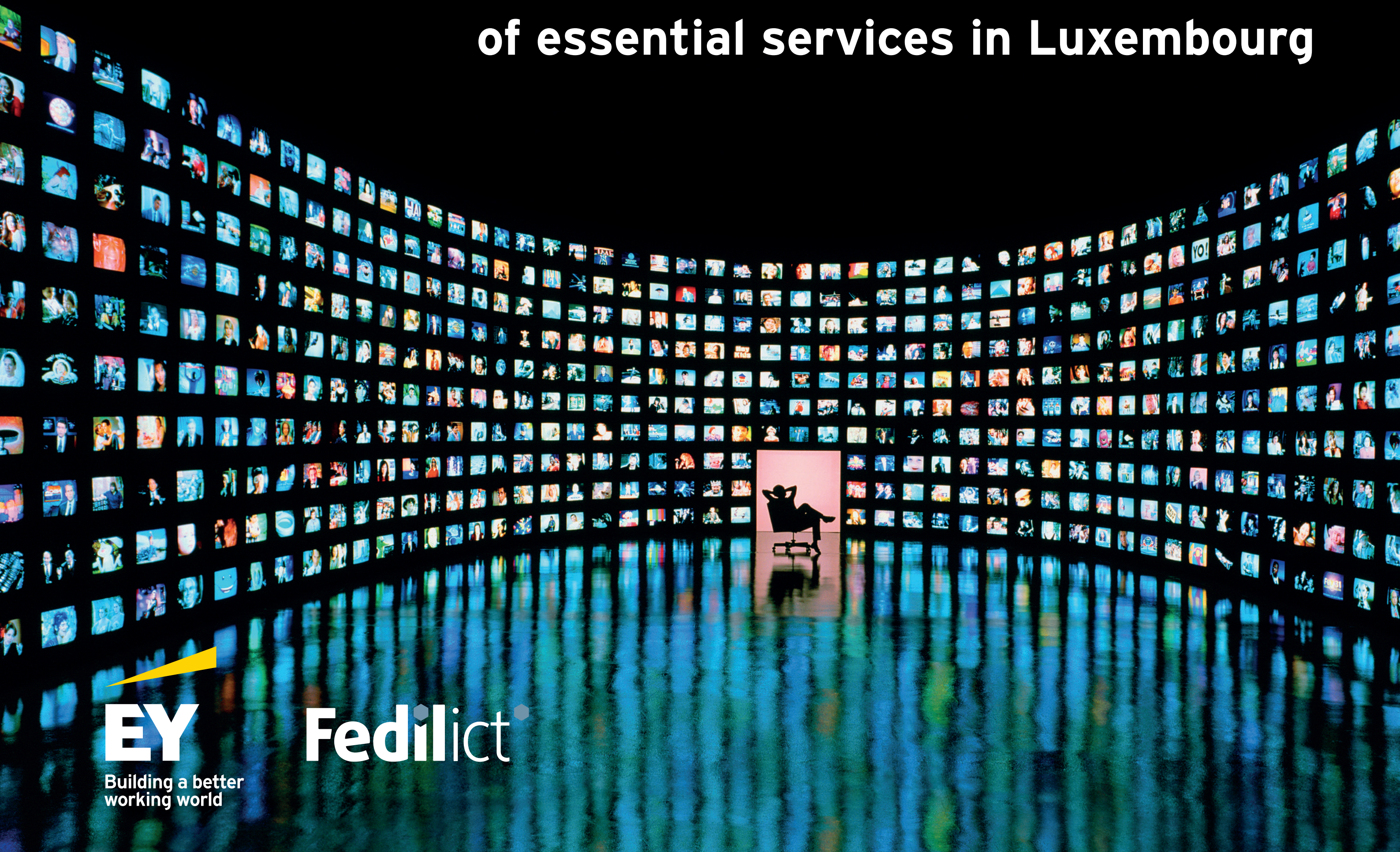
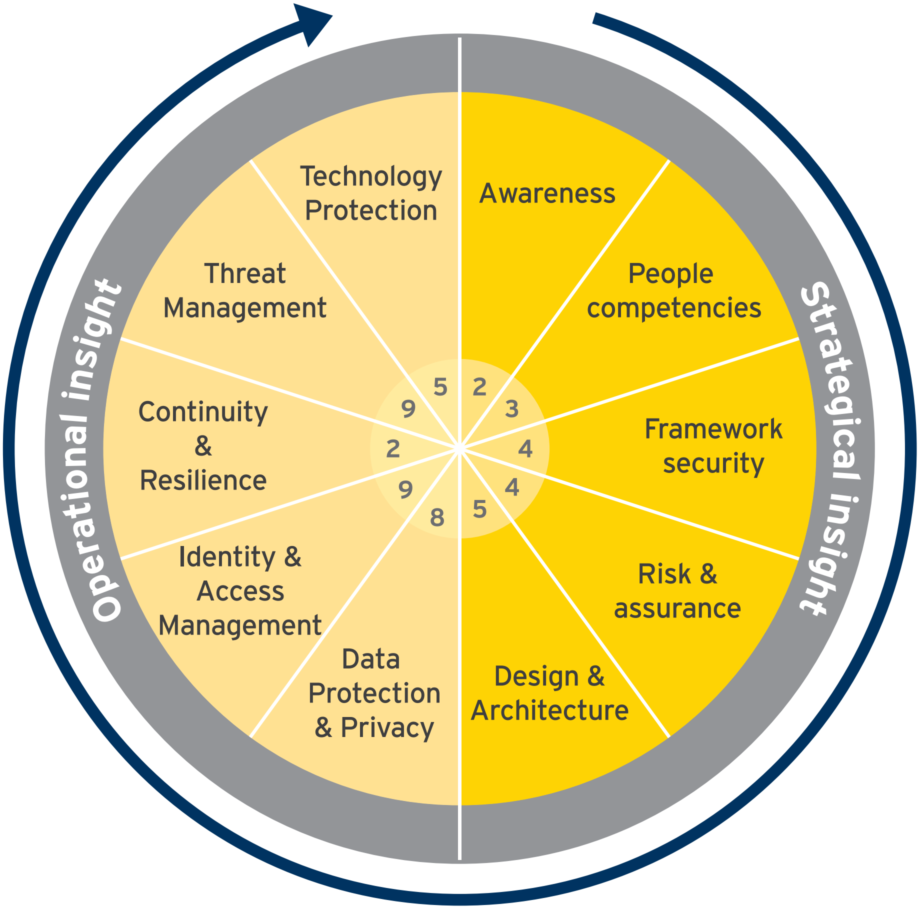
Hygiene security practices for providers of essential services in Luxembourg



