ISMS – Information Security Management System

(ISO/IEC 27001:2022)

AIBILI association for innovation and biomedical research on light and image

ISMS – Information Security Management System

Contents

Prepared by IT Infrastructure Manager: Engº Carlos Domingues

Reviewed and Approved by the Management Committee:

Profª Conceição Lobo, Dra Cecília Martinho, Prof. José Cunha-Vaz, Doutora Joana Tavares,

Doutora Inês Marques, Engº Hugo Morgado, Dr Paulo Barros, Dr Daniel Fernandes and Dra Rita Fernandes.

ISMS – Information Security Management System

Promulgation

AIBILI Board of Directors demonstrates the leadership and commitment with respect to AIBILI´s Information Security Management System (ISMS) and delegates in the President and in the Management Committee the formal approval of the AIBILI ISMS and related Policies.

AIBILI staff is responsible for the implementation, maintenance, and improvement of AIBILI ISMS.

Purpose

AIBILI ISMS – Information Security Management System is a strategic framework for governance, risk management and compliance to ensure privacy and data protection.

This document is intended to align strategical vision to operational actions, to ensure AIBILI activity in a continuous way, reducing the risk of security incidents and avoid resistance from end users or business units.

The document organization trends to follow GRC (Governance Risk and Compliance) principles with internal and external audits methodology integration.

This Information Security Management System is not intended to be a Business Continuity Plan document. AIBILI has a specific IT BCP & Disaster Recovery Plan. As said, this framework is focused on the security operations services and intents to align operational actions related to IT and data security and strategical vision for AIBILI.

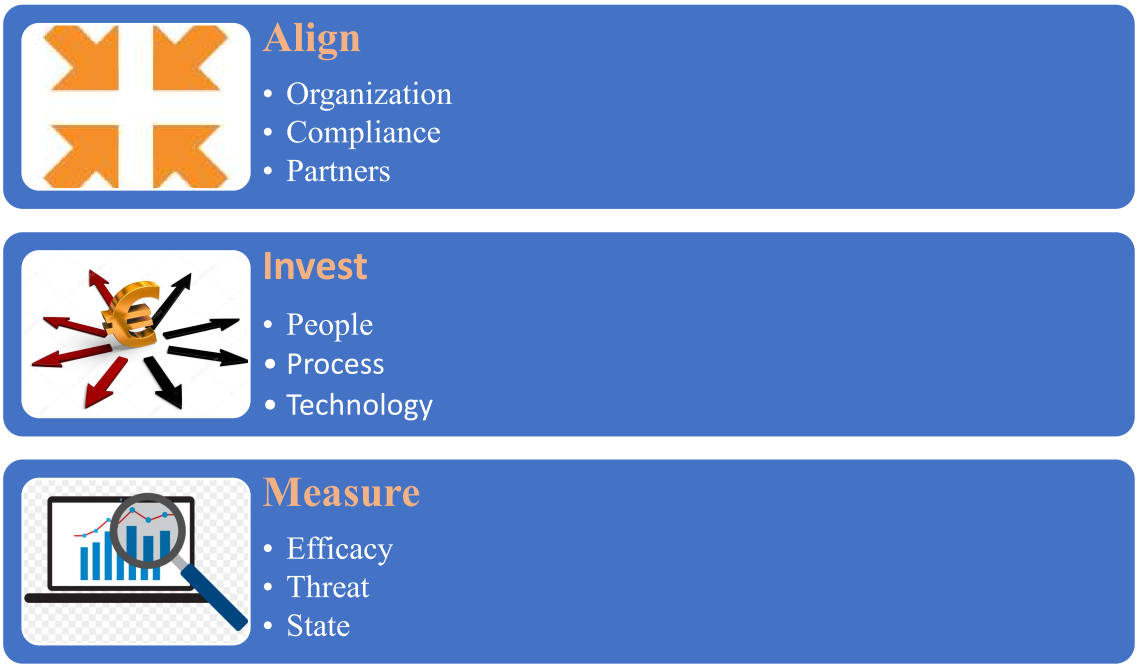
AIBILI has a Management Quality System integrated with different standards and rules, such as ISO 9001, requirements for Certification of ECRIN Data Centres when performing Data Centre activities, Principles of Good Clinical Practices whenever a clinical study is performed, Legislation applicable to the protection of personal data and the ISO/IEC 27001. The Quality Manual is available in AIBILI´s website https://www.aibili.pt/

1. Description

The operational alignment with business Unit's goals is fundamental for organization success. Therefore, it is important to identify and understand relevant threats and risks to the organization, which increases the chances of devastating security incidents. For this document purpose, security operations center (SOC) designation will be used to circumscribe all IT regular activities related to information security.

