

IT Risk Regulation and Supervision



Information Technology Audit
and Cyber Risk Supervision Department



Why is the IT risk mitigation important?

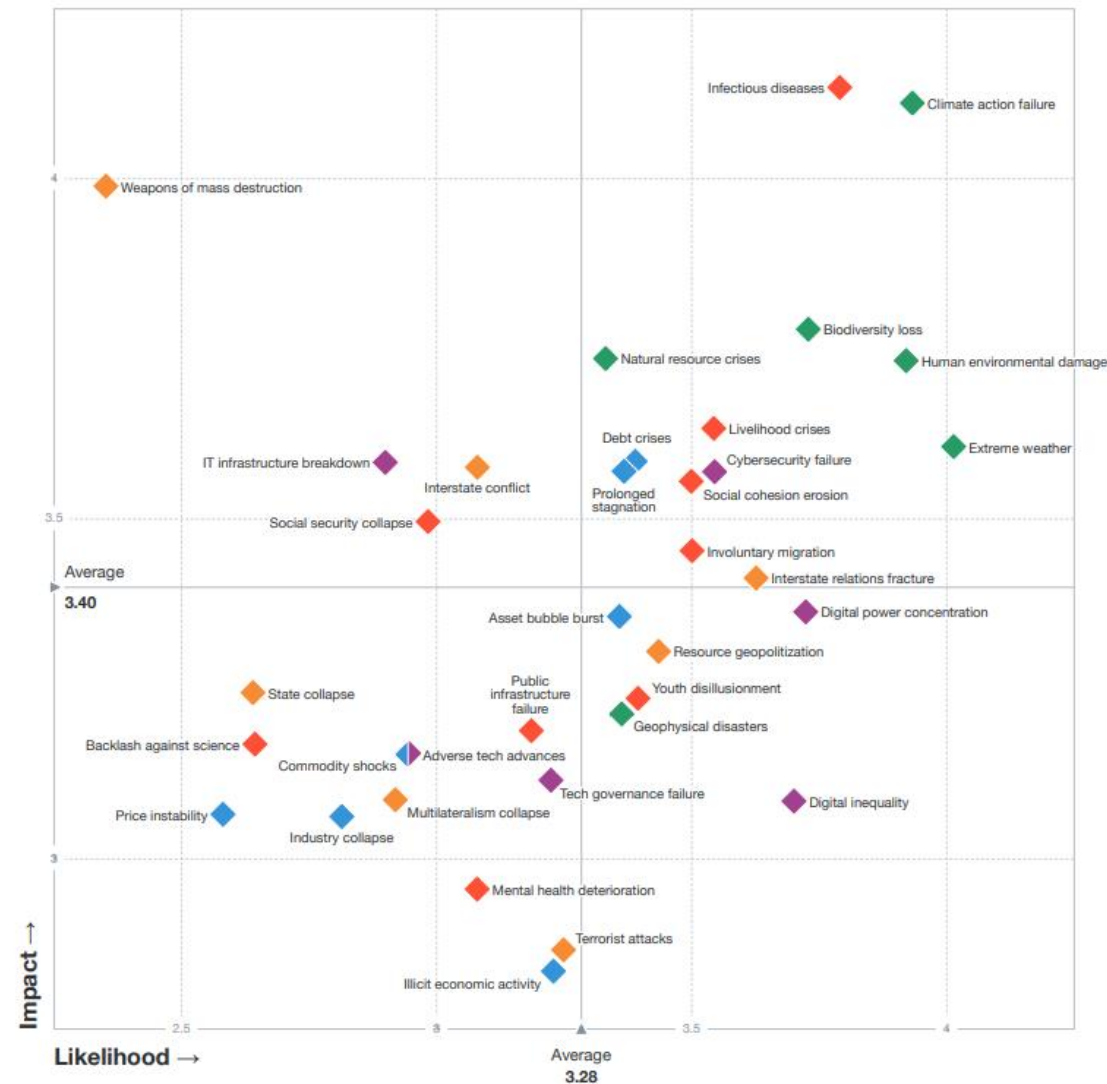
Global Risks Perception Survey 2021 Results (Source : World Economic Forum)

Top 10 risks in terms of Likelihood

- 1 Extreme weather
- 2 Climate action failure
- 3 Human environmental damage
- 4 Infectious diseases
- 5 Biodiversity Loss
- 6 Digital power concentration
- 7 Digital inequality
- 8 Interstate relations fracture
- 9 Cybersecurity failure
- 10 Livelihood crises

Top 10 risks in terms of Impact

- 1 Infectious diseases
- 2 Climate action failure
- 3 Weapons of mass destruction
- 4 Biodiversity Loss
- 5 Natural resource crisis
- 6 Human environmental damage
- 7 Livelihood crises
- 8 Extreme weather
- 9 Debt crises
- 10 IT infrastructure breakdown



Security incident caused by 3rd parties

Software vendor hacked causing security backdoor deployed on more than 18,000 of its customers.

INSIDER Log in Subscribe

HOME > TECH

Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal

Isabella Jibilian Dec 25, 2020, 12:38 AM



Online trading platform provider's service meltdown causing number of broker houses' customers unable to send online order.

The streaming services for trading securities were down in the morning session of December 23, 2019, causing investors to be unable to trade.

According to the reporter, all streaming services provided from security companies were down this morning due to technical problems from :

<https://www.kaohoon.com/content/332537>

Thai securities trading firm being hacked due to lack of software maintenance by 3rd party

Thai securities trading firm goes offline after cyberattack

DECEMBER 10, 2020 DISSENT

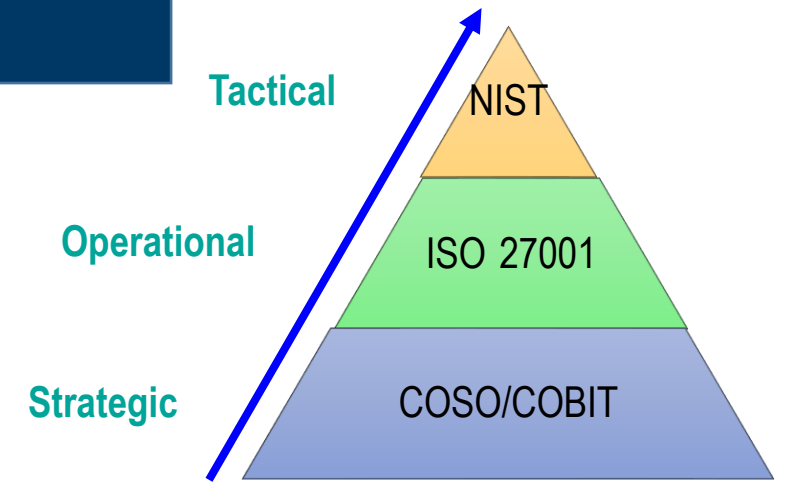
It seems that yet another group of threat actors are trying the double-extortion method. replete with trying to get media coverage.

"ALTDOS," as they call themselves, contacted a number of news outlets in Thailand and online news sites to announce that they had attacked : on December 4.

"A large Thailand SET public listed company dealing with securities trading has been hacked with its sensitive financial + customer database stolen and files encrypted last Friday (4th December 2020)," the hackers wrote, adding, deals with securities and financial trading services, however their servers are poorly protected."

Allegedly, as a result of the firm's lack of acknowledgement of their emails and demands, the attackers decided to dump some data. As proof of their claims, the attackers posted on popular file-sharing sites some of the data they claim to have exfiltrated. <https://www.databreaches.net/thai-securities-trading-firm-goes-offline-after-cyberattack/>

IT risk management framework/standard



Need to change mindset : Protection is not sufficient

Cyber Resilience framework



Identify



Protection



Detect



Respond



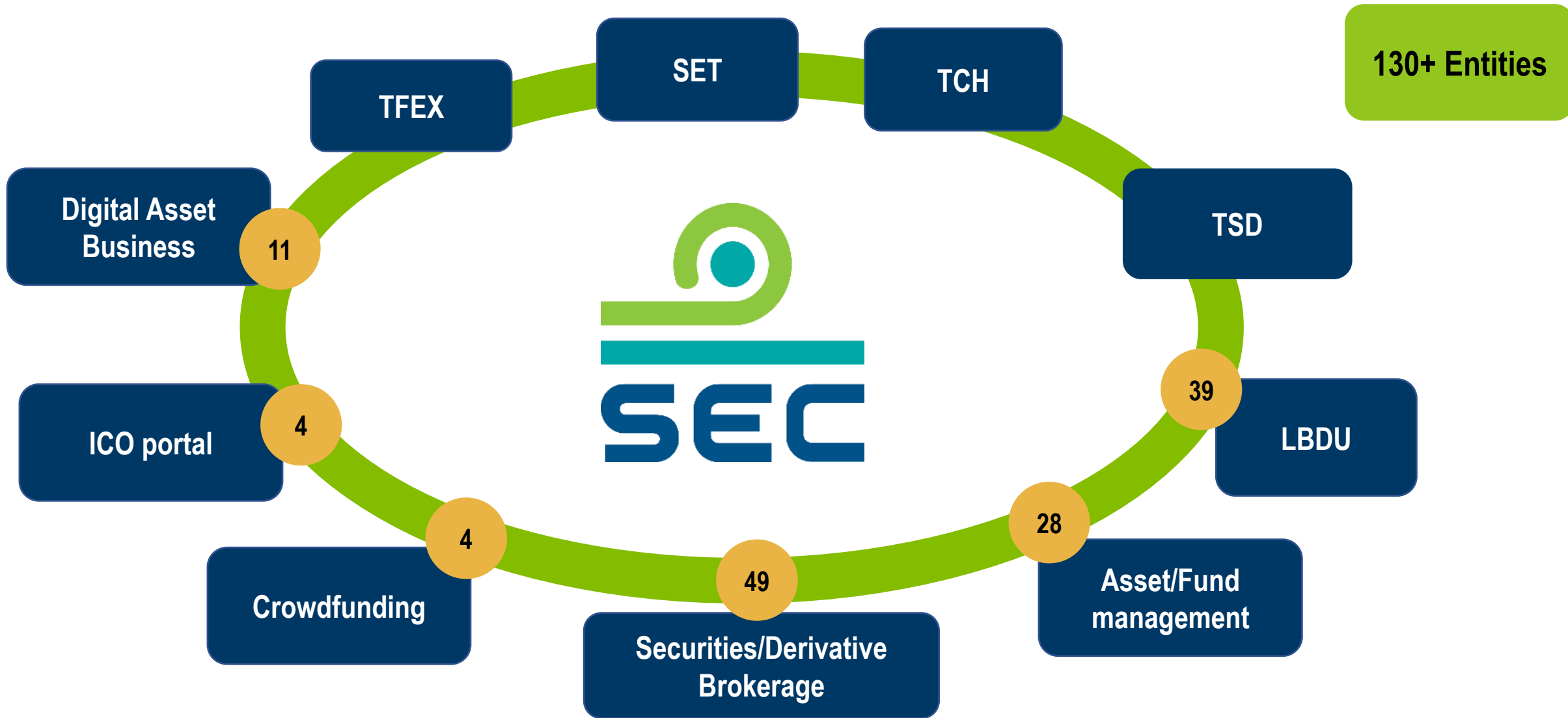
Recover

- No matter the preparation and protection measures an organization implements, it may not be able to avoid certain types of attacks
- **The Question is no longer “IF” but “When”**

Entity often fails to prepare for what to do when an attack succeeds.

Need to change mindset, focusing on cyber resilience not cybersecurity

Financial businesses under the SEC's supervision



Regulator's role

Facilitate innovation



- How easy is it for service providers to experiment with new ideas and mechanism?
- Are enabling laws and regulations in place?

Mitigate risk to trust and confidence



- Do we understand the market as it evolves?
- How can we use technology effectively?

Promote competition



- How easy is it for new business to enter the market?
- Do consumers have the information to make informed choices?
- How easy is it for consumers to switch service providers?

Our vision is:

“The SEC is ready to embrace changes and develops a sustainable capital market and economy for the benefit of all stakeholders”

Our mission is:

“To assure conducive environment for a fair, efficient, dynamic and inclusive capital market”

SEC Strategy Plan : 2021-2023



Digital for Capital Market

- To leverage digital technology to enhance business operation.
- Central Digital Infrastructure is also developed for Capital market participants.
- Capital market supervision is fair, reliable and responsive to cyber resilience.