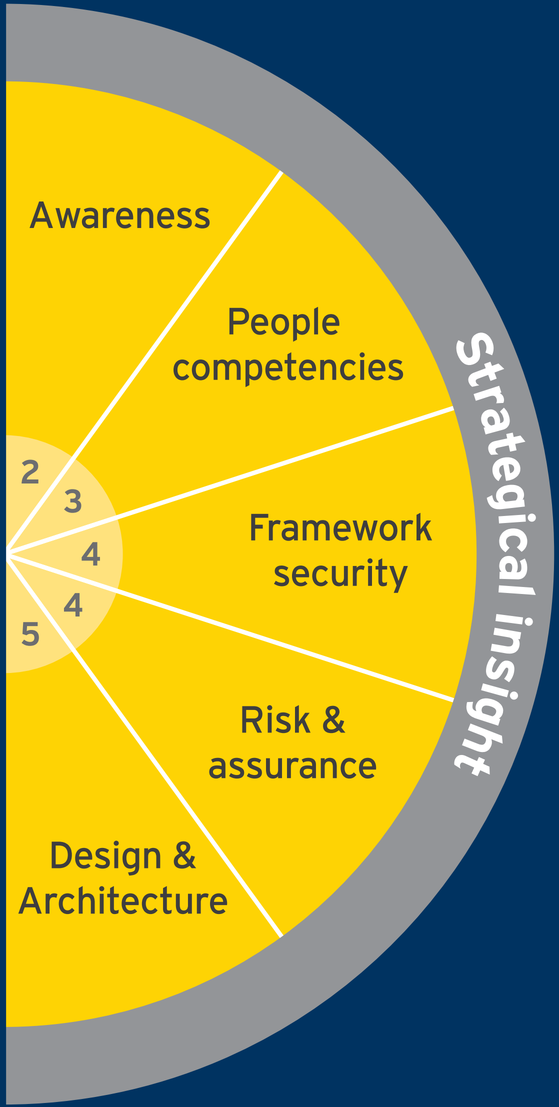
EY
Building a better
working world

Fedilict

A set of **security practices** was established to pave way for providers of essential services in their cyber security journey and to broadly strengthen the security footprint of Luxembourg.



