operations Centre).
- In **Innovating**, focus is on continuously exploring new technologies and techniques inhibiting lateral movement (e.g. deception mechanisms) which trigger alerts and inform the FMI of potential malicious activity when accessed.

Actions for the overseers - Detection

- Check how the FMI organizes monitoring of critical processes, assets and connections.
- Are there any rules describing the appropriate criteria, parameters and triggers to enable alerts and initiate the incident response process, if required?
- Is baseline profile of system activities documented?
- Is there any process to analyse the information collected? Manual? Automatic?
- Is there any process to collect, centralise and correlate event information from multiple sources? How are logs backed up and stored?
- Are employees properly trained to be able to identify and report anomalous activity and events ?



Cyber Resilience Indicators

- **Detection**

- *Training* of users to help reporting of incidents?
- Presence of a **SIEM** solution, operational and working?
- **Threat Intelligence** procedures
- Further **mechanisms** focusing on newer technologies

- **Logging and Monitoring**

- Link to **risk** assessment?
- **SIEM operational** and working at least for critical systems and their dependencies?
- **SIEM procedures**?
- **Security Incident logs**?
- Multiple **examples** of **rule changes**?
- **Training** of analysts?
- Adequate **staffing**?
- Is monitoring **24/7**?

Brainstorming question: Detection

Your FMI has recently designed and implemented a SOC. This SOC operates during business hours, and after business hours, they outsource SOC services to a third party. As an overseer, what would your concerns with such a set up be?

Response and Recovery

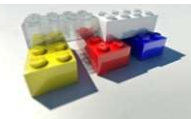
- In **Response and Recovery**, FMI's arrangements should be designed to enable it to resume critical operations rapidly, safely and with accurate data in order to mitigate the potentially systemic risks of failure to meet such obligations when participants are expecting it to meet them.
- In this chapter, ***Evolving, Advancing and Innovating*** expectations focus on:
 - Cyber resilience incident management;
 - Data integrity;
 - Communication and collaboration;
 - Contagion;
 - Crisis communication and responsible disclosure; and
 - Forensic readiness.
- The focus is not solely on an individual FMI's readiness to respond, recover and resume, but how it can do so in collaboration with the wider ecosystem, and leverages off industry best practices for business continuity.

Recovery and response

- In **Evolving**, focus is on having in place RTO/RPO, contingency and recovery plans for cyber incidents, and testing them. A back-up policy should be in place and the back-up mechanism should ensure confidentiality, integrity and availability of data, and be tested. The FMI should identify external connectivity dependencies and develop policies and procedures to enable resumption. Communication plan and procedures should be in place to communicate/coordinate with internal and external stakeholders and regularly reviewed. The FMI should have a Forensic Readiness Policy, identify digital evidence based on threat scenarios, and have procedures for the collection of digital evidence.
- In **Advancing**, focus is on 2 hours RTO, prioritization of restoration orders based upon functional/dependency maps, continuous ecosystem monitoring for technology solutions and engagement with ecosystem stakeholders to enhance contingency, response, resumption and recovery capabilities. The FMI shall have alternate back-up site with distinct risk profile, have transaction recovery mechanisms, periodic reconciliations with participants, restoration capabilities using standardized configurations. The FMI shall have roll-back mechanisms and procedures with its interconnected entities that are periodically tested. The FMI should have communication plans for a range of cyber incident scenarios.
- In **Innovating**, focus is on continuous improvement of cyber response, resumption and recovery plans, continuous collaboration with ecosystem, regular scenario testing, implementation of CSIRT and automation of incident responses. Back-up and recovery should be integrated in the acquisition/development processes, redundant system ensuring 0 data loss in place, consideration of data sharing agreements in order to recover uncorrupted data. Segmentation of network infrastructures to prevent contagion, mechanisms to notify senior management, relevant employees and stakeholders. Management review process to improve forensics, collaboration with ecosystem to improve lawful forensic investigation.

Action for overseers

	For Evolving level, request/ask	For Advancing level, request/ask in addition	For Innovating level, request/ask in addition
Cyber resilience incident management	<ul style="list-style-type: none"> Request RTO/RPOs for its service/applications Request contingency and recovery plans Request results of last test 	<ul style="list-style-type: none"> Request functional and dependency maps Confirm how the FMI continuously monitors technology and ecosystem to improve its response 	<ul style="list-style-type: none"> Confirm how the FMI continuously improve response/plans Confirm how the FMI collaborates with ecosystem (scenario testing) Confirm there is a CSIRT team (internal or outsourced) Confirm how FMI automates its cyber responses where possible
Data integrity	<ul style="list-style-type: none"> Request back-up policy Request results of last test 	<ul style="list-style-type: none"> Risk profile assessment of alternate site What are the transaction recovery mechanisms Confirm reconciliations are in place for all positions with participants/custodians Confirm restoration is done using standard IT configuration 	<ul style="list-style-type: none"> Confirm that back-up and recovery are part of change management and acquisition processes (SDLC...) Request description of redundant system ensuring 0 data loss Ask if data sharing agreements are in place with participants Confirm network segmentation
Communication and collaboration	<ul style="list-style-type: none"> Request list of external connectivity dependencies Request communication plans/procedures covering internal and external stakeholders 	<ul style="list-style-type: none"> Confirm rollback mechanisms/procedures are in place and tested with participants Confirm what cyber incident scenarios are covered by the communication plans 	<ul style="list-style-type: none"> Confirm what mechanisms (alerting tools etc..) are in place to notify senior management and relevant employees /stakeholders in case of incidents
Forensic readiness	<ul style="list-style-type: none"> Request forensic readiness policy Request procedures to retrieve evidence 	<ul style="list-style-type: none"> Confirm forensic plans are integrated with incident management plans 	<ul style="list-style-type: none"> Confirm how the FMI collaborates with ecosystem regarding forensic investigations Confirm that management have a review process in place



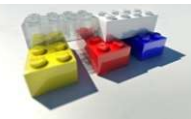
Cyber Resilience Indicators

- **Incident Response**

- *Is there a **policy/procedure and plans** for specific events?*
 - **Advanced cyber attack?**
 - **Massive compromise** of customer data?
 - **Transfer of funds?**
- *Have the **Incident Response Teams** been designated and are they demonstrably ready?*
- *Is there a **Security Operations Centre**?*
 - *How is it staffed?*
 - *How does it work?*
 - *What are the challenges they face?*
- *Are there incidents in the log?*
- *There must be additions / corrections to the process based on lessons learned*
- *Forensic and incident response capabilities internal or outsourced should exist and be able to respond timely*

- **Crisis management**

- *Is there a dedicated **CRISIS Management** team setup?*
- *Do they consist of adequate seniority level employees and span the appropriate business areas?*
- *Are they adequately trained?*
- *Have they been involved/active in the near past?*



Cyber Resilience Indicators

- **Recovery**
 - Have the **critical operations** and systems been identified?
 - What **scenarios** have been tested?
 - How often are they **tested**?
 - Has **Ecosystem Recovery** been addressed? Is there a dialogue with the Ecosystem?
 - Where do new **scenarios** come from?
 - Do the results of the **testing** improve over time?
 - Are the scenarios indicative of plausible but serious cyberattacks? Has **data integrity** scenarios being considered?
 - Can the FMIs deal with a **largely compromised IT infrastructure**?

Brainstorming question: Response and Recovery

You have asked your FMI how they manage response and recovery in the context of cyber resilience. They have said: “we have two mirrored sites, 300km apart, and all systems are available at both sites and there is synchronous data mirroring”. What would your concerns be?

You have asked your FMI for their cyber incident management plan. They have responded by saying that they have a business continuity plan, this is sufficient and they guarantee that they can recover in 2 hours with full data integrity. What are your concerns?

Why test?

What is the purpose of testing?

To understand how effective the controls on security are (not only the protective but also detection and response/recovery)

Testing principles

- Many types of test ranging from specific test of services to organisationally holistic tests.
- One test does not substitute another, there is a **time and a place** for all tests.
- **Scope** and **methodology** of the test are critical.
- How an organisation **prioritises** and **conducts remediation** of test findings is indicative of information security/ cyber security maturity.

Vulnerability Assessment

- Comprehensive activity to identify **weaknesses** on web applications, systems, and networks, that could be exploited by attackers
- Done systematically and routinely, mostly done via **automated tools** on a recurring basis
- Producing **reports** that can support the introduction of further controls/ security measures → useful to check **reports** from the **past years**
- **Criticality/ Severity** is important, but more important is the big picture of vulnerabilities and weaknesses within the IT environment.
- **Cascading effect, chaining** of vulnerabilities. A cyber attack will use multiple vulnerabilities and security weaknesses during an attack.
- Link **Vulnerability** to **Patch** management. Vulnerability management **policy** and a procedure covering all aspects from detection of the vulnerability up to its remediation
- **Register** and have **ownership** of the vulnerabilities. Vulnerability tracking is an ongoing process.