SEC Cybersecurity Strategy for the Capital Market



Regulation & supervision

- Provide **regulation & guideline** to capital market in managing cyber risk
- Perform **supervision & inspection** to assess the quality of cyber oversight & risk management



Information sharing

- Maintain situational awareness / cyber intelligence through various **information sharing groups**
- Collaborate with industry to **share information**



Competency & capacity building

- Build **competencies** and **capacities** and **collaborate with industry** to uplift cyber resilience

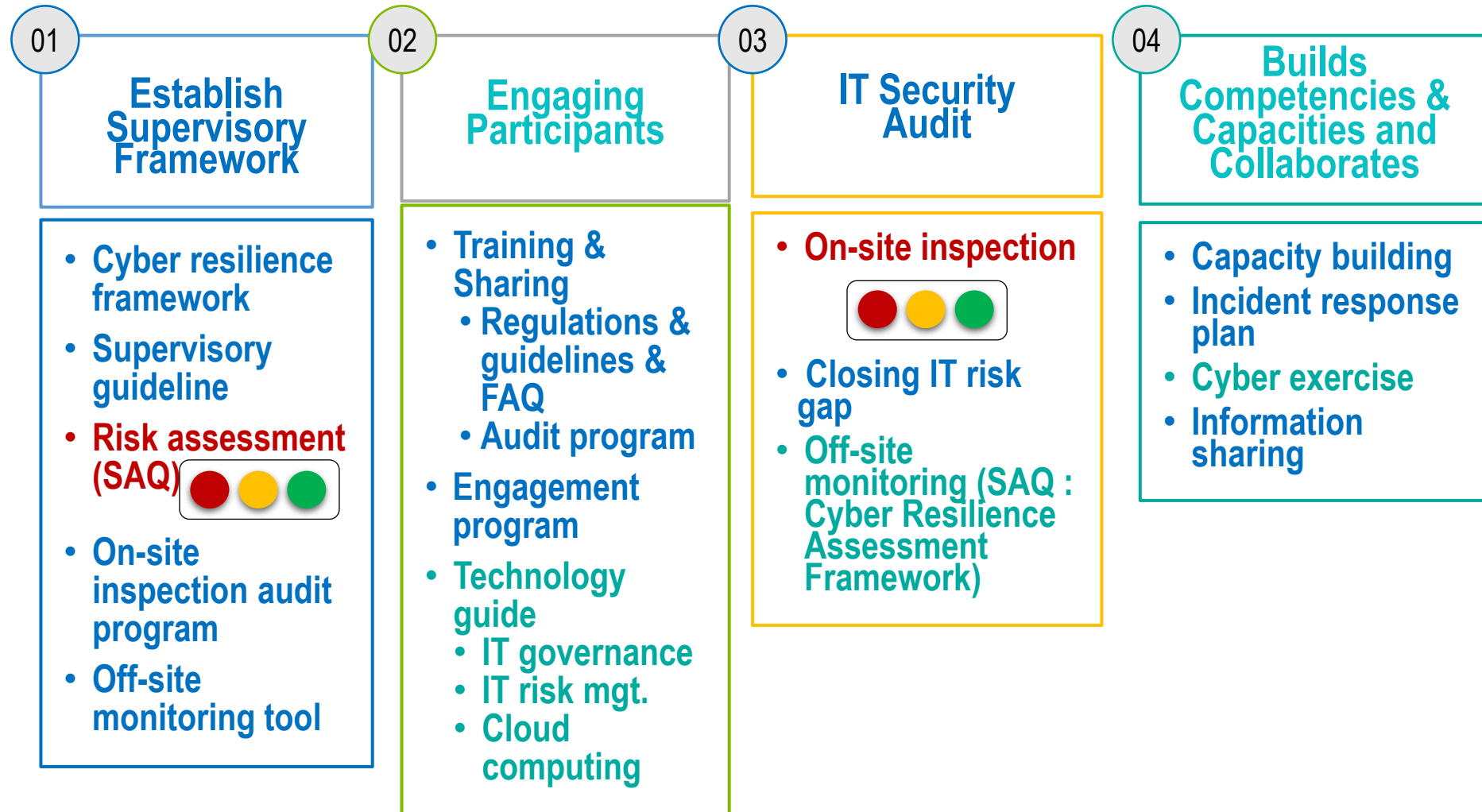


Incident Response & Cyber Exercise

- Build **incident response plan** and conduct **cyber exercise** in capital market **with industry**

SEC Supervisory Framework

Obj: To Build the Cyber Resilience in the Capital Market



Information Security Supervisory

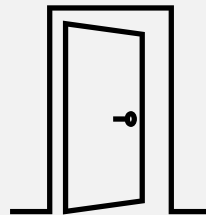
0. Pre-consult

- *Not mandatory*
- Opportunity to clarify the SEC expectations before the formal application process
- Provide feedback within 2 weeks (approximately)



1. Formal application submission

- Final document review
- Interviewing IT staffs
- On-site audit for activation (depending on the type of businesses)
- Duration depends on the type of business



2. On-going supervision

- Offsite Monitoring
- Onsite Inspection (IT Risk Supervision)

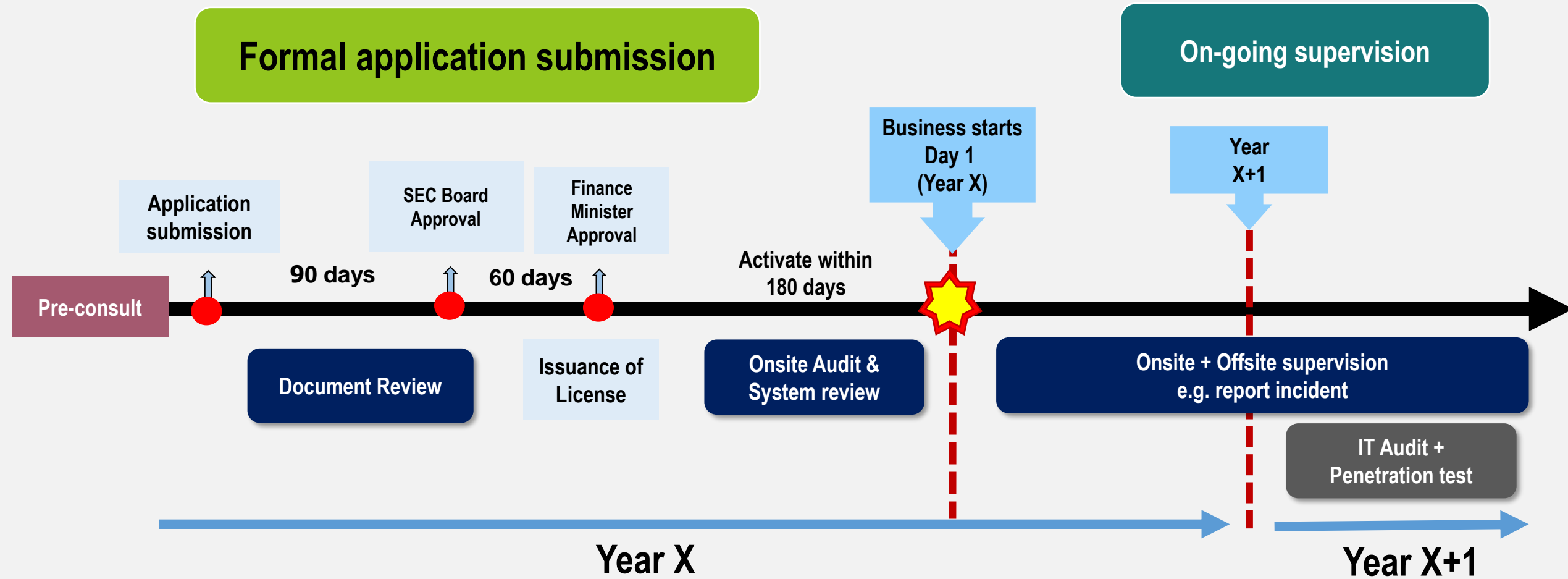


Example of Process Timeline

(Digital Asset Business)

Formal application submission

On-going supervision



IT Risk Supervision



IT Risk Supervision

Confidentiality
Integrity
Availability



International Standards



Relevant national
regulations & standards

Sor Thor. 37/2559

RULES

in Detail on Establishment of
IT System



Nor Por. 3/2559

GUIDELINES

for Establishment of
IT System



IT Governance

IT Risk Management

Cloud Computing

Supervision : SEC performs Supervision & Inspection

Onsite Inspection



Inherent risk assessment

- High
- Medium
- Low

Onsite inspection within 3 years



Starting from Q2/2017, still ongoing ...



Coverage

- Stock exchange
- Brokerage firms
- Asset managers
- Mutual fund brokerage

Offsite Monitoring

SAQ



- Provide tool for securities firm to self assessed its IT security maturity level if it is commensurate with the level of inherent risk (similar approach to FFIEC SAQ)
- Scheduled to launch an offsite SAQ in Q1/2019

Cybersecurity Risk/Maturity Relationship

| | | Inherent risk levels | | | | |
|--|--------------|----------------------|---------|----------|-------------|------|
| | | → | | | | |
| Cybersecurity maturity level for each domain | | Least | Minimal | Moderate | Significant | Most |
| | Innovative | | | | | |
| | Advanced | | | | | |
| | Intermediate | | | | | |
| | Evolving | | | | | |
| | Baseline | | | | | |

Source: FFIEC Cybersecurity Assessment Tool User's Guide (June 2015)

On-going Supervision



Offsite Tools

Objectives:

- To monitor the conduct of activities of Licensed Corporations, which allows TH SEC to keep eyes on soundness of
 - (1) Risk management
 - (2) Internal controls
 - (3) Compliance functions
 - (4) Incidents management
- To promptly implement any required actions in responding to the rising risk.

| Offsite tools | Coverage | Objective |
|---------------------------------------|--|--|
| Notification | <ul style="list-style-type: none"> IT incident | <ul style="list-style-type: none"> To report of significant IT Incident To allow SEC to promptly update the situation To provide sufficient information for SEC to take appropriate actions |
| Annual report** | <ul style="list-style-type: none"> IT Audit report Penetration test report | <ul style="list-style-type: none"> To identify security weaknesses To assess effectiveness and efficiency of information security management |
| Self-assessment Questionnaire (C-RAF) | <ul style="list-style-type: none"> IT and Cyber Security | <ul style="list-style-type: none"> To raise awareness on security controls To understand inherent risks and residual risks of each entity |

***For high-risk businesses i.e. Digital asset business operators*

On-going Supervision

Offsite Tools

Cyber Resilience Assessment
Framework (C-RAF)

C-RAF Process overview

Inherent Risk Assessment

- ❖ Assess Inherent risk level (*low/medium/high*)
- ❖ Determine expected maturity level (*Baseline / Intermediate / Advance*)

Maturity Level Assessment

- ❖ Perform maturity assessment for relevant components
- ❖ Determine current maturity level (*Baseline / Intermediate / Advance*)

Improvement work

- ❖ If Actual maturity level is lower than the Expected maturity level, then the entity should formulate an improvement plan, endorsed by management

C-RAF : Inherent and Maturity Level Assessment Sample worksheet

Inherent Risk Assessment

| Inherent risk assessment | | | |
|--------------------------------|--|--|-----------|
| No | Descriptions | Unit of measurement | Responses |
| Category 1 - Technology | | | |
| 1 | Total number of internet service provider (ISP) connections (including branch connections if not a leased line), which are connected to the corporate | No. of connections | |
| 2 | Total number of point-to-point connections via leased lines or private connections technology between the company and external parties (including service provider, customer, business | No. of private leased line connections. | |
| 3 | Use of wireless network access. | Separation of access points for guest and | |
| 4 | Non-corporate devices (Physical devices not owned by the company) allowed to connect to the corporate network. | No. of staffs who can get access corporate resources using non-corporate device or | |
| | | Mobile push mail | |
| | | laptop/PC | |
| | | Removable storage | |
| | | Others | |
| | Total of staffs who are teleworkers or use company provided mobility device. | No. of teleworkers | |
| | Application permitted for BYOD access. | Type of applications | |