Strategical insight



Awareness

People competencies

Framework security

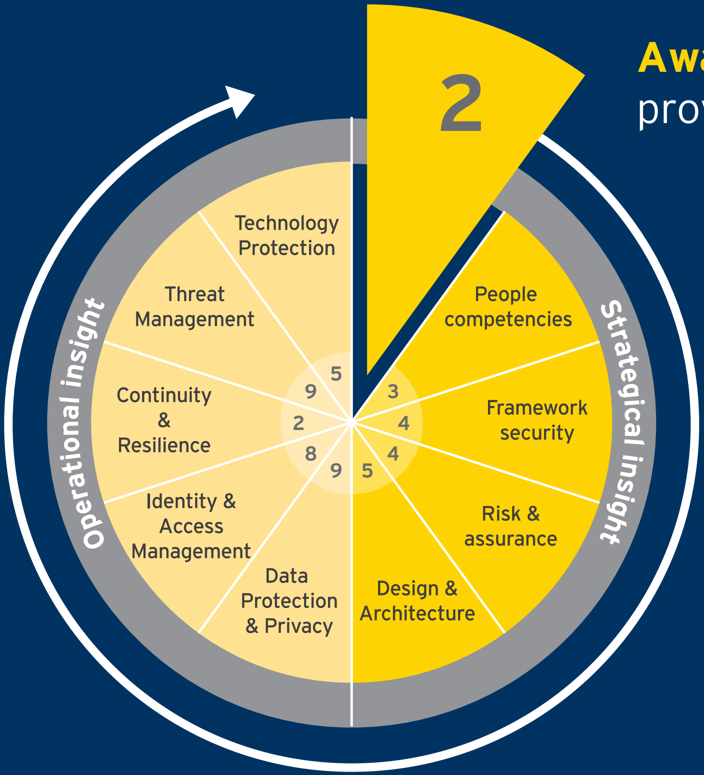
Risk & assurance

Design & Architecture

Strategical insight

Strategical insight

Awareness best practices for providers of essential services

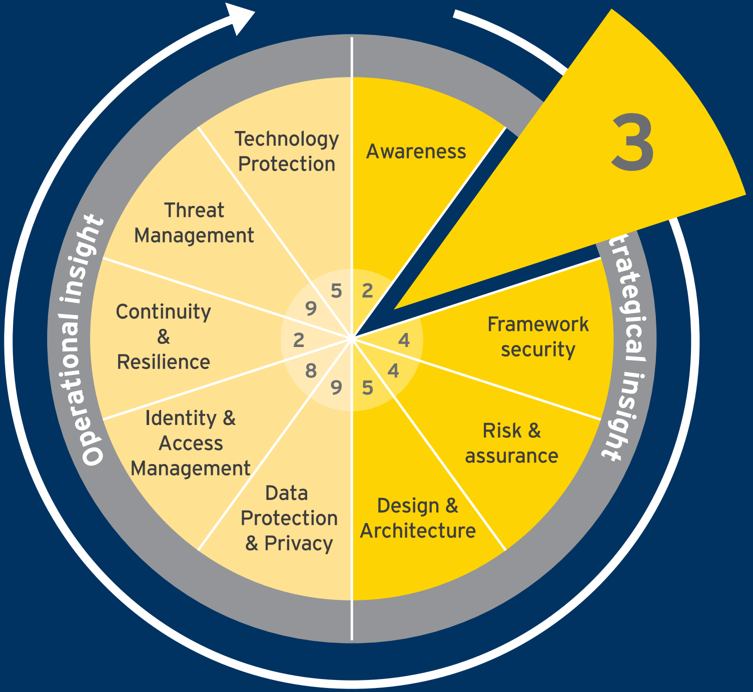


FUNCTIONAL CAPABILITY

Inform and train all employees on a real time basis (and based on user behaviour) of the hygiene rules of security.

TECHNICAL EXPERTISE

Provide an annual security and privacy development training (e.g. training on how to segregate sensitive data on a code level) to members of the IT support and development team.