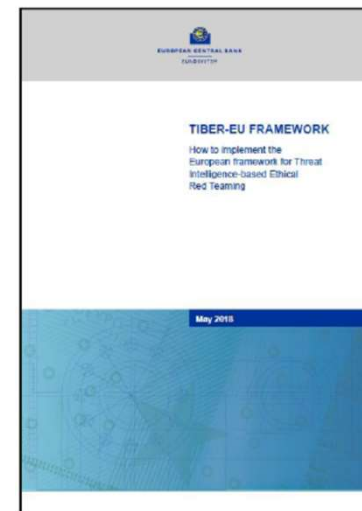
Penetration test

- Set of procedures and tools designed to **test** and **bypass** the **security controls** of a system → it is an **attempt** to defeat **systems and applications security** using the **same methods** attackers would **adopt**
- Relevant to **determine** the **effectiveness** of the **controls**, of the **patches** and of the **security measures** within an organization
- **Penetration test** is:
 - a process which should become a **routine** and be repeated to give real added value
 - a **snapshot** in time, as more vulnerabilities may be released and identified after the assessment
 - **indicative** and does not cover all vulnerabilities exhaustively
 - like any project → **responsibilities** and **tasks** of the team involved should be clearly assigned
 - live systems should be tested
- Time, human resources and **costs** could be an important limitation, as hackers may allocate more time and people if they target a specific company

Red Teaming exercise – example on a Financial Institution

***Definition:** “A simulated adversarial attempt to compromise the security of an entity by mimicking the tactics, techniques and procedures of real-life adversaries, based on reliable and bespoke threat intelligence, and looks to target the people, processes and technologies of an entity, with its minimal foreknowledge” (source: G7FE-TLPT)*

Compared to a **penetration test**, **Red Teaming** exercises have a **broader** scope and a **higher** level of **sophistication**, assessing the **full scenario** of a targeted **attack** against an **entire entity**

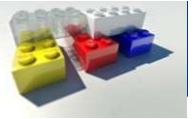


TIBER-EU framework approved by the Governing Council in April 2018 and published on the ECB website on 2 May 2018



Testing in an FMI

- Key aspects: **scope, limits, scenarios, results, remediation** – clearly defined
- Testing has **risks** on its own and must be **accepted, controlled** and **monitored**.
- Adds a constant **overhead** to IT Operations to support the effort , be ready to handle an incident and remediate.
- Tests **highlight issues** in the security configuration, **lack of security** updates of network devices and servers/clients as well as insecurely built applications.
- The findings need to be resolved which usually means to test and then deploy **security updates** or **changes to software**.
- Senior Management should be aware of the **risks/ impacts** involved in **executing a test** before giving the authorization and also receive **high level results**.
- The **teams** performing **security tests** should be independent of **IT/ IT Security operations**.
- Testers should be **adequate** and **competent**



Testing in an FMI

- **Vulnerability Scanning**
 - Automated
 - Almost no overhead
- **Penetration Testing**
 - Automated and Manual. Should be mostly 80% plus manual
 - Scope internal/external, hybrid and further scenarios
- **Web Penetration Testing**
 - Automated and Manual. Only against web servers/web applications (including mobile)
- **Other types of testing**
 - Phishing, social engineering test
 - Red teaming
 - Client side/endpoint/mobile security assessment
 - Compromise assessment



Cyber Resilience Indicators

- **Competencies of testers:** *Are they checked? Do they have experience in the specific test? Do they abide by code of ethics? Are they independent?*
- **Use of external testers** *to validate tests of internal testers and/or to conduct specific tests.*
- **Frequency of tests** *for vulnerability scanning, penetration testing, web penetration testing, red teaming and other testing. Is there a testing programme? On what basis has frequency been derived?*
- **Diversity of testing** *and evolution from year to year. Is there any clear evolution in the capability, type and scope of tests?*
- **Priority of testing and reporting:** *Are results presented to Senior Management/Board level? Do they monitor the remediation and ongoing testing activities?*



Cyber Resilience Indicators

- **Improvement on results per testing cycle:** *Are the number of unpatched/end of life systems decreasing? Is the number of known vulnerabilities decreasing?*
- **Time between test results and the fixing of security findings,** *especially critical and high severity findings.*
- **Patching processes,** *with specified timeframes, ownership and authorisation must exist and be followed.*
- **Allowance for emergency patching** *must be in place for high severity, criticality vulnerabilities.*

Testing in CROE

- In **Testing**, all elements of the cyber resilience framework should be rigorously tested to determine their overall effectiveness before being deployed within an FMI, and regularly thereafter. Sound testing regimes should produce findings that are used to identify gaps in stated resilience objectives and provide credible and meaningful inputs to the FMI's cyber risk management process.
- In this chapter, ***Evolving, Advancing and Innovating*** expectations focus on four types of testing:
 - Vulnerability assessments (**integrated in the VM process**);
 - Scenario-based testing;
 - Penetration testing; and
 - Red team testing.
- To facilitate red team testing, the ECB has developed TIBER-EU, which provides FMIs and other financial institutions with the framework to conduct intelligence-led red team testing. TIBER-EU complements the CROE and is part of the wider Eurosystem cyber strategy.

Testing

- In ***Evolving***, focus is on establishing and maintaining a comprehensive testing programme as an integral part of the FMI's cyber resilience framework. The testing programme should include methodologies, practices and tools **for monitoring, assessing and evaluating the effectiveness of the core components of the cyber resilience framework**. The testing programme should build on a risk-based approach and maintained taking in inputs the cyber threat landscape, criticality of information assets and meeting the needs of the relevant stakeholders. In ***Evolving***, expectations concern the following testing practices: **Vulnerability assessment (scanning/identification, prioritization, patching), Scenario-based testing; Penetration testing**
- In ***Advancing***, focus is on the **integration** of the security assessment and testing practices with the Enterprise Risk Management and the System Development Life Cycle at any company level (business, application and technology) and for the entire service portfolio (including mobile applications). In Advancing, the security testing should be supported by **automation** in order to extend the deepness and the breathiness of the testing programme as well as the execution of an increasing number of tests (frequency). **In Advancing, FMI should conduct both internal and independent red team exercises utilising regulatory or industry TLPT frameworks.**
- In ***Innovating***, focus is on the FMI ability to measure the effectiveness of its testing programme; Security tests are conducting in collaboration with relevant stakeholders (peers, participants and third parties). FMI has the capability to test regularly its cooperation, communication and coordination arrangements with external stakeholders and consider to share test conclusions with counterparties to improve cyber resilience of the FMI itself and its ecosystem as well.

Testing questions

- Testing process and programme
 - Is there a comprehensive security assessment and testing programme approved at the appropriate level?
 - Is there a formal process for monitoring, reviewing and regularly updating the programme?
 - Are security assessments and tests conducted on critical organizational assets (e.g., assets important to business objectives and the organization's risk strategy)?
 - Are plans, processes and policies updated based on lessons learned from tests (e.g., business continuity, disaster recovery, incident response)?
 - How is the effectiveness of the testing programme measured (KPI, KRI)?

- Vulnerability assessment
 - Is a vulnerability management plan developed and implemented?
 - What is the frequency and coverage of vulnerability assessments?
 - Is the vulnerability assessment process regularly reviewed, updated and integrated with other relevant operational processes (e.g. Vulnerability and Patching Management, Change management, etc)?
 - Is a specific programme/campaign to support the timely identification and remediation of vulnerabilities and weaknesses (e.g. Bug Bounty programme) in place?

Testing questions

- Scenario-based testing
 - Is there a formalised enterprise methodology for conducting scenario-based tests?
 - Are a broad array of cyber incident scenarios included?
 - Are incident response and recovery plans (including back-up, DR and BC plans) regularly tested?
 - Are Board and Senior management engaged?
 - Are ecosystem implications and collaboration with external stakeholders tested?
- Penetration testing
 - Is Pen Testing conducted on the basis of a formalised enterprise methodology, informed by the most common internationally recognized practices (e.g. OWASP, NIST SP 800-53A, 115, PCI-DSS, OSSTMM, ...)?
 - Which information assets are subject to Pen Testing and on what criteria?
 - Are realistic TTPs of potential adversaries simulated?
 - How are Pen Testing results incorporated as lessons learned to fix discovered vulnerabilities and weaknesses?
 - To what extent is Pen Testing externalised to Security Service Providers?
- Red team testing
 - To what extent are critical functions subject to red team exercises?
 - To what extent are there internal capabilities to conduct red teaming testing?
 - To what extent are red team tests conducted in line with common regulatory and industry frameworks (e.g. TIBER-XX)?