The core mission of any security operations center (SOC) is to defend an organization against the internal and external threat landscape, while accounting for the risk tolerance of the organization. However, planning high level security and risk management assessment are very complex and uncertain missions since the operational strategy depended on many possible scenarios. In 2019, the SANS Institute[1] conducted an SOC survey, Common and Best Practices for Security Operations Centers. The top challenges respondents reported were a lack of skilled staff (57%), with too many tools not integrated (43%), and a lack of processes (36%) that contribute to the issues that centralized security operations.

To avoid this situation, in the first approach, AIBILI will follow the Gartner[2] SOCTOM (Security Operations Center Target Operating Model) model, detailed in Figure 1.



Align

- Organization
- Compliance
- Partners

Invest

- People
- Process
- Technology

Measure

- Efficacy
- Threat
- State

Figure 1 - Security Operations Center Target Operating Model

This three-vector model Align-Invest-Measure will allow AIBILI to define an initial high-level strategy for governance, communication, and compliance directives, considering the risk assessment, investment needs, indicators and expected results. The main goal is to address the major security properties: Confidentiality, Integrity, and Availability.

On the other hand, this model should be complemented with specific preventive, detective, and corrective actions, to fulfill the continuous time evaluation.

[1] https://www.sans.org/
[2] https://www.gartner.com/en

1.1. Information Security Management System Scope

The scope of the Information Security Management system is documented in the Statement of Applicability, classified as restricted and confidential information.

1.2. Leadership and Commitment

Top management is committed to providing effective information security and, through the implementation of this ISMS, has taken steps to:

a) ensure the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) ensure the integration of the information security management system requirements into the organization's processes;

c) ensure that the resources needed for the information security management system are available;

d) communicate the importance of effective information security management and of conforming to the information security management system requirements;

e) ensure that the information security management system achieves its intended outcome(s);

f) direct and support persons to contribute to the effectiveness of the information security management system;

g) promote continual improvement; and

h) support other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

1.3. Context of organization – Security roles and responsibilities

The Information Security organization revolves around an Information Security Management System (ISMS) and a series of roles and responsibilities involved in its scope, namely the Management Committee, IT/DC Director and the IT Infrastructure Manager, Financial Manager and Quality Manager. The IT/DC organizational Flowchart and the Job descriptions identify the IT/DC Unit staff involved in the "Network, Infrastructures and Data Centre Security" as the AIBILI´s security operational center.

General internal roles and responsibilities related to security roles and responsibilities are assigned in the specific Job Description for each position.

The AIBILI Management Committee including the IT Infrastructure Manager are responsible for approving this ISMS. The IT/DC Director and the IT Infrastructure Manager together with the Quality Manager are responsible for ensuring the ISMS revision. The IT/DC Director and the IT Infrastructure Manager are responsible for maintaining this ISMS.

It is very important to ensure a clear understanding of roles, responsibilities, expectations, and dependencies between the security operational center "Network, Infrastructures and Data Centre Security" and AIBILI Units.

For each critical information system, AIBILI Information system characterization should be used to identify Informatic Security Manager but also Key User and Information System Administrator assignments. Moreover, for each personal data processing it will be identified each responsible for personal data protection. This segregation of duties will prevent any misuse of AIBILI assets and avoid the "one person full power" to control an activity, information system or sensitive asset.

Ref. Docs: PGQ 03- Human Resources Management, Job Description (Imp.03-1-5); PGQ 08- Personal Data Processing, Personal Data Processing Activities Log (Imp.08-01-01)

1.4. Context of organization – Relevant Internal and External requirements for Information Security Management

AIBILI determines external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system. This analysis is documented and approved by the Management Committee in the "Context of the Organization - SWOT ANALYSIS- Strategic Direction, Objectives and actions", which is reviewed at least annually or whenever justified.