People competencies
best practices for providers of essential services

Strategical insight

FUNCTIONAL CAPABILITY

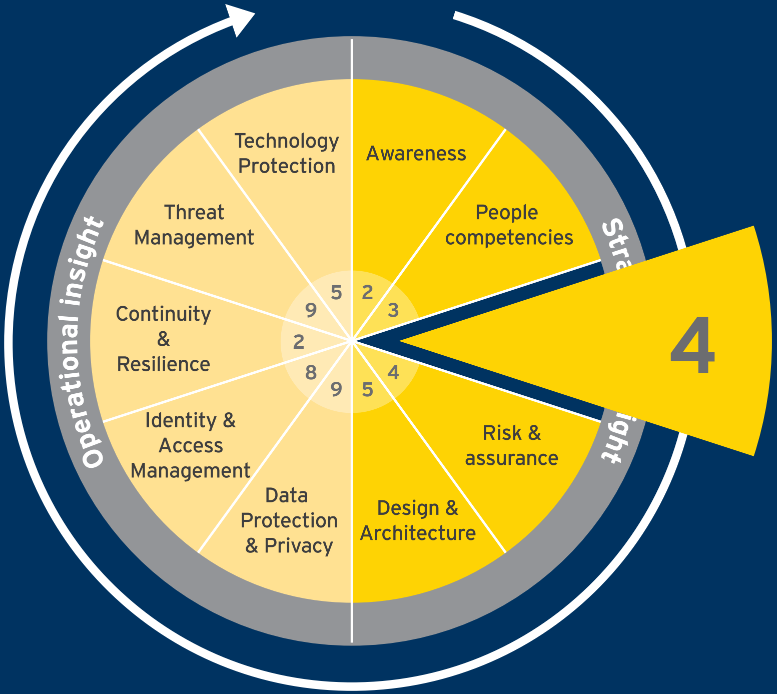
Designate through the executive management committee, a Chief Information Security Officer (CISO), ISMS roles and responsibilities.

Designate a mandatory CISO who is part of the top-management board and has a say in the decision-making.

TECHNICAL EXPERTISE

Ensure that the IT security function can rely on a qualified workforce of IT Security Professionals, with no relevant shortage and low turnover.

Strategical insight



Framework security best practices for providers of essential services

FUNCTIONAL CAPABILITY

Ensure that key security projects and programs are sponsored by at least one senior executive and provided by supporting resources and budget for treatment of main risks.

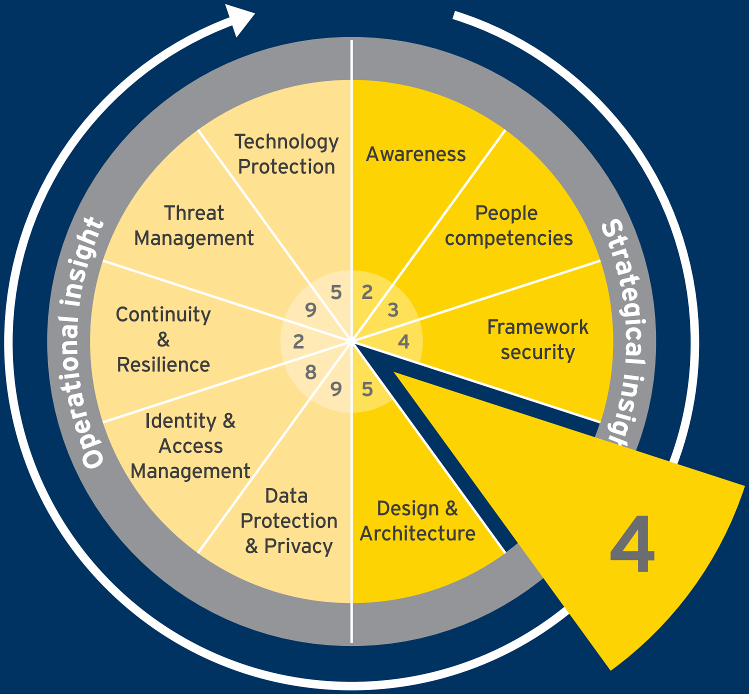
TECHNICAL EXPERTISE

Draft a brief, legible and functional corpus of Information Security policy and procedures, agree on the respective granularity of levels of guidance considered by the Management.

Perform an annual holistic assessment of the current IT and security policy and procedures to be in line with leading international best practices (e.g. ISO 27001/2, ITIL/ITSMF, CoBIT, NIST).

Incorporate penetration testing and organizational clauses in each contract with IT/Cloud/SaaS providers. Describe procedures for permanent controls in a security assurance plan, indexed to the contract including a reversibility clause.

Strategical insight



Risk assurance best practices for providers of essential services

FUNCTIONAL CAPABILITY

Ensure that at least one senior executive, who has a clear knowledge of his/her company on the protection/exposure level, has quarterly oversight and reporting from the information security function about security Key Performance Indicators/Key Risk Indicators.