Assessment actions for overseers

	For Evolving level, request/ask	For Advancing level, request/ask in addition	For Innovating level, request/ask in addition
Testing programme	<ul style="list-style-type: none"> Security Testing Programme Testing process to update, review and execute the testing programme Most relevant testing exercise reports and action plans 	<ul style="list-style-type: none"> Evidence that testing results are incorporated in the ERM Evidence of the automation of the testing process Interactions with other relevant business and operational processes (e.g. vulnerability and patch management; change management; configuration management; ...) 	<ul style="list-style-type: none"> Metrics of the testing programme Engagement with peers, participants and third parties Cooperation and coordination arrangements with relevant internal and external stakeholders Communication plans
Vulnerability assessment	<ul style="list-style-type: none"> Vulnerability management plan FMI's risk assessment to ensure that vulnerabilities identified during the vulnerability management process are included. 	<ul style="list-style-type: none"> Frequency and coverage of vulnerability scanning 	<ul style="list-style-type: none"> Range of effective practices and tools to support VA process (e.g. Bug Bounty programme)
Scenario-based testing	<ul style="list-style-type: none"> Type of exercises and variety of covered scenarios Evidence of Board and Senior management engagement 	<ul style="list-style-type: none"> Cyber-attack scenarios cover CIA security objectives Business implications are considered (e.g. significant financial loss, brand reputation, financial spillovers, ...) 	<ul style="list-style-type: none"> FMI's ecosystem testing scenarios
Penetration testing	<ul style="list-style-type: none"> Frequency and coverage of penetration testing Interaction with other operational processes (e.g. Change Management) Stakeholder engagement (BC, SOC, CSIRT) 	<ul style="list-style-type: none"> Realistic TTPs are simulated for different tested components (networks, applications, ...) 	
Red team testing		<ul style="list-style-type: none"> Critical functions subjected to RT tests Methodology, practices and capabilities in place to conduct RT tests Reference Frameworks (e.g. TIBER-EU) 	<ul style="list-style-type: none"> Internal capabilities in terms of specialized team (Red Team), skills, competences and tools

Brainstorming question: Testing

You have reviewed two test reports of the FMI in the last six months and noted the same critical vulnerabilities being found in both. What are your concerns and what would ask the FMI?

Your FMI conducts regular vulnerability scanning and targeted penetration testing when there is a new software being introduced into the systems. Is this sufficient?

Situational Awareness

- In **Situational Awareness**, an FMI should understand the cyber threat environment within which it operates, and the implications of being in that environment for its business and the adequacy of its cyber risk mitigation measures. Strong situational awareness can be acquired through an effective cyber threat intelligence process and active participation in information-sharing arrangements and collaboration with trusted stakeholders within and outside the industry.
- In this chapter, ***Evolving, Advancing and Innovating*** expectations focus on:
 - Cyber Threat Intelligence; and
 - Information sharing.
- This chapter places a lot of focus on the FMI's interaction with the wider ecosystem to enhance threat intelligence and information sharing, and how the Board is well informed about the threat landscape that the FMI is exposed to.

Situational Awareness: Cyber Threat Intelligence

Evolving

- Step 1: **Identify** cyber threats
- Step 2: **Gather** cyber threat information from internal and external sources (e.g. application, system and network logs; security products such as firewalls and IDSs; trusted threat intelligence providers; and publicly available information) and belong or subscribe to a threat and vulnerability information-sharing source and/or ISAC that provides information on cyber threats and vulnerabilities. Cyber threat information gathered by the FMI should include analysis of tactics, techniques and procedures (TTPs) of real-life attackers, their modus operandi and information on geopolitical developments that may trigger cyber attacks on any entity within the FMI's ecosystem.
- Step 3: Have the capabilities to **analyse** the cyber threat information gathered from different sources, while taking into account the business and technical characteristics of the FMI, in order to: (a) determine the motivation and capabilities of threat actors (including their TTPs) and the extent to which the FMI is at risk of a targeted attack from them; (b) assess the risk of technical vulnerabilities in operating systems, applications and other software, which could be exploited to perform attacks on the FMI; (c) analyse cybersecurity incidents experienced by other organisations (where available), including types of incident and origin of attacks, target of attacks, preceding threat events and frequency of occurrence, and determine the potential risk these pose to the FMI.
- Step 4: **Produce** relevant cyber threat intelligence, and continuously use it to assess and manage security threats and vulnerabilities – review and update the cyber threat intelligence regularly.
- Step 5: **Disseminate** the cyber threat intelligence to appropriate staff who are responsible for mitigating cyber risks at the strategic, tactical and operational levels within the FMI.
- Step 6: **Incorporate** lessons learned from analysis of the cyber threat information into the employee training and awareness programmes.

Advancing

- Step 7: Use cyber threat intelligence to **anticipate**, as much as possible, a cyber attacker's capabilities, intentions and modus operandi, and subsequently possible future attacks.
- Step 8: **Develop a cyber threat risk dashboard** (incl the most likely threat actors for the FMI, the TTPs that may be used by such threat actors, likely vulnerabilities that may be exploited by such threat actors, likelihood of attack from such threat actors and the impact on the confidentiality, integrity and availability, impact of attacks already conducted by such threat actors on the ecosystem and risk mitigation measures in place to manage a potential attack.
- Step 9: **Continuously review and update** dashboard in the light of new threats and vulnerabilities and discuss at Board and senior management.

Situational Awareness: Information Sharing

Evolving

- Step 1: Define **goals and objectives** of information sharing - at the very least, collecting and exchanging information could facilitate the detection, response, resumption and recovery during and following a cyber attack.
- Step 2: Define **scope of information-sharing** by identifying the types of information available to be shared, the circumstances under which sharing this information is permitted, those with whom the information can and should be shared and how information will be acted upon.
- Step 3: Establish and regularly review the information-sharing **rules and agreements**.
- Step 4: Establish trusted and safe **channels of communication** for exchanging information.
- Step 5: Establish process to **access and share** information with external stakeholders in a timely manner (e.g. regulators, law enforcement or other organisations within the FMI's ecosystem).

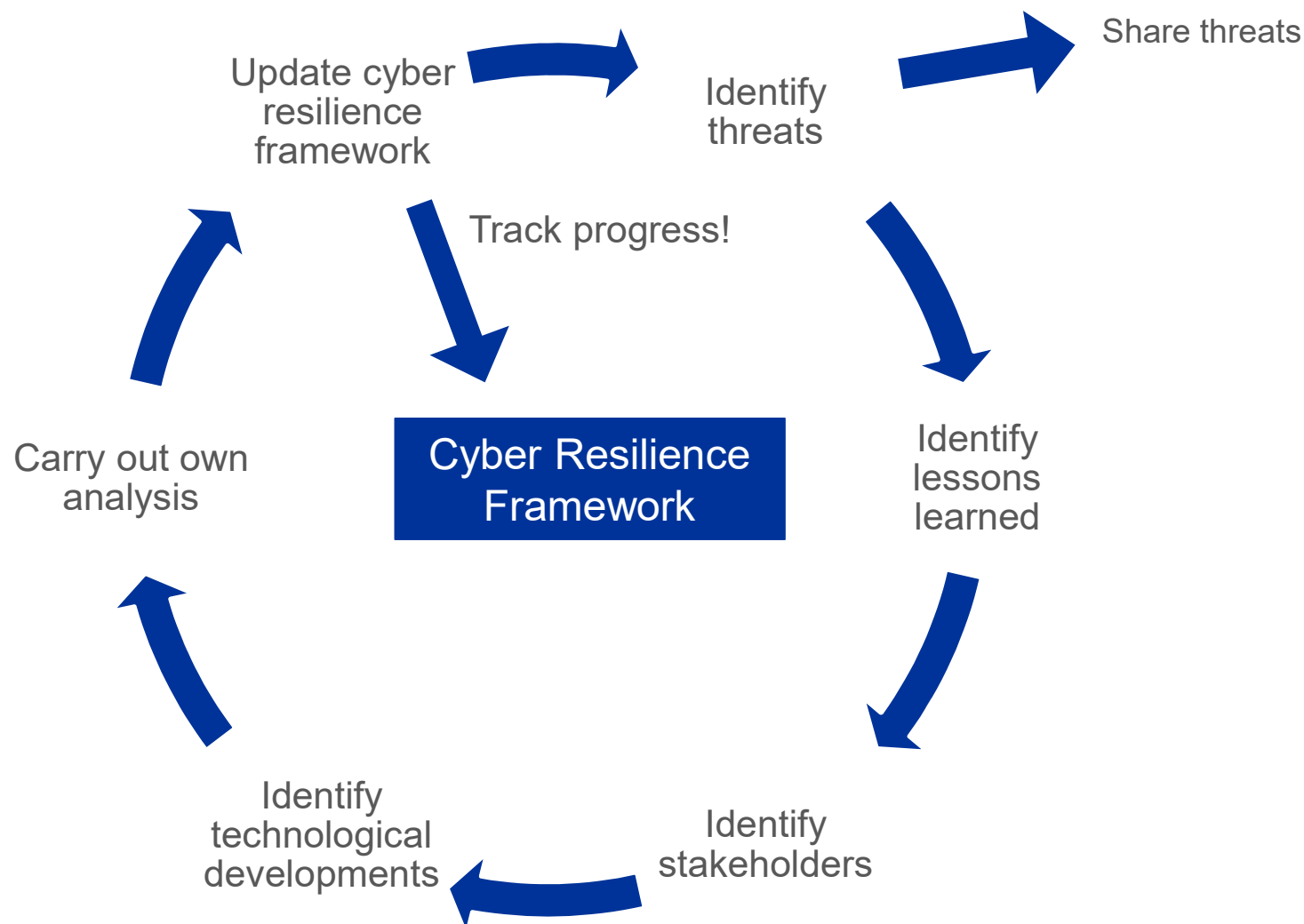
Advancing

- Participate actively in existing **information-sharing groups and facilities**, including cross-industry, cross-government and cross-border groups to gather, distribute and assess information about cyber practices, cyber threats and early warning indicators relating to cyber threats.
- **Share information with relevant stakeholders** in the ecosystem to achieve broader cyber resilience situational awareness, including promoting an understanding of each other's approach to achieving cyber resilience.