Maturity Level Assessment

| Domains | Sub Domains | Level 1 | Level 2 |
|------------|-------------|---|--|
| Governance | Oversight | 1.Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. | 4.At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program. |
| | | 2.Information security risks are discussed in management meetings when prompted by the visible cyber events or regulatory reports. | 5.Cybersecurity tools and staff are requested through the budget process. |
| | | 3.Management provides a written report on the overall status of the information security and business | |

Inherent Risk Assessment from SAQ



Track records on cyber threats

(5 ข้อ)

010101010101010100
0001Hacker00101010
100110011110001111



Technology (12 ข้อ)

Internet



BYOD

CLOUD



Business Size (6 ข้อ)



Product & Services

(2 ข้อ)



\$

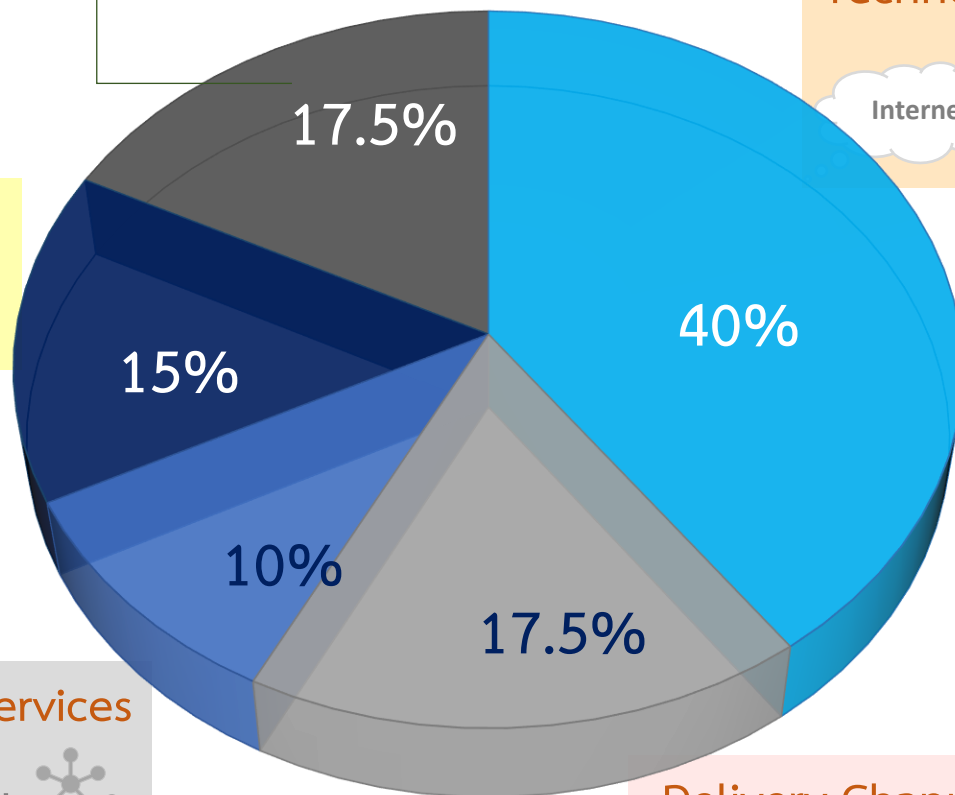


%

Delivery Channels (5 ข้อ)



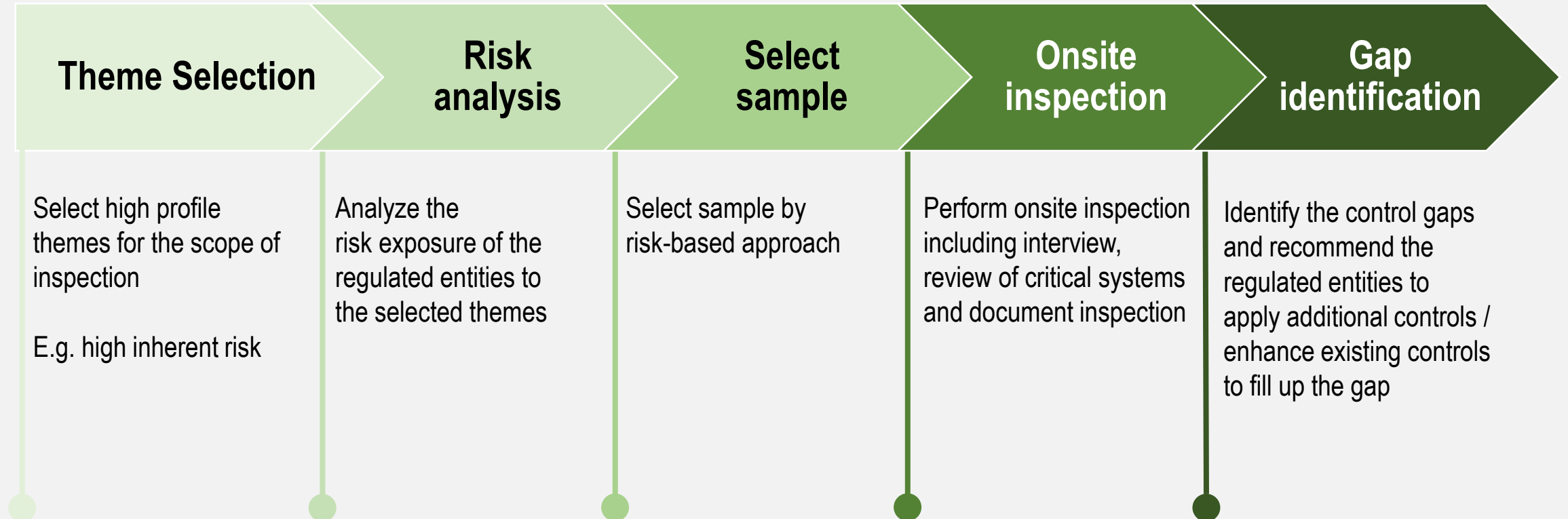
APP



On-going Supervision

Onsite Tools

5 phrases for onsite audit

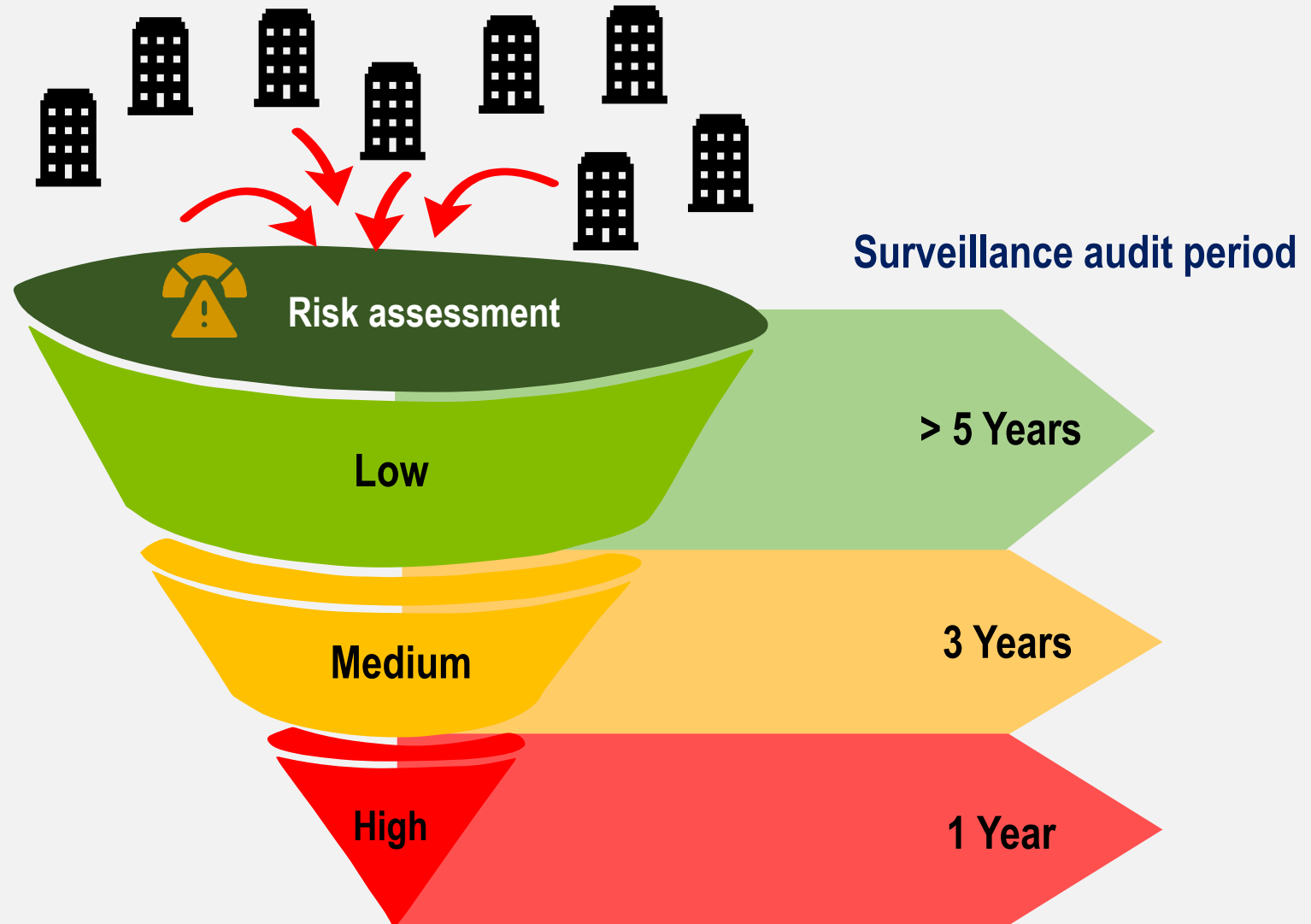


On-going Supervision

Onsite Tools

Objectives:

- To ensure soundness of business and IT practices against reference standard or requirements
- Evaluate adequacy of IT risk management process against IT security and cybersecurity
- Evaluating the internal control procedures established by licensees



Scope of work

| Area of Control | Basic Control | Intermediate Control | Advance Control | Total |
|--|---------------|----------------------|-----------------|------------|
| 1. IT Governance | 10 | 9 | 6 | 25 |
| 2. Information security policy | 3 | | | 3 |
| 3. Organization of Information Security | 9 | 18 | 7 | 34 |
| 4. Human resource Security | 8 | 1 | 1 | 10 |
| 5. Asset Management | 11 | 9 | 2 | 22 |
| 6. Access Control | 16 | 7 | 4 | 27 |
| 7. Cryptographic control | 4 | 5 | 2 | 11 |
| 8. Physical and Environment Security | 12 | 4 | 1 | 17 |
| 9. Operations Security | 25 | 23 | 4 | 52 |
| 10. Communication security | 23 | 11 | 6 | 40 |
| 11. System Acquisition, Development and MA. | 16 | 3 | 12 | 31 |
| 12. IT Outsourcing | 10 | 4 | | 14 |
| 13. Information security incident management | 8 | 12 | 1 | 21 |
| 14. Business Continuity Management | 6 | 8 | 2 | 16 |
| Total | 161 | 114 | 48 | 323 |

How to gather data?

Interview



Documentation



Observation



Re-perform



Gap Assessment

| Finding Area | Low | Medium | High |
|--|-----|--------|------|
| 1. IT Governance | | | |
| 2. Information security policy | | | |
| 3. Organization of Information Security | | | |
| 4. Human resource Security | | | |
| 5. Asset Management | | | |
| 6. Access Control | | | |
| 7. Cryptographic control | | | |
| 8. Physical and Environment Security | | | |
| 9. Operations Security | | | |
| 10. Communication security | | | |
| 11. System Acquisition, Development and MA. | | | |
| 12. IT Outsourcing | | | |
| 13. Information security incident management | | | |
| 14. Business Continuity Management | | | |
| Total | | | |

Regulation : SEC guides firms using rules and guidelines

Rules



Regulation

Requiring firms to implement risk management and control proportionate to risk

Set out key principal objectives



Governance of enterprise IT



Notify SEC of security incident



Cyber resilience

- Identify, protect, Detect, respond, and recover
- Cyber exercise
- Vulnerability assessment and penetration test



Addressing new trend

- Cloud computing
- Teleworking
- BYOD

Guideline & FAQ



Guideline

Safe harbor on implementation to meet objective



FAQ

Provide frequently asked question

Set out supervisory expectations on good practice on IT risk



BoD & high-level management oversight



Operational controls on
Identify, Protection, detection, response, and recovery



Business resource



IT audit



IT outsourcing

NOTE: The SEC is in the process of issuing good practice/manual with regard to IT governance, cloud computing, and IT risk assessment.