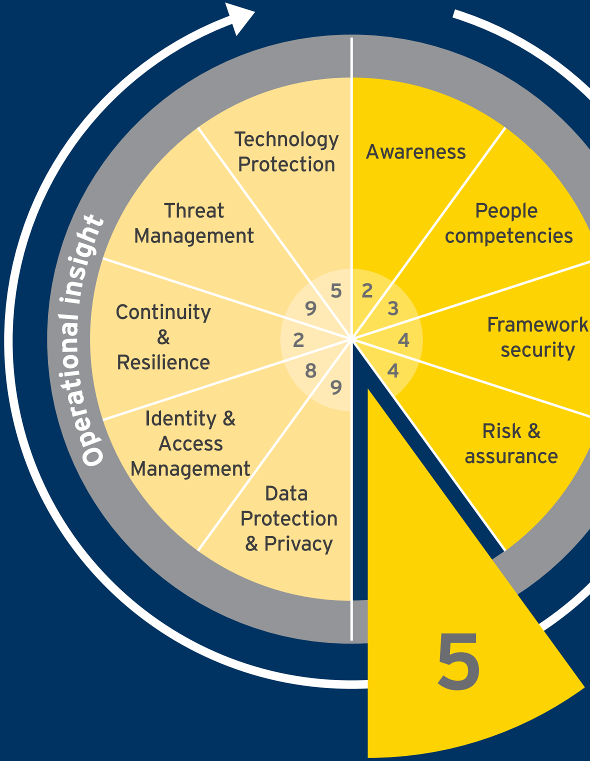
Ensure that residual risk is re-evaluated for each major updates of a system, and accepted by risk owner before go-live.

TECHNICAL EXPERTISE

Continuously conduct risk assessments and risk treatments (acceptance/mitigation) explicitly stated before go-live of a project.

Include concepts of “privacy by design” and “security by default” in each project design or evolution.

Strategical insight



Security architecture best practices for providers of essential services

FUNCTIONAL CAPABILITY

Maintain and review on an annual basis, as well as perform an inventory on the high-risk profile devices and critical information assets (applications, softwares, systems).

Establish periodic configuration audits and penetration testing of company managed mobile devices which have access to information systems (bear in-mind that access to information systems is not only limited to company managed devices).