Learning and Evolving

- In **Learning and Evolving**, an FMI needs to achieve continuous cyber resilience amid a changing threat environment. To be effective in keeping pace with the rapid evolution of cyber threats, an FMI should implement an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks and allows the FMI to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems.
- In ***Evolving***, the focus is on distilling and classifying the lessons learned (e.g. strategic, tactical and operational), identifying the key stakeholders to whom these apply, incorporating them to improve the FMI's cyber resilience framework and capabilities, and conveying them to each relevant stakeholder on an ongoing basis.
- In ***Advancing***, the focus is on the FMI continuously tracking its progress in developing its cyber resilience capabilities from a current state to a defined future state.
- In ***Innovating***, the FMI should have capabilities in place to use multiple sources of intelligence, cyber events, etc across other sectors and geopolitical events to better understand the evolving threat landscape and proactively take the appropriate measures to improve its cyber resilience capabilities.

A continuous cycle of improvement



Training and awareness

In order to constantly improve training and awareness, FMIs should:

- Include **real life events** in training and awareness
- **Validate** the effectiveness of training
- Make training available **during visible cyber event**
- Use their experiences to continuously **improve training and awareness** campaigns

Brainstorming question: Situational Awareness and Learning & Evolving

Your FMI has just heard rumours of an attack that took place on another FMI that operates a similar business. What would you expect the FMI to do? As an overseer, what are the questions you would ask?



Annex: Reference Frameworks

International standard and frameworks relevant for cybersecurity

COBIT 5 (ISACA, 2012)

NIST CSF 1.1 (NIST, 2018)

Other related standards and cross-references

- ISO/IEC 27000 (Information security)
- ISO/IEC 31000 (Risk management)
- ISO/IEC 22300 (Business continuity)
- ...

Reference Frameworks

NIST Cyber Security Framework 1.1 (2018)

- The Framework provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes
- V 1.1 of CSF refines, clarifies, and enhances Version 1.0 issued in February 2014

Core structure:

5 Function

(es. ID - Identify)

23 Category V1.1

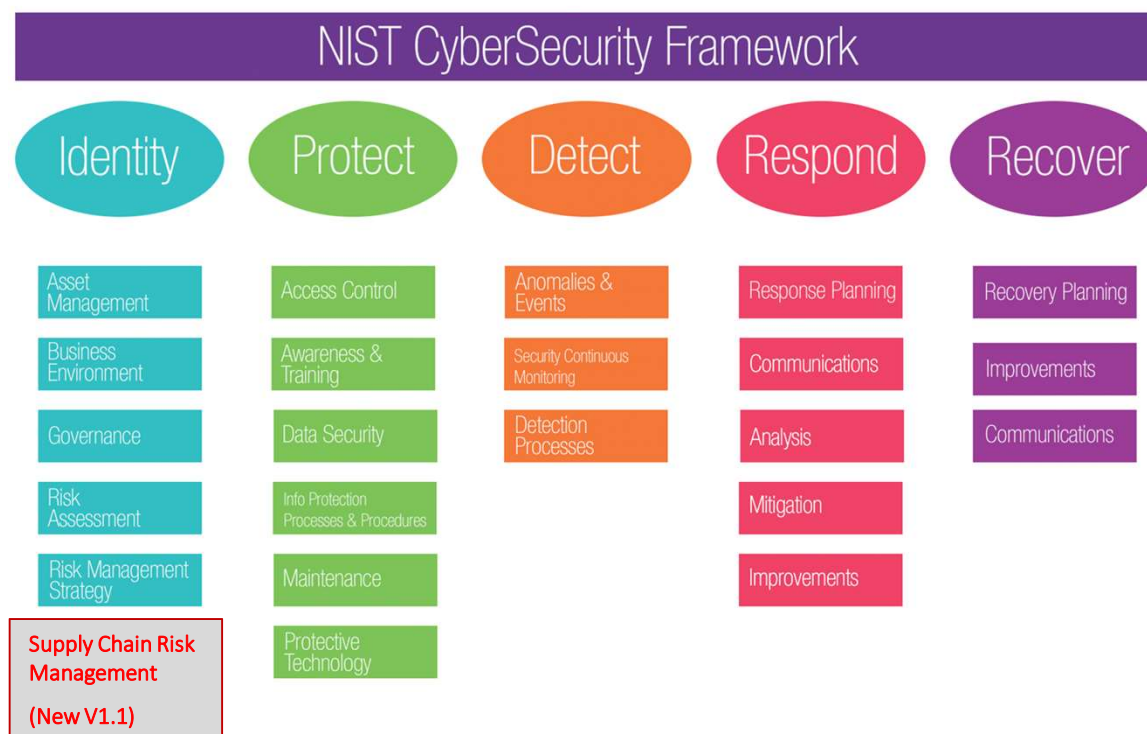
(es. ID-AM Asset Management)

106 Subcategory V1.1

(es. ID-AM-1 Physical devices and systems within the organization are inventoried)

Informative References

(**Cobit5**, CSC, NIST SP 800-53 Rev. 4, ISO/IEC 27001:2013, ecc.)



NIST CSF - TAXONOMY

The framework is divided into three parts, "Core", "Profile" and "Tiers"



- The "Framework Core" contains an **array of activities**, outcomes and references about aspects and approaches to cyber security

TIERS (4 levels and 3 categories)

- The "Framework Implementation Tiers" are used by an organization to **clarify for itself and its partners how it views cybersecurity risk** and the degree of sophistication of its management approach

PROFILE

- A "Framework Profile" is a **list of outcomes** that an organization has chosen from the categories and subcategories, based on its needs and risk assessments
- An organization typically starts by using the framework to develop a **"Current Profile"** which describes its cybersecurity activities and what outcomes it is achieving. It can then develop a **"Target Profile"**, or adopt a baseline profile tailored to its sector (e.g. Banks, FMs) or type of organization. It can then define steps switch from its current profile to its target profile (**roadmap**)