IT Risk Supervision

Chapter 1 Governance of Enterprise IT

- Roles and responsibilities of BoDs and senior managements
- Policy on the governance of IT, including
 - IT risk management
 - IT resource allocation and management
 - IT security
- Policy communication
- Internal control for IT operation

Chapter 2 IT Security

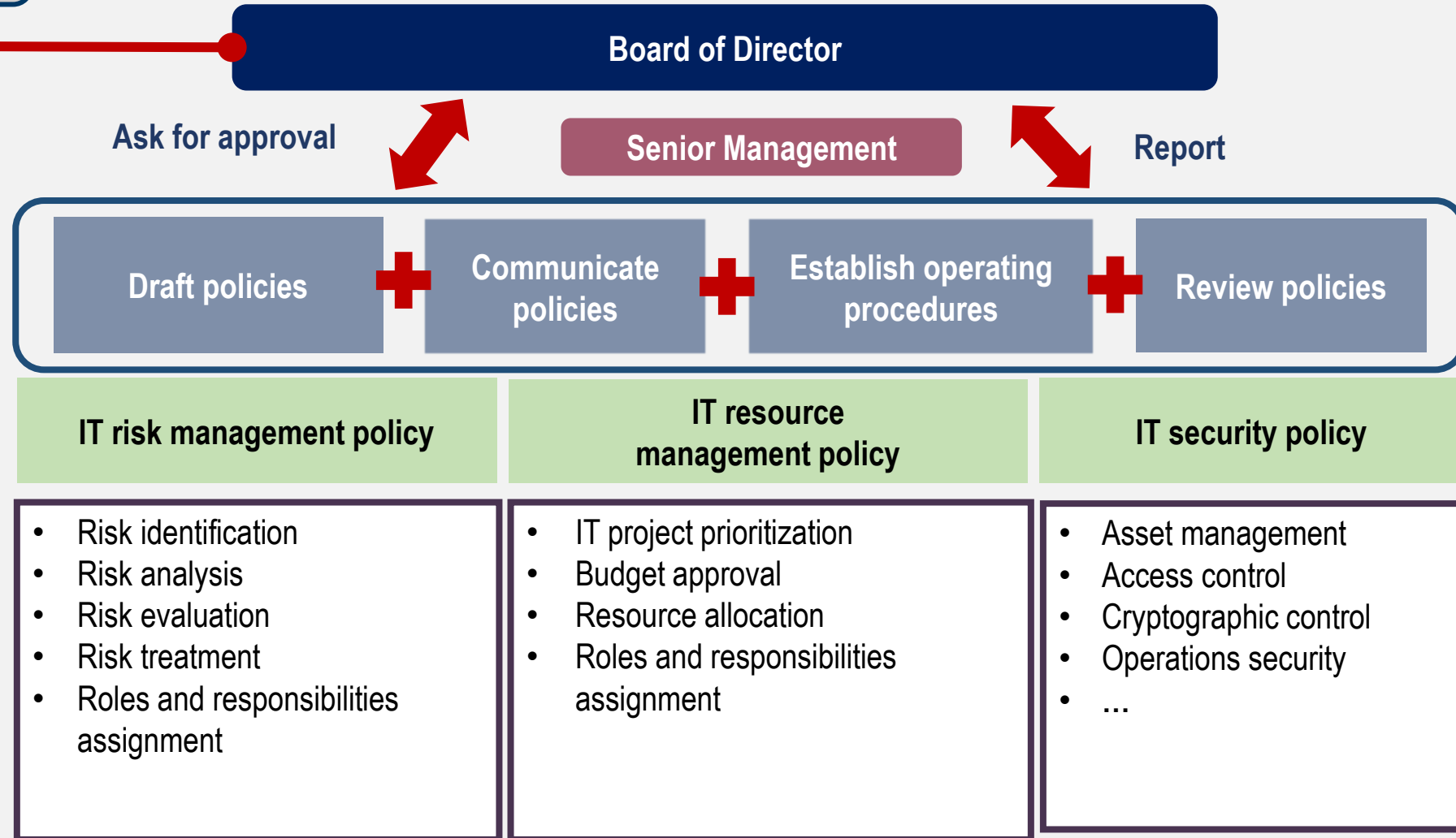
- Organization of information security
- Human resources security
- Asset management
- Access control
- Cryptographic control
- Physical and Environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- IT outsourcing
- Information security incident management
- Information Security Aspects of BCM

IT Governance



Roles and responsibilities of BoDs**

- Approve the IT governance policy
- Reported on the conformance of the IT governance policy
- Reported on the evaluation of incident response test
- Evaluate, direct, monitor for effective Governance of Enterprise IT

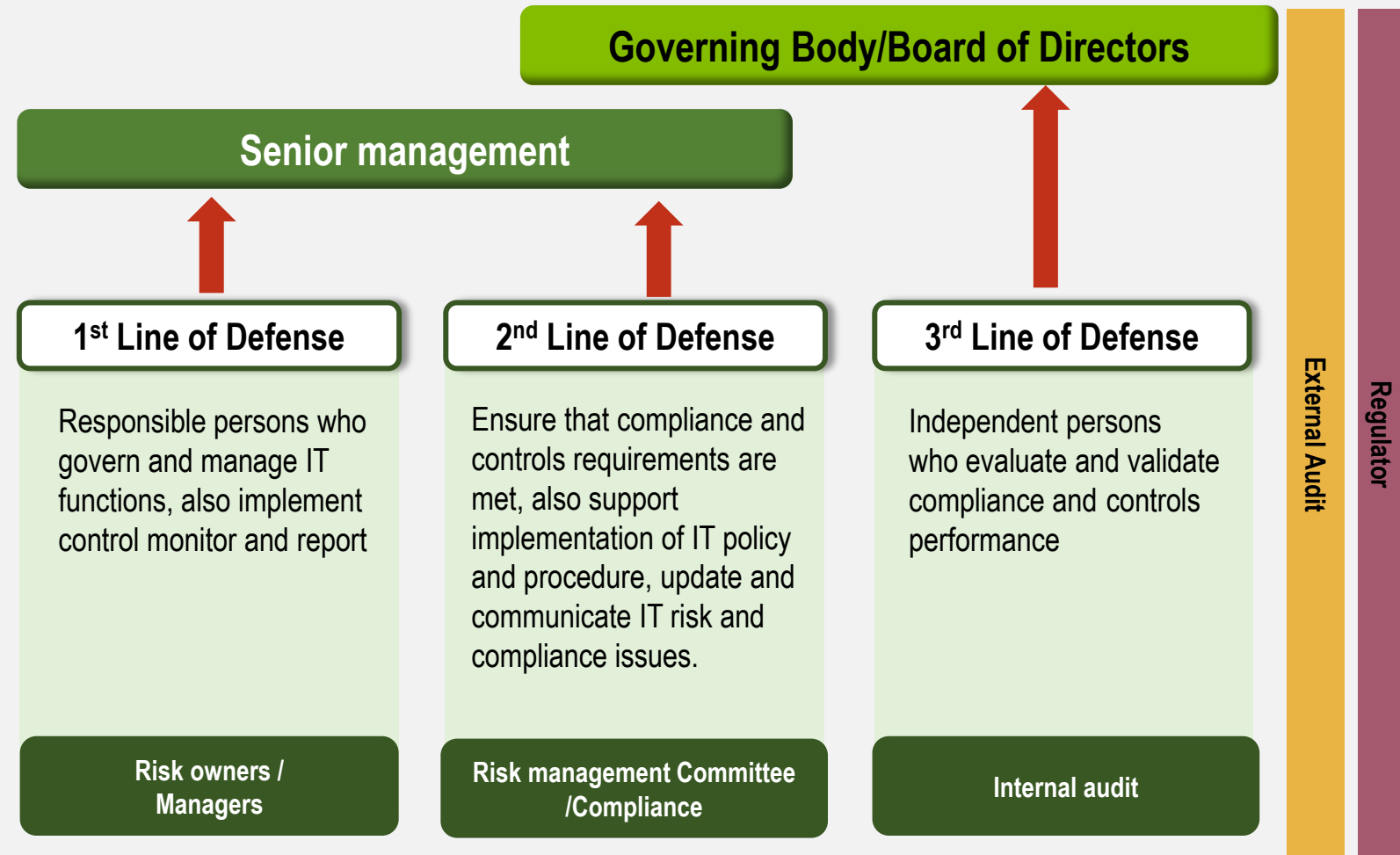
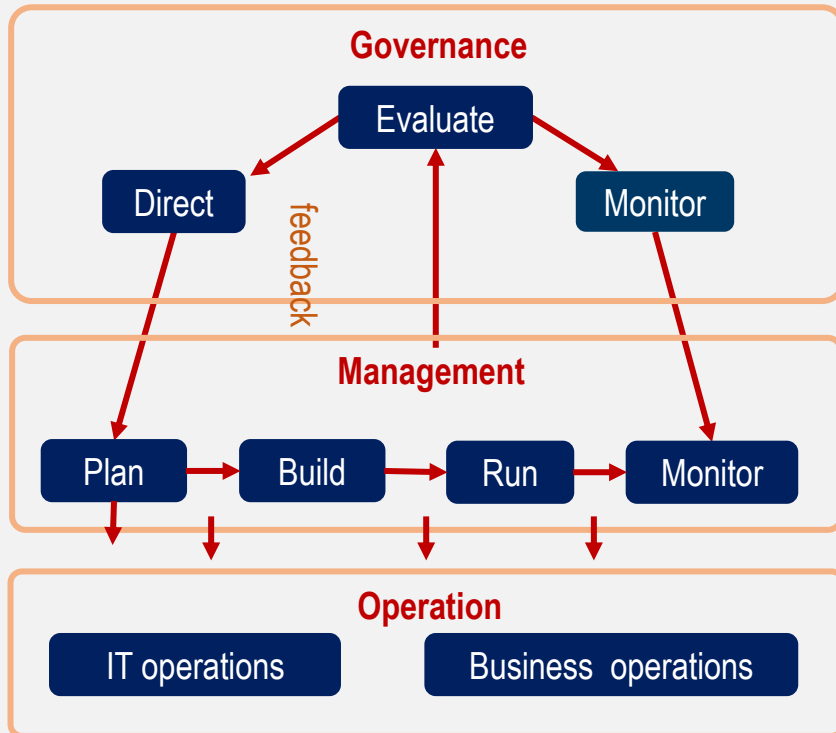