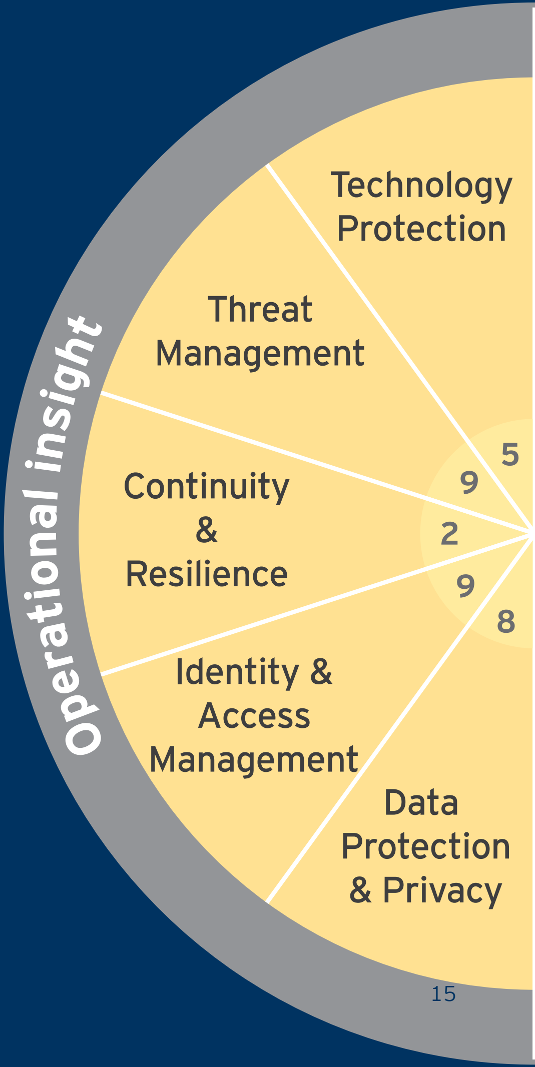
TECHNICAL EXPERTISE

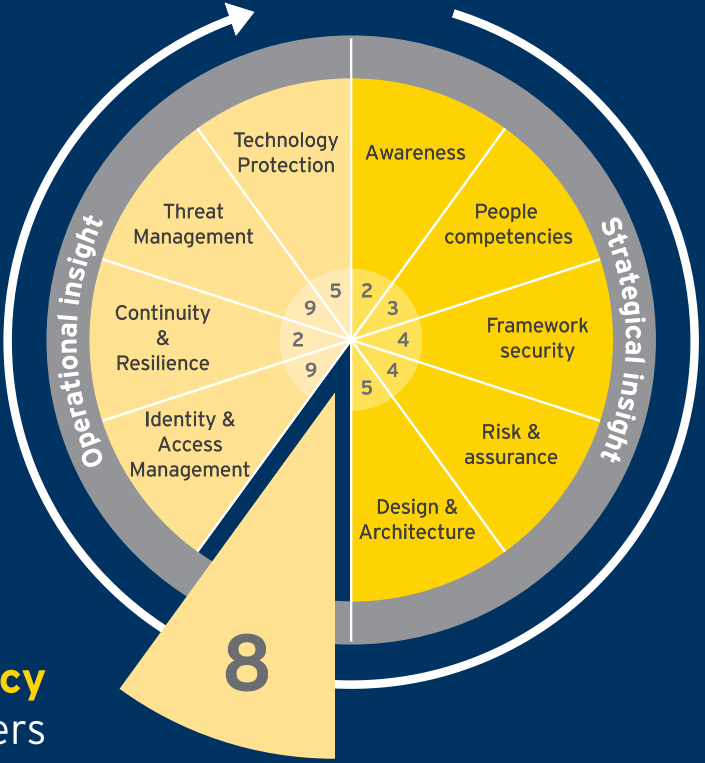
Only allow remote access to the corporate network, including network administration, from company-trusted equipment.

Deploy in a timely fashion all critical vendor patches and published security fixes on sensitive and/or web exposed workstations and servers.

Retrieve and revoke access to all mobile devices upon employee termination (e.g. laptops, phones, portable media).

Operational insight


Operational insight
Technology Protection
Threat Management
Continuity & Resilience
Identity & Access Management
Data Protection & Privacy
5
9
2
9
8



Operational insight

Data protection & privacy best practices for providers of essential services

FUNCTIONAL CAPABILITY

Classify your information in terms of availability, confidentiality and integrity and get explicit validation of classification results by data ownership.

Conduct privacy impact assessment for each new/evolution of business process, in order to address risk and security impact of breaches/incidents on personal data.

Establish privacy procedures describing normal use and information retention period of personal data in a clear and concise manner.

Validate each cross border transmission of personal data by the Executive Management, Legal and IT departments.

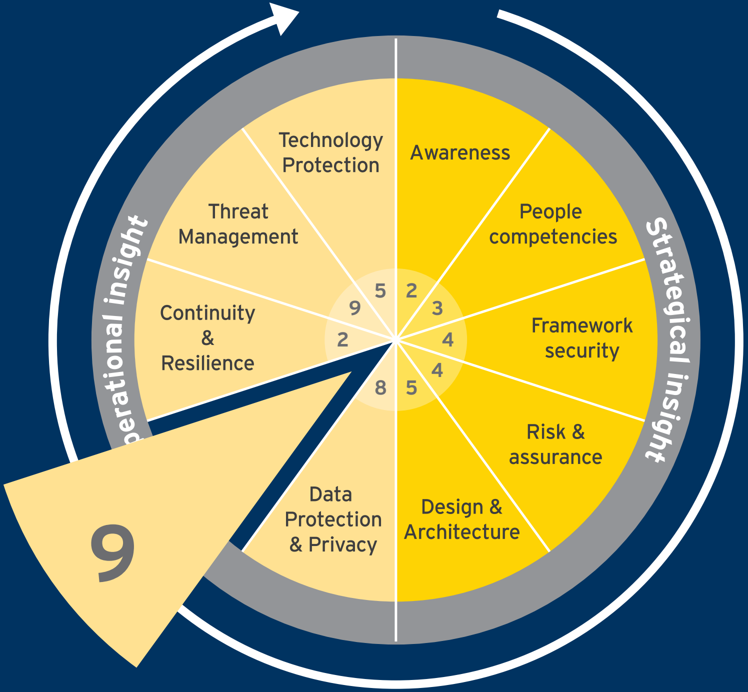
TECHNICAL EXPERTISE

Destroy physical assets (e.g. systems, hard disks, copiers, media, hard copy records, etc.) containing sensitive information when no longer used.

Implement secure/encrypted channels for transmission and storage of sensitive data (e.g. directly on hard drive). In particular, key encryption must be known by limited internal employees.

Technically prohibit the connection of removable media unless strictly necessary (e.g. USB locking on workstations).

Erase transmitted data once it is no longer required for the purpose for which it was transmitted.



Identity and access management best practices for providers of essential services

Operational insight

FUNCTIONAL CAPABILITY

Do not keep clear plaintext nor generic passwords to the information system in files or other systems (e.g. Database).

Implement procedures for provisioning/de-provisioning arrival and departure of users (staff, interns, ...).

Perform an inventory and regularly control privileged accounts to ensure that they are strictly reserved to appropriate users.

Conduct an annual segregation of duties review and access rights of business and IT users with access to sensitive resources.

Identify and restrict the list of employees with physical access via badge system to appropriate areas within the company.