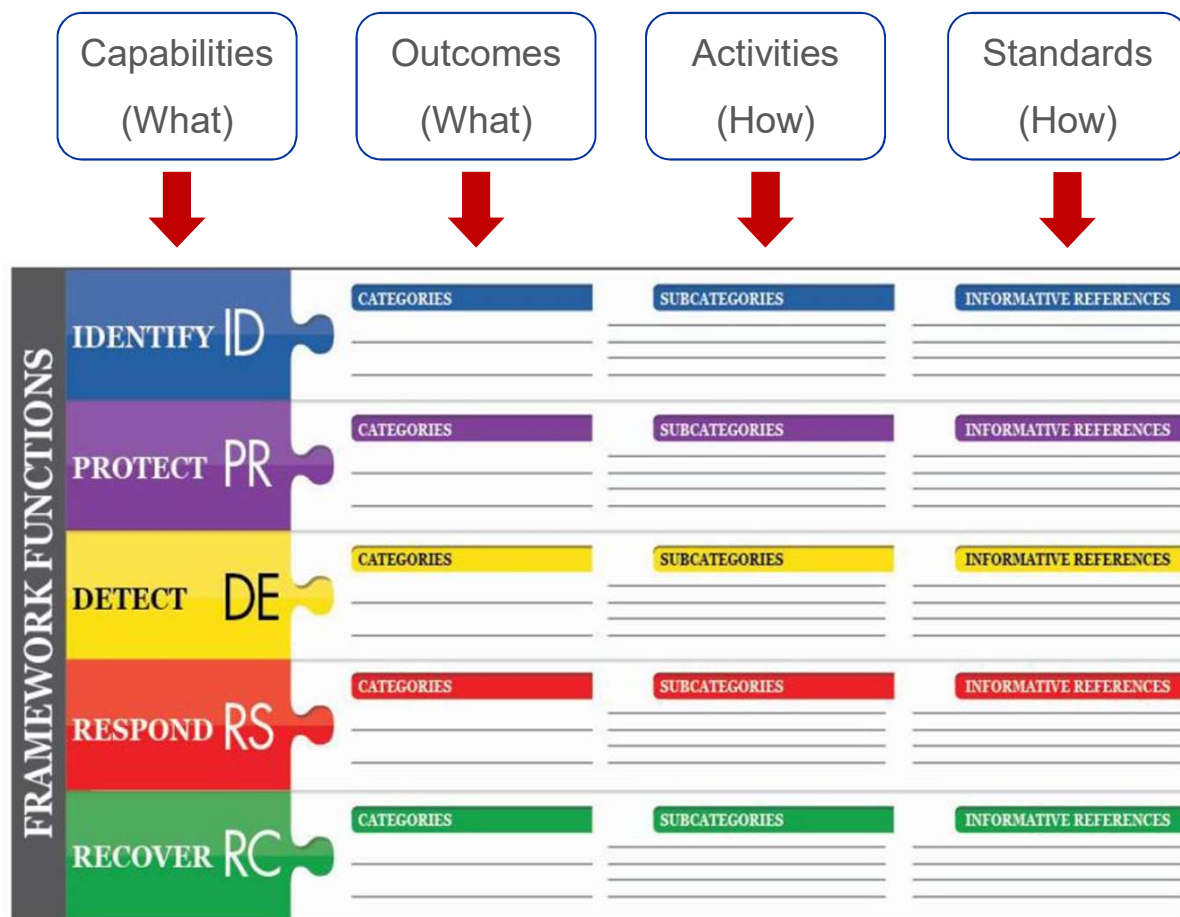
NIST Cyber Security Framework - CORE

Functions: provide a high-level, strategic view of the **lifecycle of an organization's management of cybersecurity risk**

Categories: provide a **group of cybersecurity outcomes** tied to programmatic needs and particular activities

Subcategories: provides a **specific activity or result** mapped to a reference that helps support achievement of higher level outcomes Informative

References: provides specific sections of standards, guidelines, and practices **common** among critical infrastructure sectors that illustrate a method to achieve an associated outcome



NIST Cyber Security Framework - Functions

ID - Identify

- Develop an organizational **understanding** to manage cybersecurity risk to **systems, people, assets**, data, and capabilities.
- The activities in the Identify Function are foundational for effective use of the Framework.
- **Understanding the business context, the resources that support critical functions**, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

PR - Protect

- Develop and implement **appropriate safeguards** to ensure delivery of critical services.
- The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

DE - Detect

- Develop and implement **appropriate activities to identify the occurrence of a cybersecurity event**.
- The Detect Function enables **timely discovery of cybersecurity events**.

RS - Respond

- Develop and implement appropriate activities to take action regarding a **detected cybersecurity incident**.
- The Respond Function supports the ability to **contain the impact of a potential cybersecurity incident**.

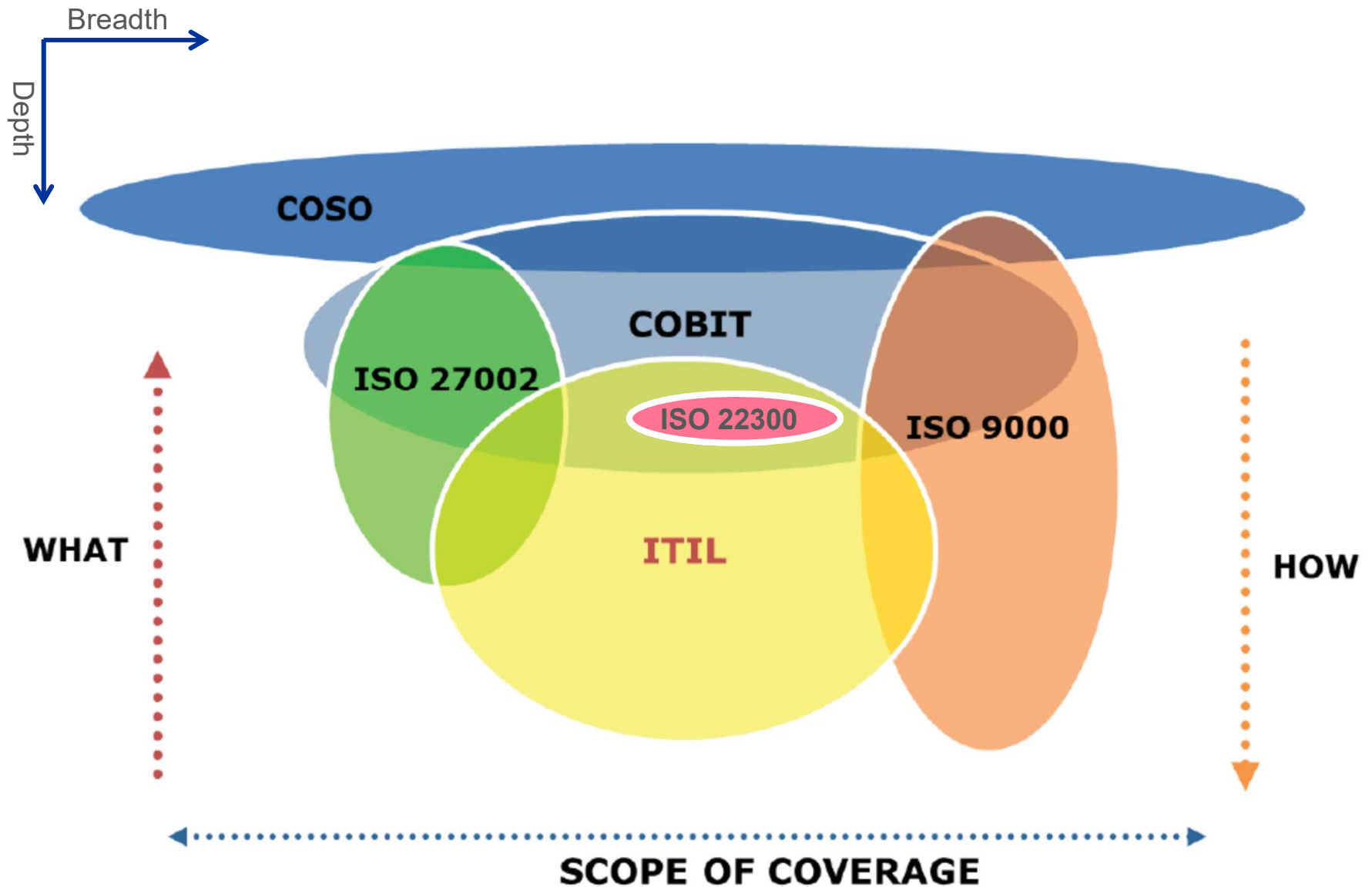
RC - Recover

- Develop and implement **appropriate activities to maintain plans for resilience and to restore any capabilities or services** that were impaired due to a cybersecurity incident.
- The Recover Function supports **timely recovery to normal operations** to reduce the impact from a cybersecurity incident

Standard ISO/IEC 2700x

- **ISO/IEC 27000 family of standards helps organizations keep information assets secure**
 - Using this family of standards will help the organization to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.
- **ISO/IEC 27001:2013 (what to do in terms of requirements, objectives and controls)**
 - It is the internationally recognized **standard for an information security management system**. It gives a great foundation framework to address information security risks with appropriate measures and controls.
 - It is an ideal starting point for any organization that needs to manage and respond to information threats and build resilience.
- **ISO/IEC 27002:2013 (how to do)**
 - Provides guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls (Annex A ISO/IEC 27001) taking into consideration the organization's information security risk environment(s)

COBIT5 compared to other frameworks and standards



NIST CSF – Cross-references example

Asset Management (ID.AM):

The data, personnel, devices, systems, and facilities that enable organization to achieve business purposes are identified and managed consistently with their relative importance to business objectives and the organization's risk strategy.

ID.AM-1: Physical devices and systems within the organization are inventoried	<ul style="list-style-type: none"> • CCS CSC 1 • COBIT 5 BAI09.01, BAO09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev.4 CM-8
ID.AM-2: Software platforms and application within the organization are inventoried	<ul style="list-style-type: none"> • CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev.4 CM-8
ID.AM-3: Organizational communication and data flows are mapped	<ul style="list-style-type: none"> • CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
ID.AM-4: External information systems are catalogued	<ul style="list-style-type: none"> • COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9
ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	<ul style="list-style-type: none"> • COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g. suppliers, customers, partners) are established	<ul style="list-style-type: none"> • COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

BAI09.01

P: Manage Assets

MP: Identify and record current assets

BAI09.02

P: Manage Assets

MP: Manage critical assets

A.13 Information security incident management (Requirement)

A.13.2 Management of information security incidents and improvements (Objective)

A.13.2.1 Responsibilities and procedures (Control)

Cobit 5

What is it and why is it important?