**BoDs or a committee assigned by the BoDs

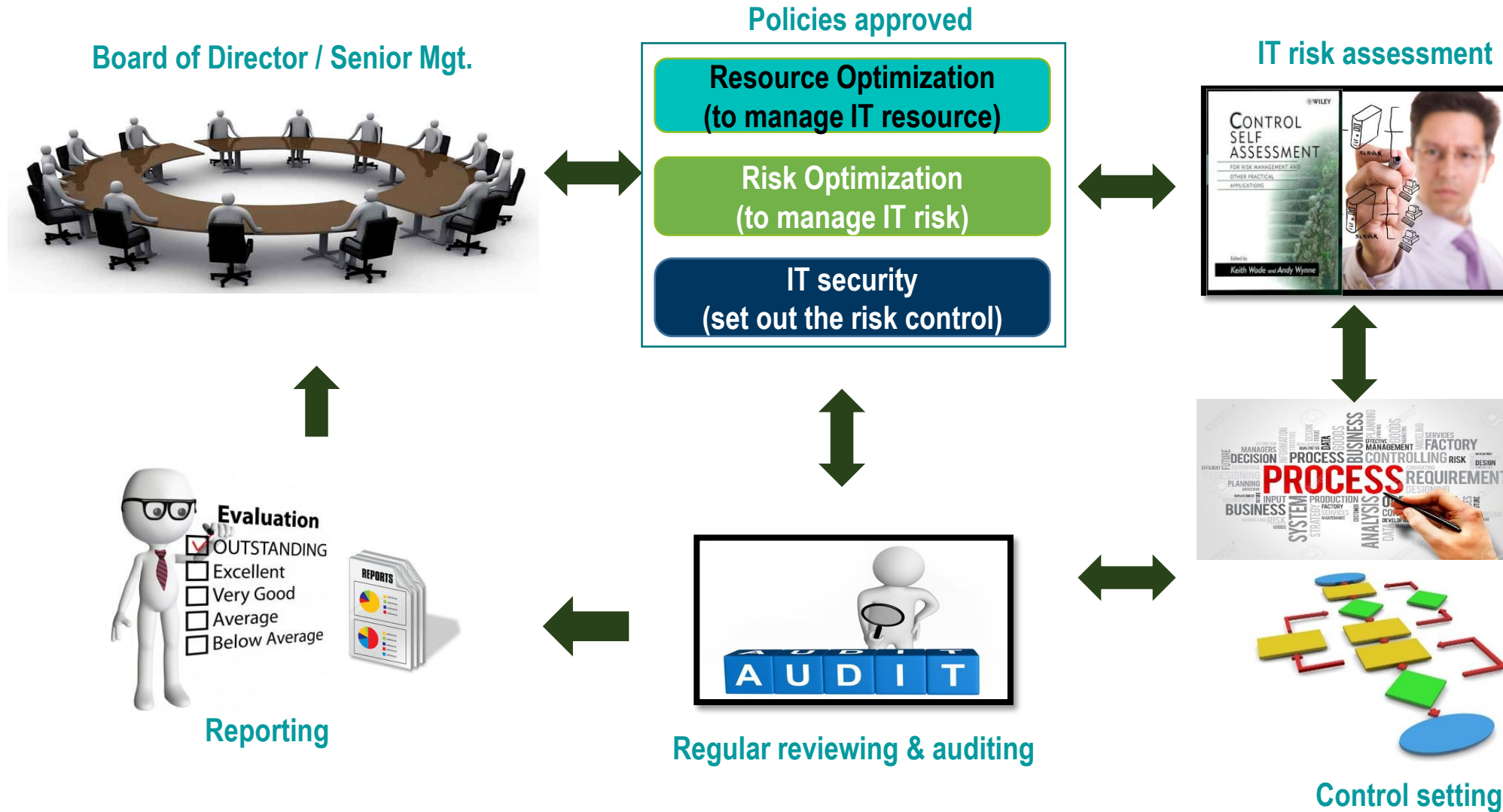
Three Lines of Defense

Governance structure

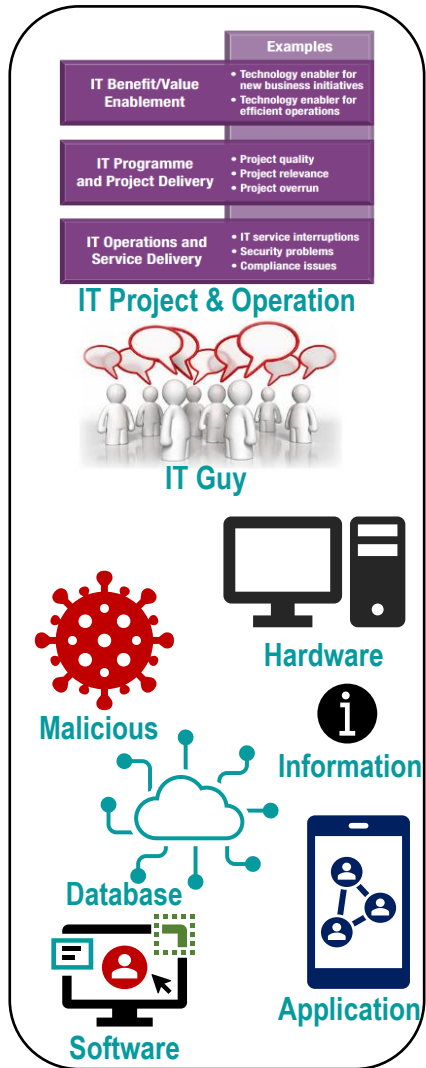
Reference : COBIT 5 Governance and Management Key Areas



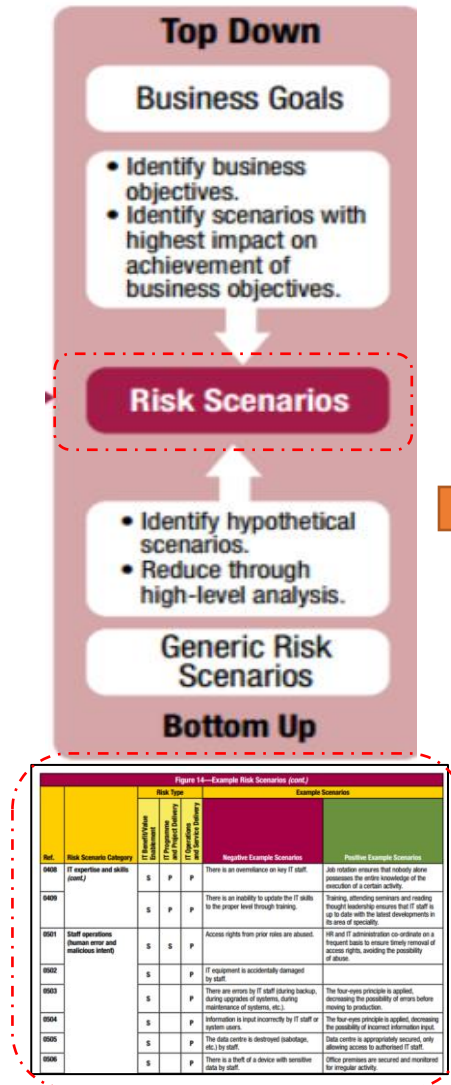
Overview : Governance of Enterprise IT



IT related risk



Risk scenarios



Risk register

| ID | Risks | Owner(s) of the risk | I | L | S | Controls | Owner(s) of the control |
|----|--|----------------------|---|---|----|---|--------------------------------|
| 1 | Failure to attract, recruit and retain key staff | SR | 4 | 4 | 16 | - Salary surveys - Training and mentoring schemes - Retention packages for key staff | TJ TB TJ |
| 2 | Financial advisors misinterpret/fail to understand the complexity of 'equity release' products | PL AB | 4 | 4 | 16 | - Staff training - Learning gained from previous deals - Review of individual needs in performance appraisal process - Procedure manuals for processes | TB KW & EL TB EL |
| 3 | Poor staff communication | SR JK | 4 | 4 | 16 | - Defined communication channels - Documented procedures and processes | ZK EL |
| 4 | Failure to understand the law and/or regulations | PL | 4 | 3 | 12 | - Internal training courses - Regular updates from various sources - External training courses | EL EL TB & EL |
| 5 | Poor detection of money laundering | PL | 4 | 3 | 12 | - AML annual training - Circulation of BBA awareness circulars - KYC | TB & EL EL & ZK ALL |
| 6 | Insufficient funds/deposits to cater for lending activities | CK | 4 | 3 | 12 | - Liquidity risk policy - Advertising - Economic forecasting | ZK KW CK |
| 7 | Over-selling credit cards | CK | 4 | 3 | 12 | - Staff training - Credit scoring - Forward business planning | TB EL ZK |
| 8 | Over-deployment of management resources on regulatory issues | RU CK | 3 | 4 | 12 | - Monthly budget against actual review - Corporate governance - Monthly head of compliance & CEO meetings | TJ CK CK |
| 9 | Failure to capture market opportunities | AB | 3 | 3 | 9 | - Competitor monitoring - Product development | TB TB |
| 10 | Overdependency on outsourcing | CK | 3 | 3 | 9 | - SLAs - Outsourcing monitoring - Due diligence - Policy | CK & EL CK & EL CK CK |

Example: Risk scenarios

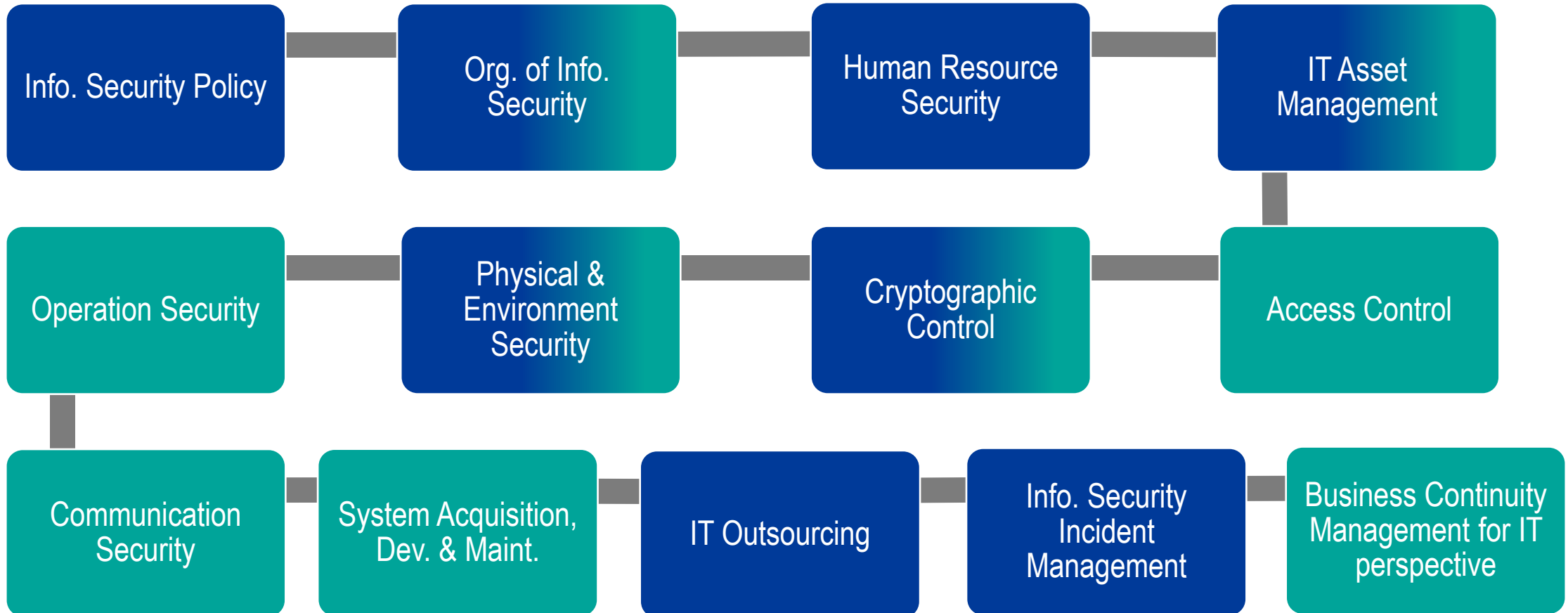
| Risk Scenario Category | Example scenarios |
|--|--|
| 1. IT Investment Decision Making | <ul style="list-style-type: none"> - Business managers are not involved in important IT investment decision making - Selection of wrong software / infrastructure - Purchase of redundant software |
| 2. IT Expertise and Skills | <ul style="list-style-type: none"> - Lack of or mismatched IT-related skills - Lack of business understanding by IT staff - Inability to recruit IT staff. - Overreliance on key IT staff. - Critical staff turnover |
| 3. Staff Operations | <ul style="list-style-type: none"> - Human error and malicious intent |
| 4. Business ownership of IT | <ul style="list-style-type: none"> - Business failing to be accountable - Ineffective Service Level Agreements (aggressive sales) |
| 5. Information | <ul style="list-style-type: none"> - Data breach / damage / leakage / unauthorized access |
| 6. Infrastructure | <ul style="list-style-type: none"> - New infrastructure is installed and whole systems become unstable - Systems cannot handle load increasing - Failure of utilities (telecom, electricity) - IT in use is obsolete / cannot satisfy business needs |
| 7. Software | <ul style="list-style-type: none"> - Failure to develop s/w as business required - Use of immature s/w (bugs) - s/w glitch / malfunction - Unintentional / intentional modification of s/w |
| 8. Portfolio Establishment and Maintenance | <ul style="list-style-type: none"> - Selected programs are not optimizing business benefits - Incompatibility of business systems |