Ensure that physical access is reviewed on an annual basis.

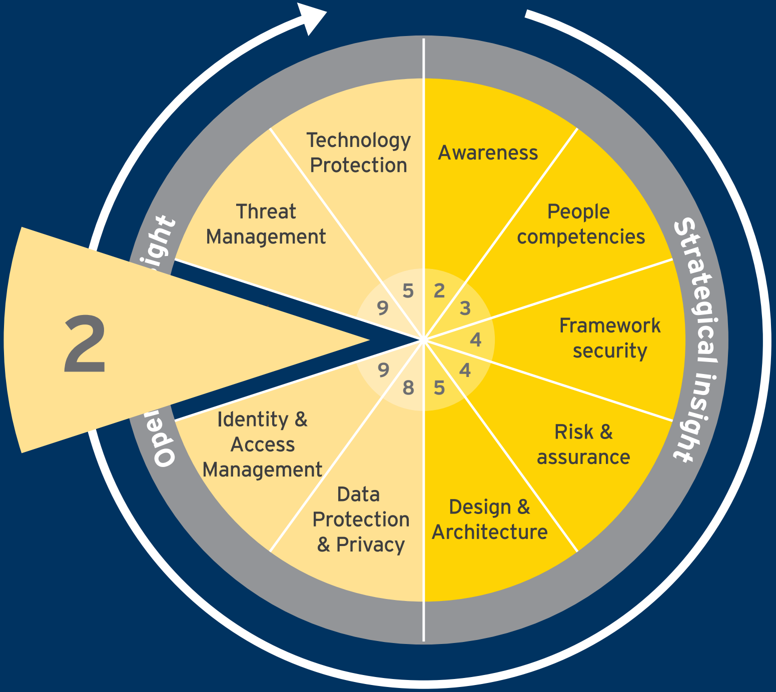
TECHNICAL EXPERTISE

Realize strong password checking for all business and IT/OT access on sensitive systems at minimum twice per year.

Use a “smart-card” based strong or at least multi-factor system authentication for users with access to critical and/or non-isolated resources.

Create unique identities and credentials, for all authorized internal devices and users, hosted in a non exposed central repository.

Business continuity best practices for providers of essential services



Operational insight

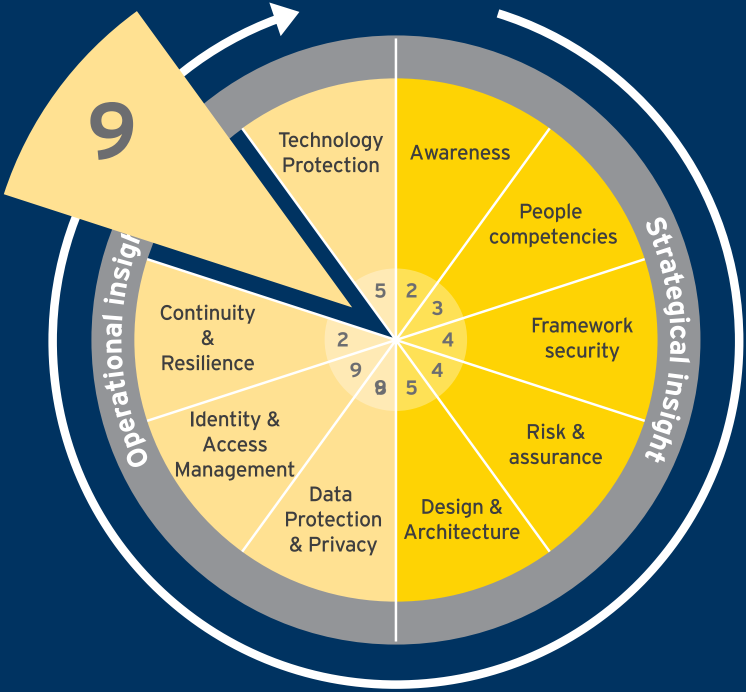
FUNCTIONAL CAPABILITY

Implement disaster recovery and business continuity plans which describe in particular how to back up critical business data. Ensure that these plans are reviewed and tested on an annual basis.

TECHNICAL EXPERTISE

Ensure that a Business Impact Analysis is conducted on an annual basis. Establish dependencies, critical functions and resilience requirements of critical services.

Cyber **threat management** best practices for providers of essential services



Operational insight

FUNCTIONAL CAPABILITY

Ensure that an incident response mechanism and scope of coverage (e.g. SIEM, CERT/CSIRT) are precisely defined and that the people involved are trained on an annual basis. A contact person should be identified.