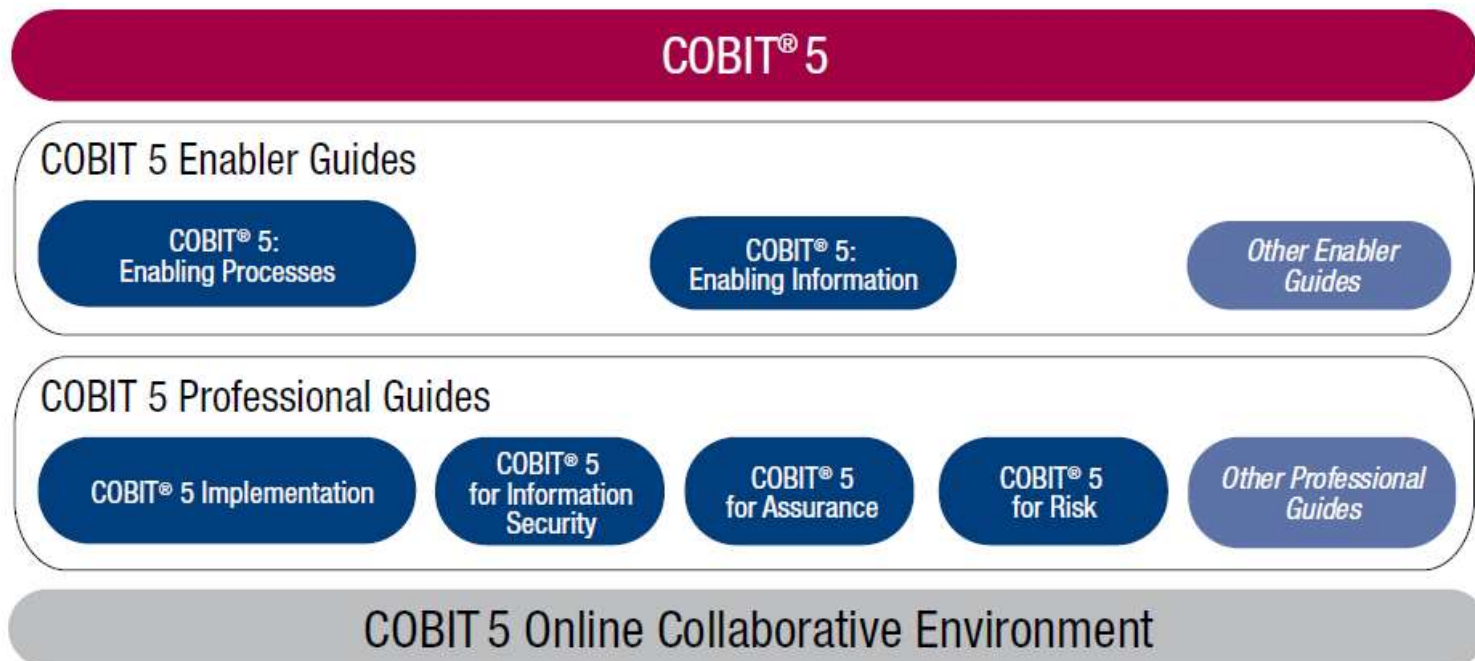
- It is a **business leading and comprehensive framework for the governance and management of the Enterprise IT**
- It helps enterprises to **meet many stakeholders' needs** (operations, audit, compliance, decision making, ...)



- It consists of **guides and tools** that assist enterprises to **create value from their IT environment** by maintaining the right balance among **benefits realization, resources optimization and risks mitigation**

Cobit 5

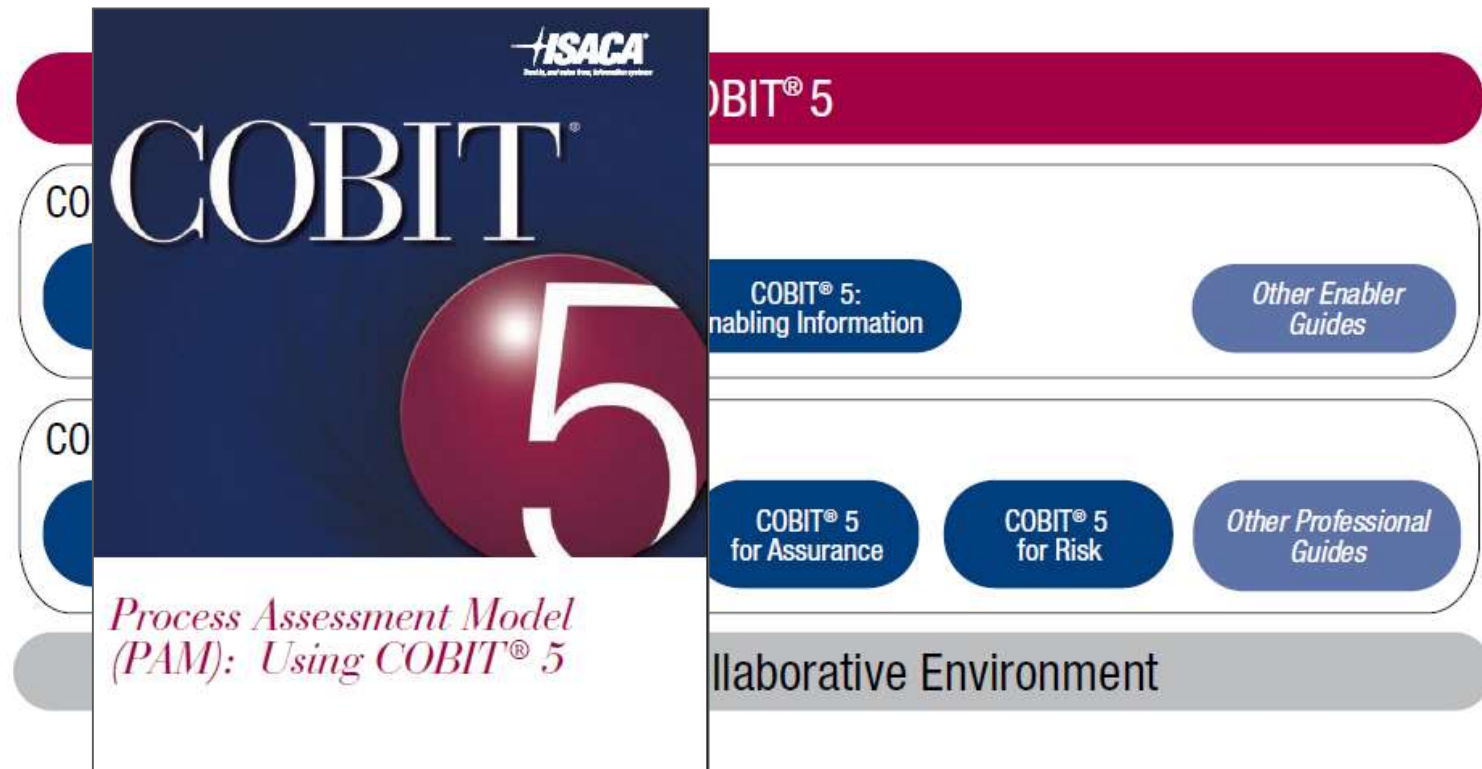
Key documents: the framework, enabler guides, professional guides



- Implemented in a gradual or holistic manner
- Useful for enterprises of all sizes: commercial, not-for-profit, public
- Distinction between Governance and Management