Example: Risk scenarios

| Risk Scenario Category | Example scenarios |
|--|---|
| 9. Infrastructure theft or destruction | <ul style="list-style-type: none"> - Unauthorized physical access - Theft of development servers - Accidental destruction caused by individual |
| 10. Malware | <ul style="list-style-type: none"> - Virus Infection / Phishing |
| 11. Logical attacks | <ul style="list-style-type: none"> - Network penetration / Industrial espionage / Hacktivism |
| 12. Industrial action | <ul style="list-style-type: none"> - Staff's strike / building is not accessible - Third party is unable to provide service |
| 13. Environmental | <ul style="list-style-type: none"> - Environmental impact of the used technology |
| 14. Acts of nature | <ul style="list-style-type: none"> - Earthquake / Flooding |
| 15. Innovation | <ul style="list-style-type: none"> - Failure to adopt and exploit new technology |
| 16. Suppliers | <ul style="list-style-type: none"> - Outsourcing (inability to comply SLA) |
| 17. Program/Projects Life Cycle Management | <ul style="list-style-type: none"> - Failing projects are not terminated - Delays in IT projects - Project budget overrun |
| 18. Regulatory compliance | <ul style="list-style-type: none"> - Noncompliance with Regulation |
| 19. Geopolitical | <ul style="list-style-type: none"> - Damage caused by political activists / Government intervention / Terrorist attacks |

IT Security

Chapter 2 : IT Security (12 domain controls)



1. Organization of Information Security

Internal Organization



- Information security roles and responsibilities
- Segregation of duties
- Contact with SEC, relevant authorities, and service providers

Mobile devices and teleworking



- Policy and measures on the use of mobile devices, teleworking
- Policy and measures for Cloud computing

2. Human resource Security

- Information security awareness, education and training
- IT Policy communication
- Disciplinary process



**Prior to
employment**



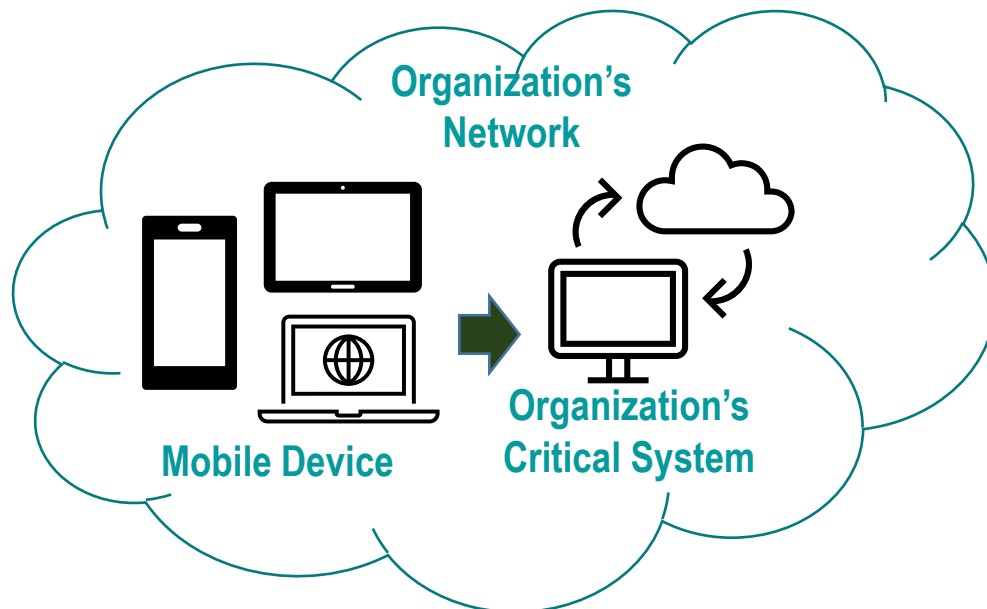
**During
employment**



**Termination of
employment**

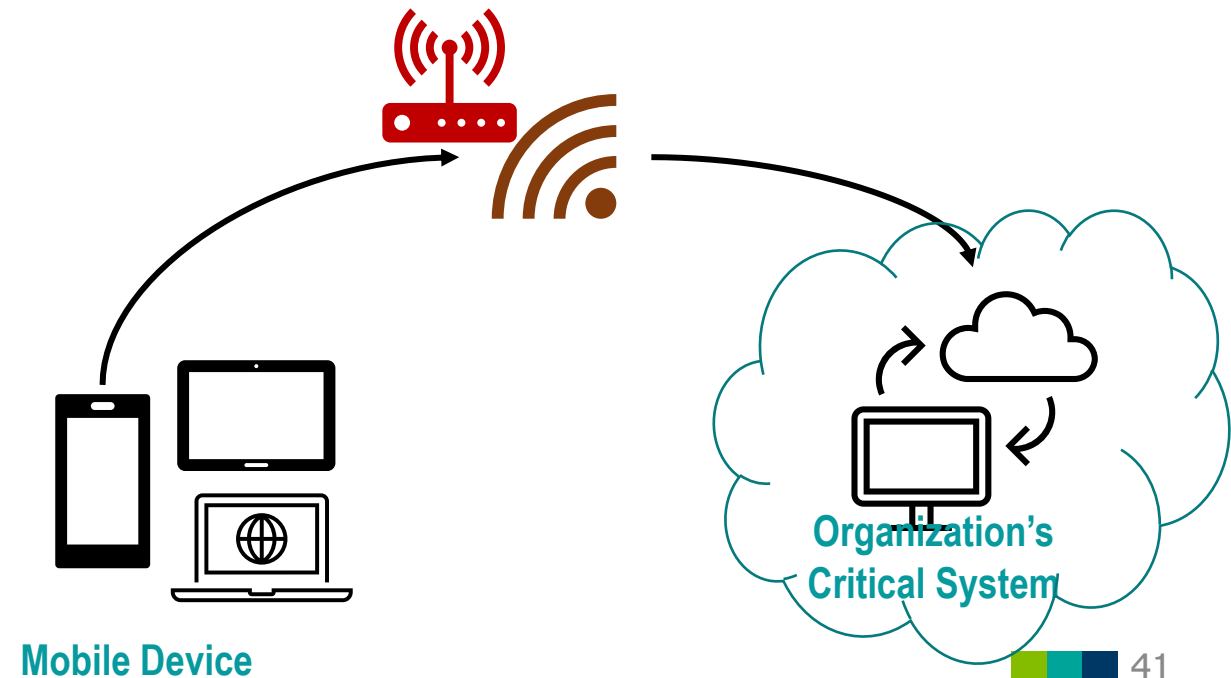
Mobile Device

use of mobile devices in the operation to access the critical information system via direct connection to the organization's internal network systems



Teleworking

accesses the critical information system with indirect connection to the organization's internal network systems



What is Cloud Services ?



Service Models:



Software (Consume)

Software as a Service (SaaS)

to use the provider's applications running on a cloud infrastructure



- Web-based email
- Application
- Social media (Blog, Wiki)
- Productivity tools (Office365)



Platform (Build on it)

Platform as a Service (PaaS)

to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider



- Application Development
- Developer tool for database & testing
- Decision Support System



Infrastructure (Migrate to it)

Infrastructure as a Service (IaaS)

to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software



- CPU load
- Storage
- Server Capacity
- Network (Bandwidth/Latency)

Cloud characteristics

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity (scale out)



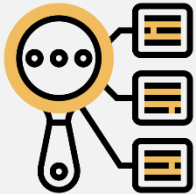
3. Asset management

Responsibility for Assets



- Asset inventory
- Ownership of assets
- Acceptable use of IT assets

Asset Classification



- Classification of information
- Handling of assets

Media Handling



- Management of removable media
- Transfer and Disposal of media

4. Access Control

Business Requirements of Access Control



- Access control policy

User Access Management



- User registration and de-registration
- Management of privileged access rights
- Credential (password) management
- Monitor and review of user access rights

User Responsibilities



- Use of password

System and Application Access Control



- Information access restriction
- Secure log-on procedures
- Password management system
- User of privileged utility programs
- Access control to source code

5. Cryptographic control



- Policy on the use of cryptographic controls
- Key management

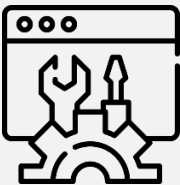
6. Physical and Environmental security

Secure areas



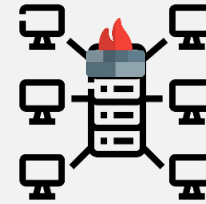
- Define the secure areas based on risk
- Physical entry controls
- Securing the areas

Equipment



- Prevent loss, damage, theft or compromising of equipment assets

7. Communications Security



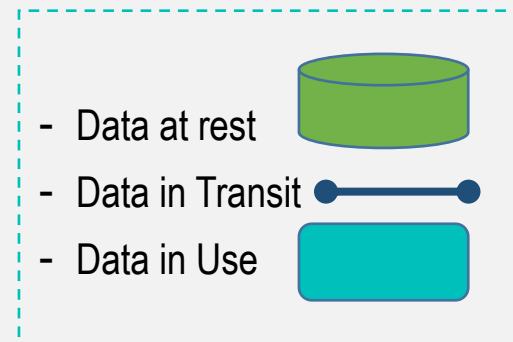
Network Security Management

- Network controls
- Network services agreements
- Segregation in networks



Information Transfer

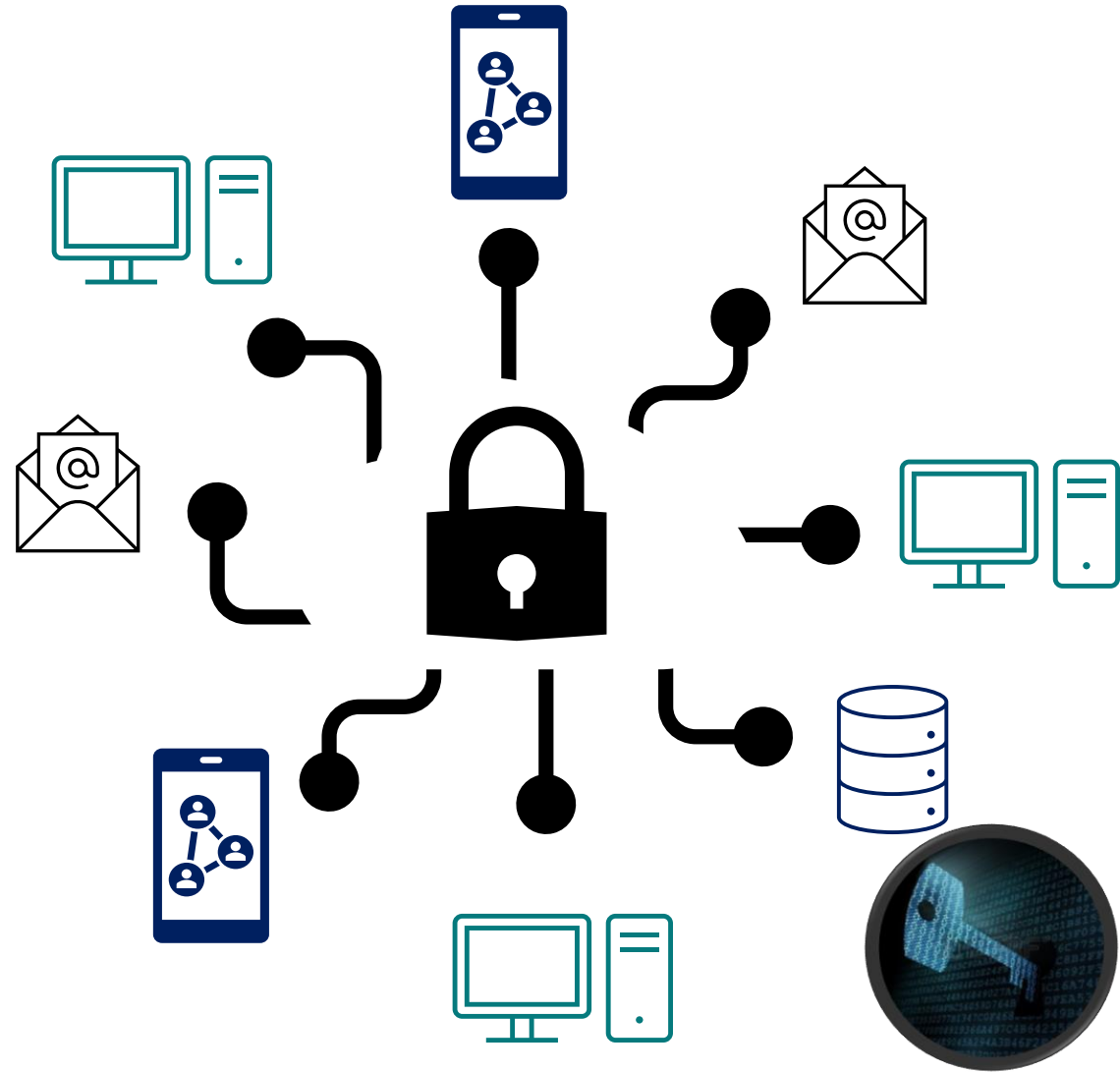
- Information transfer policies and procedures
- Electronic messaging protection
- Confidentiality or Non-disclosure agreements