Accomplish a regular manual analysis of log repositories monitoring for all critical components and sensitive assets of the infrastructure.

Include a description of how a machine is infected and describe if it has spread elsewhere in the network and what information may have been exploited for each treatment of threat. Ensure that the process is proactive rather than reactive.

Use the CIRCL framework for high risk alert notifications and collaboration.

TECHNICAL EXPERTISE

Schedule an annual incident response simulation to test readiness of staff and board.

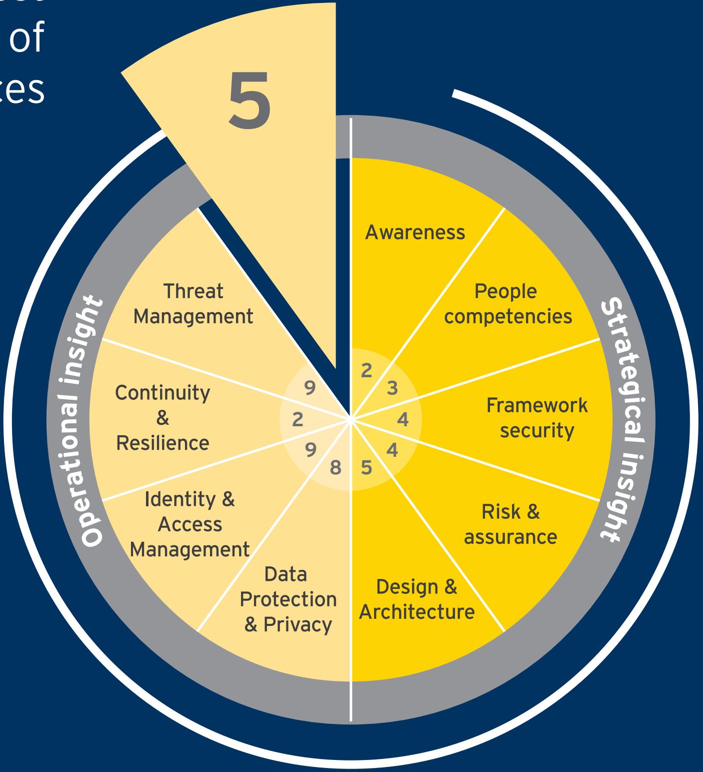
Record business and IT sensitive events in logs, which are protected and stored in a central repository for 3 years.

Limit usage of Wi-Fi. If the use of this technology cannot be limited, implement a partition of the Wi-Fi network from the rest of the network.

Develop and monitor a vulnerability management plan which is prioritized based on the main vulnerabilities after each IT audit (including penetration testing and organizational audits). Ensure that assessments are proactive rather than reactive.

Perform a penetration testing every year on critical and web exposed systems before migration to production.

Technology protection best practices for providers of essential services



Operational insight

FUNCTIONAL CAPABILITY

Define a patch management policy for critical systems in which sources, roles and responsibilities of vulnerability remediations are described.

TECHNICAL EXPERTISE

Conduct an annual network intrusion testing.

Create network segmentation for stations or servers that contain critical information for the company and resources reachable by devices not managed by the company.

Implement a malware protection policy that will contain guidance on obtaining up to date patch information.

Perform continuous code analysis and vulnerability assessments as part of the software development process.

Contacts

EY Building a better working world

35E avenue John F. Kennedy
L-1855 Luxembourg
+352 42 124-1

www.ey.com/lu

Fedil ict

7 rue Alcide de Gasperi
L-1615 Luxembourg
+352 43 53 66-1

www.fedil.lu

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

About FEDIL

FEDIL is a federation with entrepreneurial spirit, resolutely proactive and oriented towards the future. Our mission is

... to support our members of today and tomorrow during their decision-making process and development towards the future. To guarantee a highly qualified support, FEDIL constantly focuses on creating a dynamic and diversified network.

... to create the best synergies around developing projects of our members in Luxembourg and internationally,

... to promote a constructive dialogue with the stakeholders of our ecosystem in Luxembourg and internationally,

We want to accompany our members in the preparation of their future and thereby contribute to the sustainable growth of our country, to make Luxembourg the best place for business.

FEDIL works and speaks for more than 550 companies of all sizes and from all sectors. Despite the fact that all of these are very different, they all need the same basic conditions to be able to grow and thereby contribute to the prosperity of Luxembourg's ecosystem. Our program offers the conditions to help you achieve the goal of sustainable growth for your business.

Counselling and service offers of FEDIL towards its members, as well as the efforts of promoting industry, are organised on several axes at the crossroads of companies' interests on the one hand and national as well as international socio-economic realities on the other hand.