Cobit 5

Key documents: the framework, enabler guides, professional guides

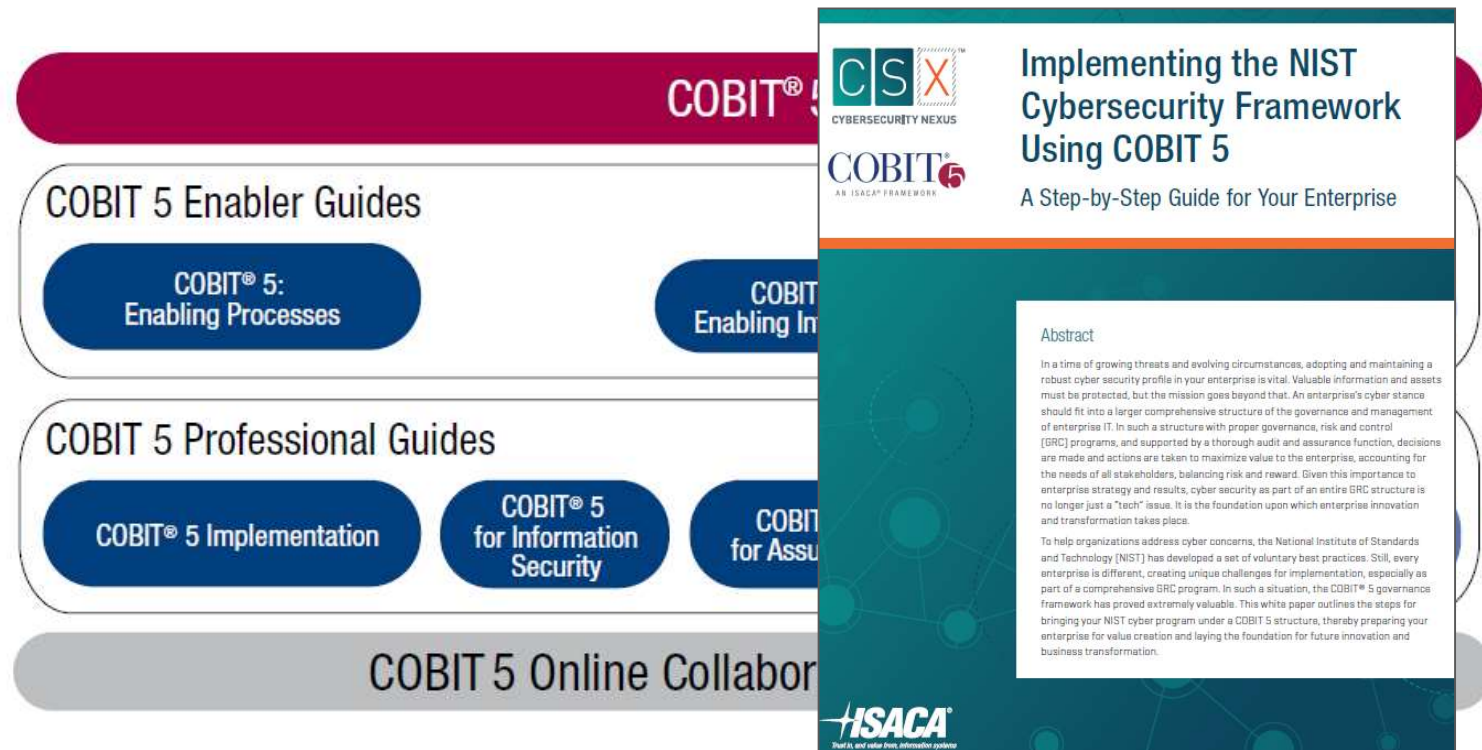


- Implemented in a gradual or holistic manner
- Useful for enterprises of all sizes: commercial, not-for-profit, public
- Distinction between Governance and Management

Reference Frameworks

Cobit 5

Key documents: the framework, enabler guides, professional guides

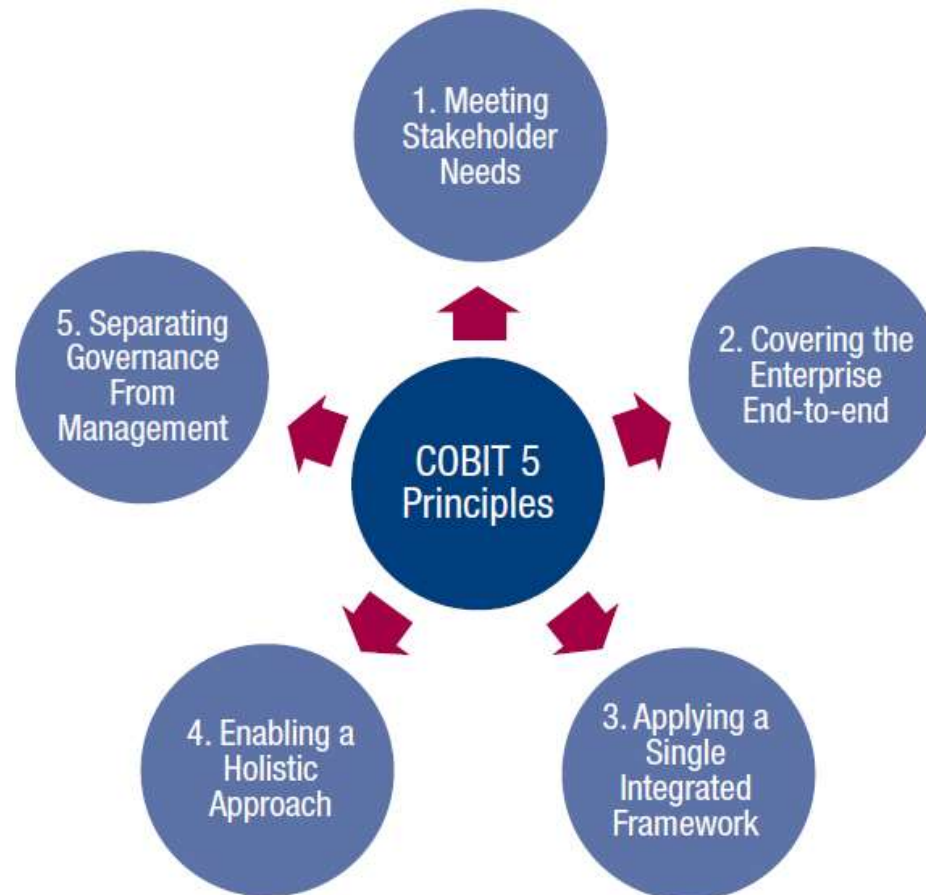


- Implemented in a gradual or holistic manner
- Useful for enterprises of all sizes: commercial, not-for-profit, public
- Distinction between Governance and Management

Source: ISACA® (<http://www.isaca.org/COBIT/Pages/default.aspx>)

Cobit 5

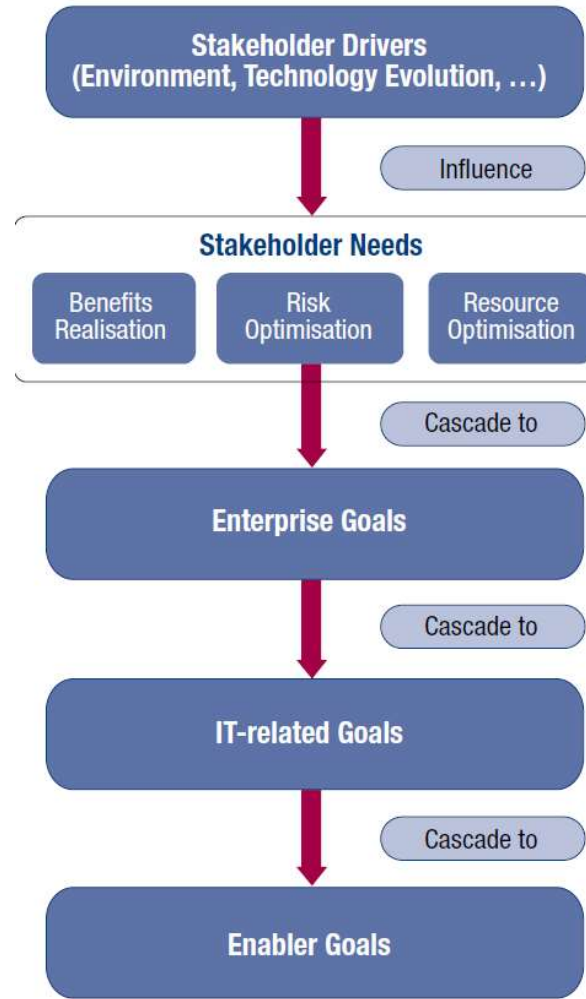
Key concepts: **principles**, goals cascade, enablers



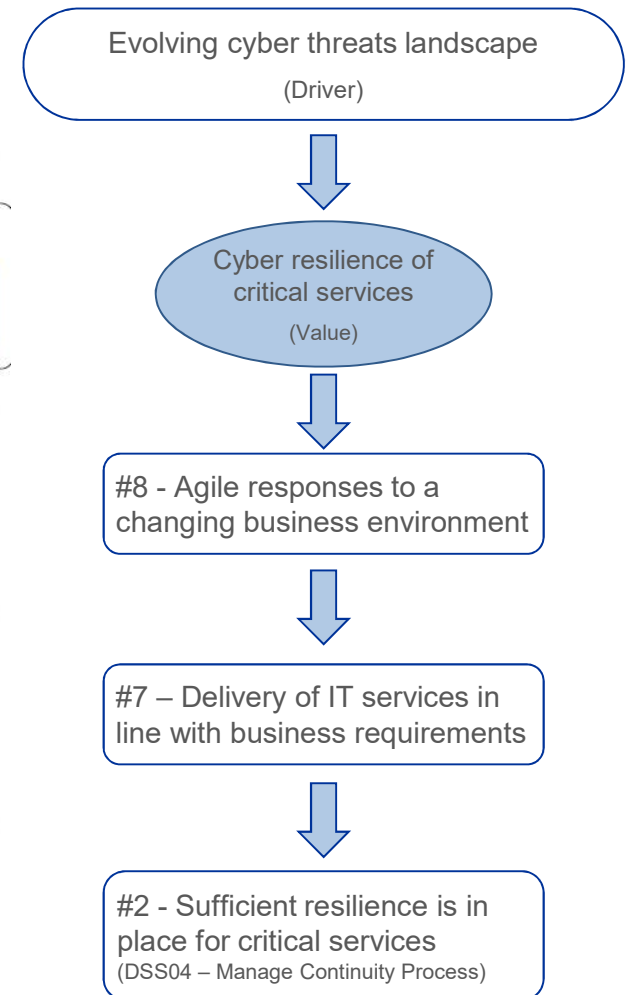
Cobit 5

Key concepts: principles, goals cascade, enablers

The **Goals Cascade** translates stakeholder needs into specific, actionable and customized enterprise goals, IT-related goals and enabler goals.