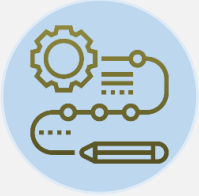


Encryption Control

- Address the type, strength and quality of the encryption algorithm
- Required level of protection on sensitive and critical information
- Managing cryptographic keys through their whole lifecycle : cryptographic algorithm, key length, secure process for key management and monitor key management



8. IT Operations security



Operational procedures and responsibilities

- Documented operating procedures
- Change management
- Capacity management
- Separation of development, testing, and operational environment



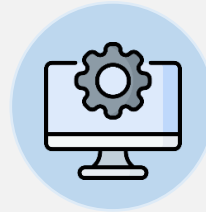
Protection against malware

- Measures against malware



Backup

- Information backup and recovery test



Control of operation software

- Controls on installation of software on the operating systems



Technical Vulnerability Management

- Vulnerability assessments with all critical information systems
- Penetration testing with critical information systems connected to untrusted networks



Logging and monitoring

- Event logging e.g. physical access, firewall, authentication, internet access, and database
- Protection of log information
- Monitoring and reviewing logs



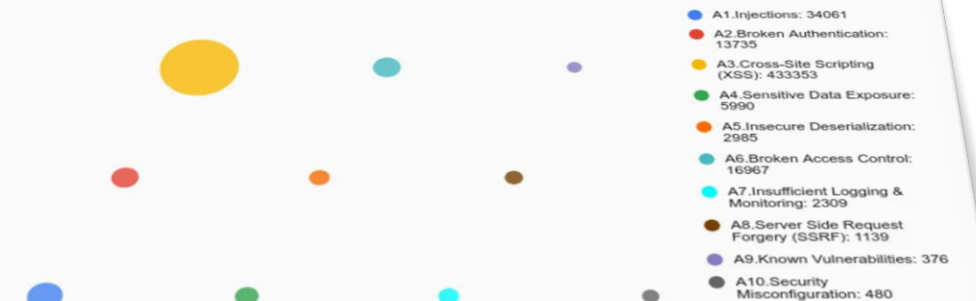
Information Systems Audit

- Information systems audit controls

| OWASP Top 10 2017 | | change | OWASP Top 10 2021 proposal | |
|-------------------|-----------------------------------|-------------|----------------------------|--|
| A1 | Injections | as is | A1 | Injections |
| A2 | Broken Authentication | as is | A2 | Broken Authentication |
| A3 | Sensitive Data Exposure | down 1 | A3 | Cross-Site Scripting (XSS) |
| A4 | XML eXternal Entities (XXE) | down 1 + A8 | A4 | Sensitive Data Exposure |
| A5 | Broken Access Control | down 1 | A5 | Insecure Deserialization (merged with XXE) |
| A6 | Security Misconfiguration | down 4 | A6 | Broken Access Control |
| A7 | Cross-Site Scripting (XSS) | up 4 | A7 | Insufficient Logging & Monitoring |
| A8 | Insecure Deserialization | up 3 + A4 | A8 | NEW: Server Side Request Forgery (SSRF) |
| A9 | Known Vulnerabilities | as is | A9 | Known Vulnerabilities |
| A10 | Insufficient Logging & Monitoring | up 3 | A10 | Security Misconfiguration |

OWASP : Open Web Application Security Project

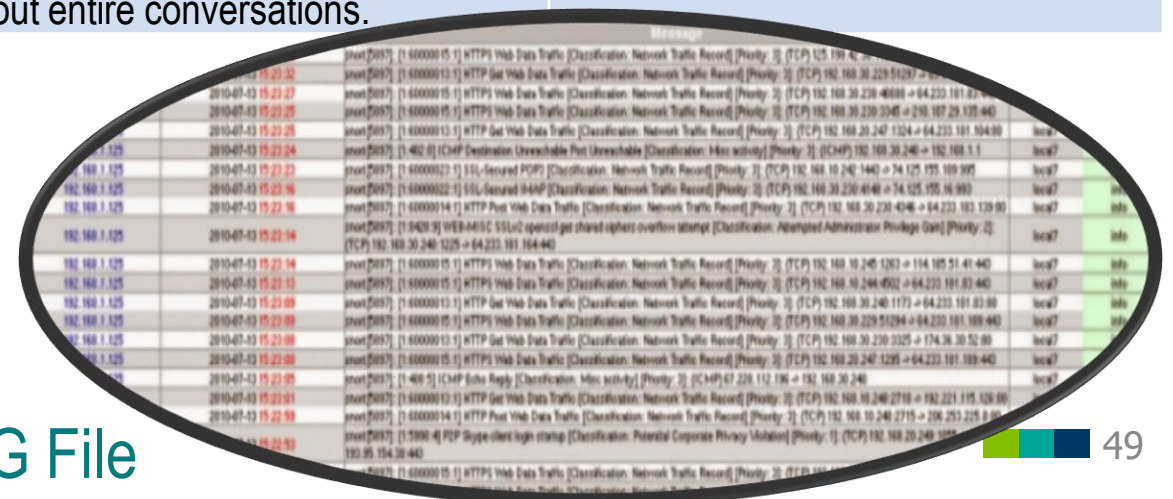
Application security experts could also find interesting distribution these categories by amount of security reports, mean bulletins, bug bounties, exploits, altogether:



Source : <https://www.immuniweb.com/resources/owasp-top-ten/>

| Category of logs | Minimum Logging Details | Minimum Period of Retention |
|--|--|--|
| 1. Physical Access Logs | <ul style="list-style-type: none"> Name of access persons Dates Times Access Attempts (if any) | At least 3 months |
| 2. Authentication Logs for Database and Network Access | <ul style="list-style-type: none"> User IDs Dates Times Access Attempts | At least 3 months |
| 3. Application Logs | <ul style="list-style-type: none"> User IDs IP Addresses Dates Times. In case of the securities trading system, the details shall include: Securities Symbol Broker Numbers (4-digit) SET Order IDs Account IDs Dates & Times of transactions (yyyy/mm/dd - hh:mm:ss:sss) Source Public and Local IP Addresses Destination IP Addresses Full URL Terminal Type (if any, such as iPad, iPhone). The intermediary must be able to identify user identities and Local IP addresses at the time of use (not applicable to the use via employees' personal devices). | <p>At least 1 year for the intermediary undertaking securities business in the brokerage, dealing or underwriting of any securities, which is not limited to debt securities or investment unit, and derivatives agent.</p> <p>At least 6 months for the intermediary undertaking securities business in the area not covered above.</p> |
| 4. Internet Access Logs | <ul style="list-style-type: none"> User IDs IP addresses Organization IP addresses Date Times Full URL of destination website. The intermediary must be able to identify user identities and IP addresses at the time of use. | |

| Category of logs | Minimum Logging Details | Minimum Period of Retention |
|---|--|---|
| 5. Audit Logs | <ul style="list-style-type: none"> User IDs Dates Times records of reading & editing on data. | At least 6 months . |
| 6. Event Logs of Operating Systems and Network Firewall | <ul style="list-style-type: none"> Dates Times Event Services for OS such as service status Event Services for Network Firewall such as rules modification of network firewall. | As necessary and sufficient for inspection , based on risk assessment of the organization. |
| 7. Network Firewall Logs | <ul style="list-style-type: none"> Dates Times Source and Destination IP addresses Firewall Actions Port Connections. | |
| 8. Database Logs | <ul style="list-style-type: none"> User IDs Dates Times. | |
| 9. Electronic Messaging Logs | <ul style="list-style-type: none"> User IDs Dates Times Messages (including attached files) throughout entire conversations. | At least 6 months . |



9. Systems Acquisition, Development and Maintenance

Security Requirements



- Information security requirements specification for new information systems or enhancements to existing information systems
- Protecting application services information

Security in Development and Support Process



- Testing on new information systems or enhancements to existing information systems
- Secure development environment
- BCP update
- Supervising and monitoring the activity of outsourced development
- Acceptance testing by users or independent testers

10. IT Outsourcing

Information security in IT outsourcing



- Information security policy for IT outsourcing
- Addressing information security within the outsourcing agreement
- Measures for supervising the outsourcee to comply with the SEC requirement
- Incident response policy for the outsourcee
- Right to inspect operations of the outsourcee

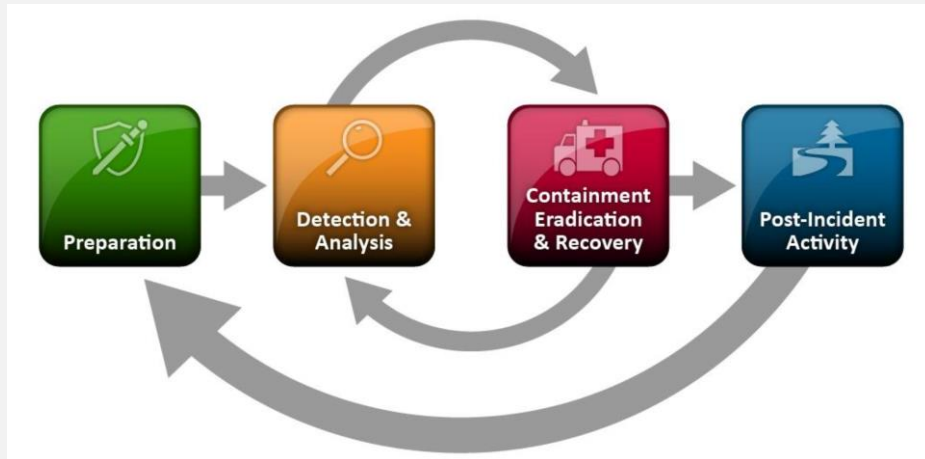
Supplier Service Delivery Management



- Monitoring and review of supplier services
- Managing changes to supplier services

11. Information Security Incident Management

- Incident management procedures
- Incident management responsibilities
- Reporting information security events
- Testing and review the incident management procedures
- Collection of evidence



NIST incident response process

12. Information Security Aspects of Business Continuity Management

- Planning information security continuity
- Implementing procedures, processes and controls to ensure the required level of continuity for information security
- Defining the recovery time objective (RTO) based on business impact analysis (BIA)
- Considering redundant information systems



Top 5 Common Findings



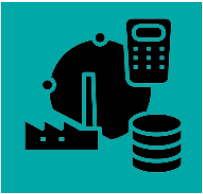
Top 5 common findings



การบริหารจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศไม่ครอบคลุมความเสี่ยงสำคัญ



ยังไม่มีการบริหารจัดการอุปกรณ์เคลื่อนที่อย่างเหมาะสม



ยังไม่ดำเนินการบริหารจัดการทรัพย์สินทางด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

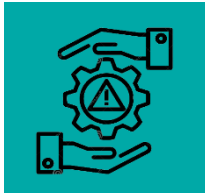


การตั้งค่ารหัสผ่านไม่สอดคล้องตามที่นโยบายกำหนด



ไม่ได้ดำเนินการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ และกฎไฟร์วอลล์อย่างเหมาะสม