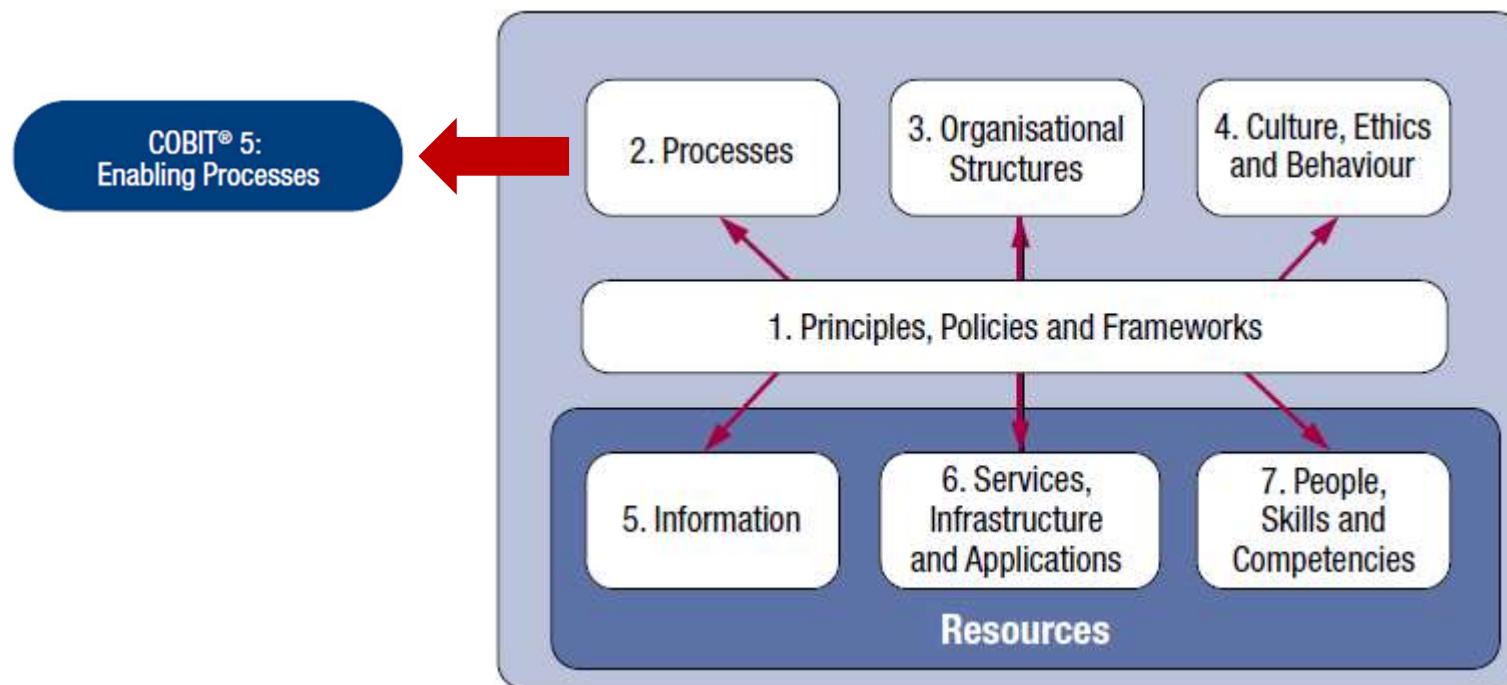
... an example



Cobit 5

Key concepts: principles, goals cascade, **enablers**

- The COBIT 5 framework describes **seven categories of enablers** as factors that, individually and collectively, influence the governance and management over enterprise IT
- **Enablers are driven by the goals cascade**, i.e., higher-level IT-related goals define what the different enablers should achieve

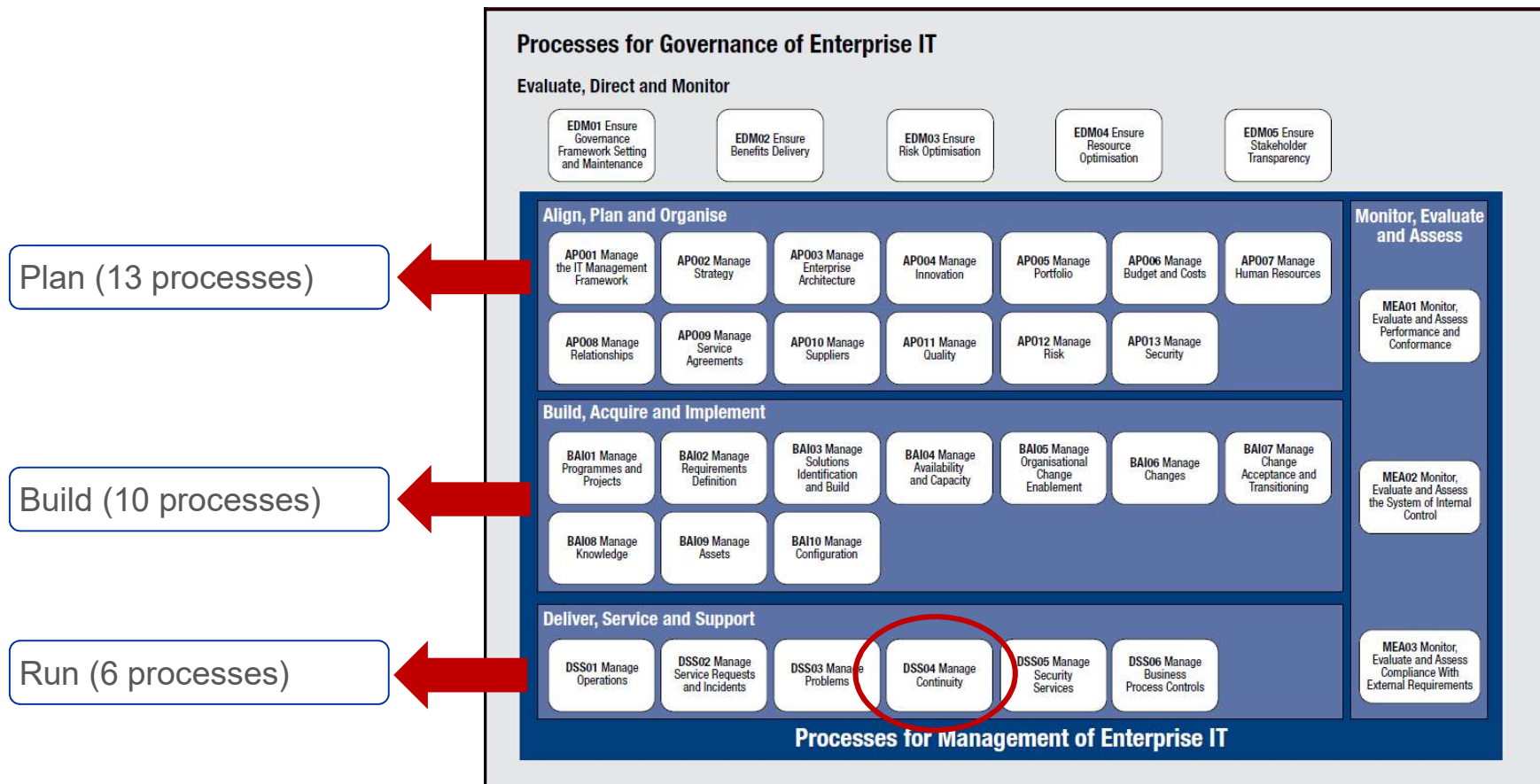


Reference Frameworks

Cobit 5

The Process reference model

PRM represents all of the processes (37) normally found in an enterprise relating to IT activities, offering a common reference model, understandable to operational IT and business managers



Cross-references in COBIT 5

Enterprise IT Governance and Management