Top 5 common findings



การบริหารจัดการความเสี่ยงทางด้านเทคโนโลยีสารสนเทศไม่ครบถ้วนตามที่นโยบายของบริษัทกำหนด



Risk Management
Policy & Procedure







1. การระบุความเสี่ยง
2. การประเมินความเสี่ยง
3. การควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้
4. การติดตามความเสี่ยง
5. กำหนดหน้าที่และความรับผิดชอบของผู้รับผิดชอบ



Board of Director



การประเมินความเสี่ยง

1. ความเสี่ยงในการเข้าถึงข้อมูลอย่างไม่เหมาะสม 
2. ความเสี่ยงในการไม่ปฏิบัติตามสัญญา 
3. ความเสี่ยงจากการใช้งาน Cloud Computing 
4. ความเสี่ยงในการใช้งาน Cryptographic key 

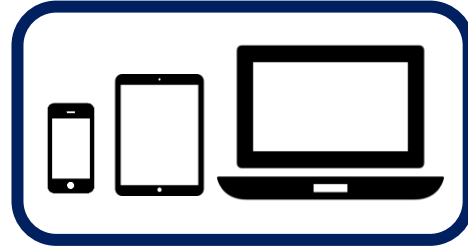
Top 5 common findings



ยังไม่มีการบริหารจัดการอุปกรณ์เคลื่อนที่อย่างเหมาะสม



BYOD Management
Policy & Procedure



Mobile phone, Tablet, Laptop

ไม่มีกระบวนการขอใช้งาน BYOD



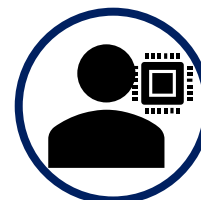
ไม่ได้ป้องกันการเข้าถึง Cloud Storage ส่วนตัว



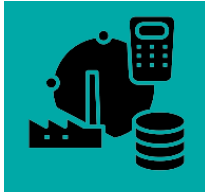
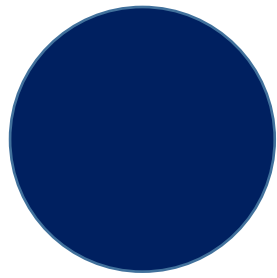
ไม่มีกระบวนการในการบริหารจัดการกรณีอุปกรณ์สูญหาย



ไม่ได้กำหนดให้ตั้งคำรหัสผ่าน



ไม่ได้ปิดสิทธิ์ Local Admin



ยังไม่ดำเนินการบริหารจัดการทรัพย์สินทางด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

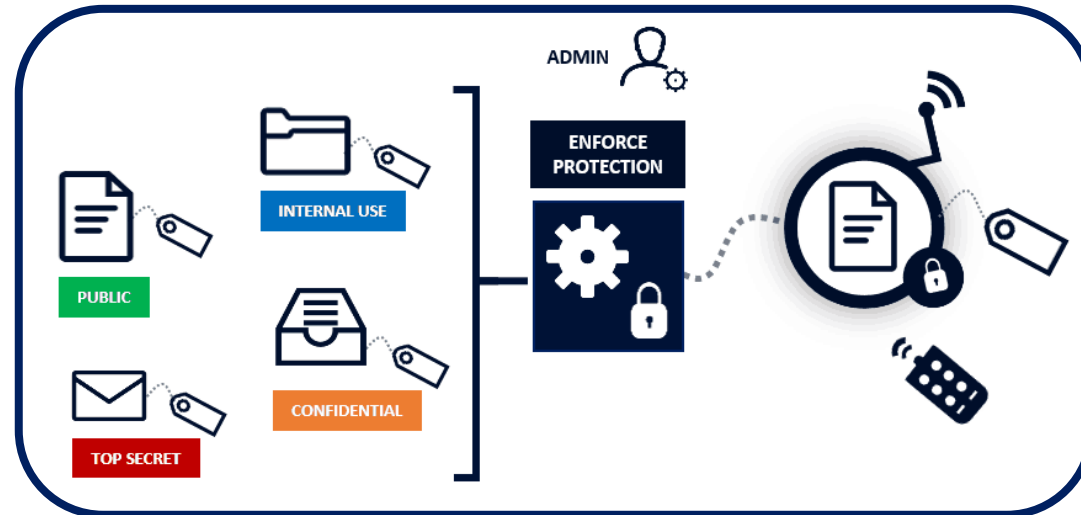


1. ทะเบียนทรัพย์สินสารสนเทศอุปกรณ์ (Hardware) ☒
2. ทะเบียนทรัพย์สินสารสนเทศระบบ (Software) ☐
3. ทะเบียนทรัพย์สินสารสนเทศข้อมูล (Data) ☐

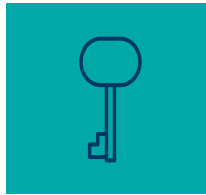
- ☐ ทะเบียนมีรายการไม่ครบถ้วน (เทียบกับรายการทางบัญชี)
- ☐ ไม่มีการทบทวนเป็นประจำ และรายงานไปยังผู้บริหาร

การจัดการทรัพย์สินสารสนเทศข้อมูล

- ☐ ไม่มีการจัดลำดับชั้นความลับข้อมูล
- ☐ ไม่มีการระบุเจ้าของข้อมูล
- ☐ ไม่มีการกำหนดแนวทางการจัดการข้อมูล



Top 5 common findings



การตั้งค่ารหัสผ่านไม่สอดคล้องตามทีนโยบายกำหนด

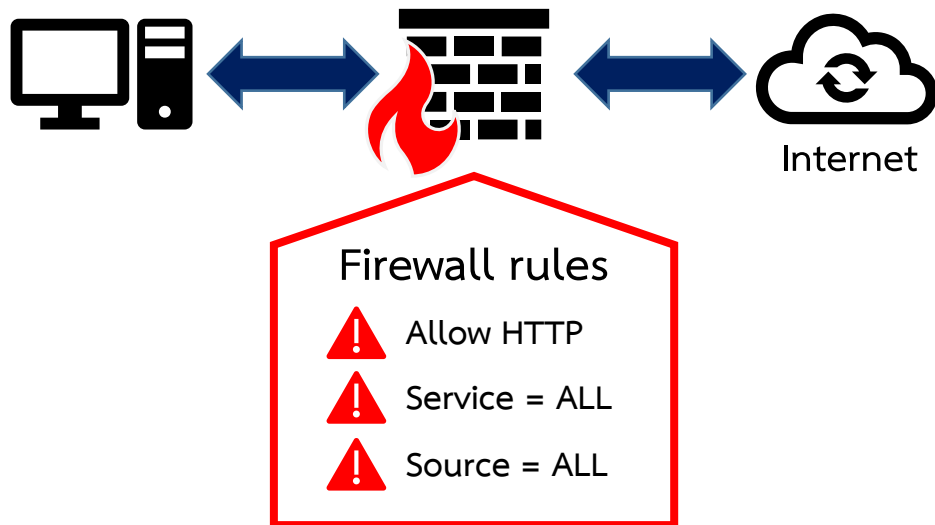
| รายละเอียด | การกำหนดค่าตามประกาศสำนักงานฯ | นโยบายรหัสผ่านที่บริษัทกำหนด | System 1 | System 2 | System 3 | System 4 |
|-----------------------|-------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------|---------------------|
| Password expiration | 180 วัน | 120 วัน | 120 วัน | 90 วัน | ไม่กำหนด | ไม่กำหนด |
| Password length | 6-8 ตัวอักษร | ขั้นต่ำ 10 ตัวอักษร | 6-8 ตัวอักษร | 12-16 ตัวอักษร | ขั้นต่ำ 6 ตัวอักษร | ขั้นต่ำ 12 ตัวอักษร |
| Password complexity | กำหนด | กำหนดให้ใช้ตัวเลขร่วมกับอักขระพิเศษ | กำหนดให้ใช้ตัวเลขร่วมกับอักขระพิเศษ | กำหนดให้ใช้ตัวเลขร่วมกับอักขระพิเศษ | ไม่กำหนด | ไม่กำหนด |
| Password history | 1 รหัสผ่าน | 5 รหัสผ่าน | ไม่กำหนด | ไม่กำหนด | ไม่กำหนด | ไม่กำหนด |
| Failed log-on attempt | ไม่เกิน 10 ครั้ง | ไม่เกิน 5 ครั้ง | ไม่กำหนด | ไม่กำหนด | ไม่กำหนด | ไม่กำหนด |

Top 5 common findings

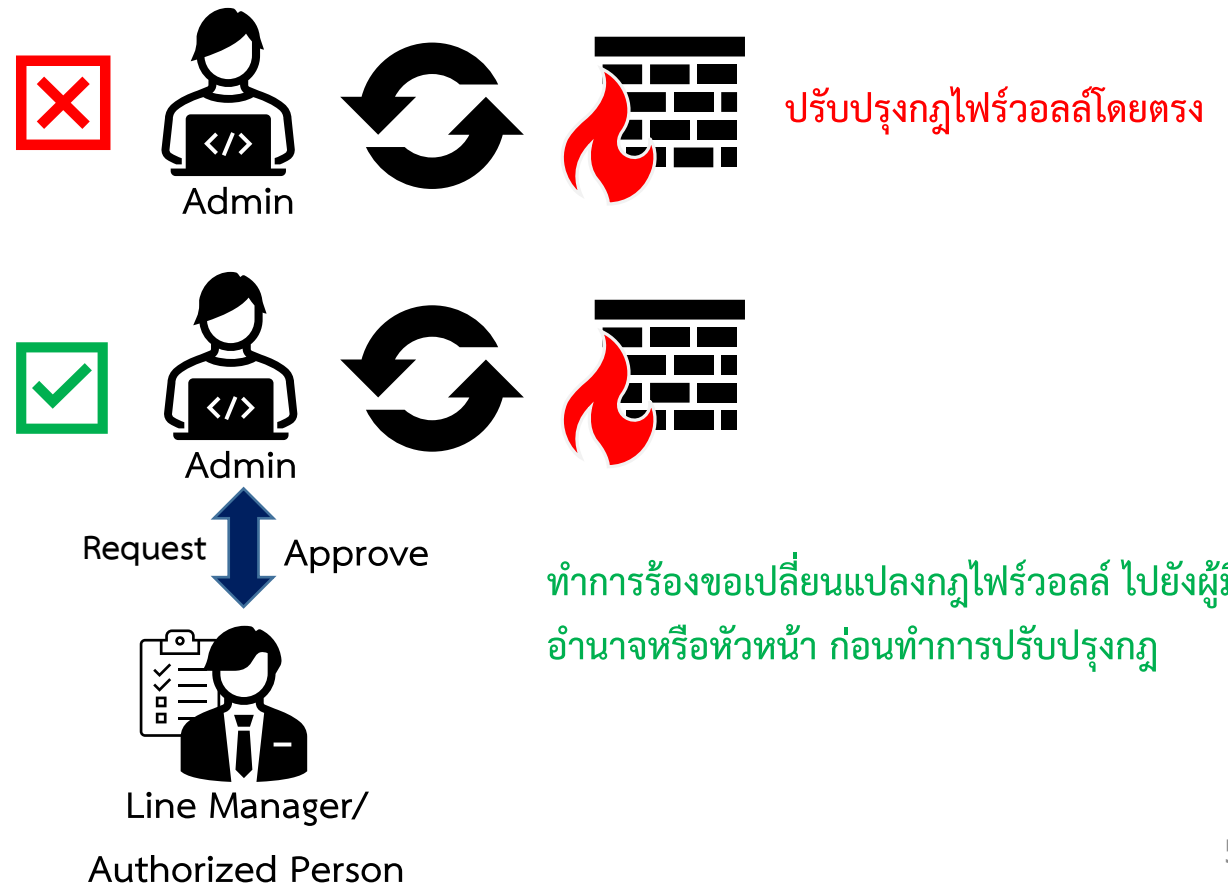


ไม่ได้ดำเนินการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ และกฎไฟร์วอลล์อย่างเหมาะสม

มีการใช้งานกฎไฟร์วอลล์ที่ไม่ปลอดภัย



ไม่มีการควบคุมกระบวนการตั้งค่ากฎไฟร์วอลล์



Q & A