Ref. Docs: PGQ 01- Strategy Management, Planning and Performance Control; Context of the Organization - SWOT ANALYSIS- Strategic Direction, Objectives and actions.

1.5. Context of organization – Stakeholders (Interested Parties)

AIBILI determines the interested parties that are relevant to the information security management system, their relevant requirements and those that will be addressed through the information security management system. This analysis is documented and approved by the Management Committee in the "Context of the Organization, Relevant QMS Stakeholders", which is reviewed at least annually or whenever justified.

Ref. Docs: PGQ 01- Strategy Management, Planning and Performance Control; Context of the Organization, Relevant QMS Stakeholders

1.6. Context of organization – Legal, Regulatory and contractual requirements

It is very important to identify and ensure compliance with legal and regulatory requirements, determine requirements for compliance and/or industry security frameworks and how they will affect the security development and roadmap. This requires alignment with IT, AIBILI Personal Data Protection Committee (CPDP), Unit risk matrix and legal issues to ensure that all is meeting regulatory or industry requirements.

Partners identification is very important to understand their needs and expectations, establish common objectives and ensure there is strong communication around bidirectional change regarding material changes to agreements, architecture and eventually delivery of services.

Communicating and aligning with business leaders, organizational peers, compliance requirements and partners will enable AIBILI to reduce friction and increase operational effectiveness earlier in the security development cycle. Defining a roadmap requires an understanding of the current state and is essential for security operations creation, function and maturation.

This analysis is documented and approved by the Management Committee in the “Context of the Organization, Relevant QMS Stakeholders”, which is reviewed at least annually or whenever justified.

The data communicated is critical, and how it is communicated is even more vital to security operations reputation and validation. This is not just a security issue, but a strategic need to make documented decision.

The strategy to produce value in “the security communication” at AIBILI should be embraced according to the Gartner Model:

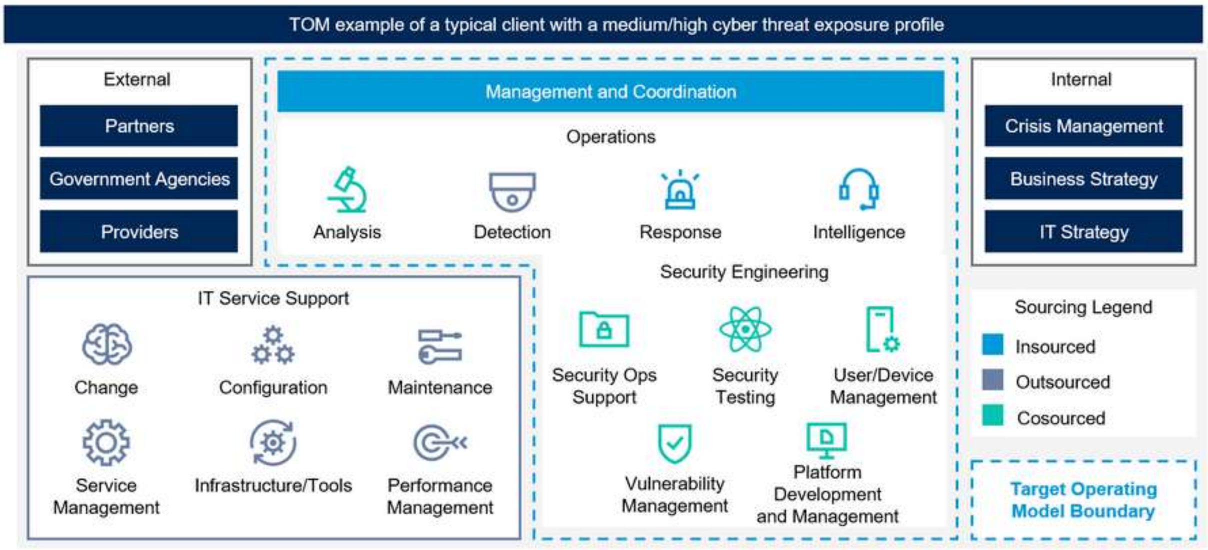
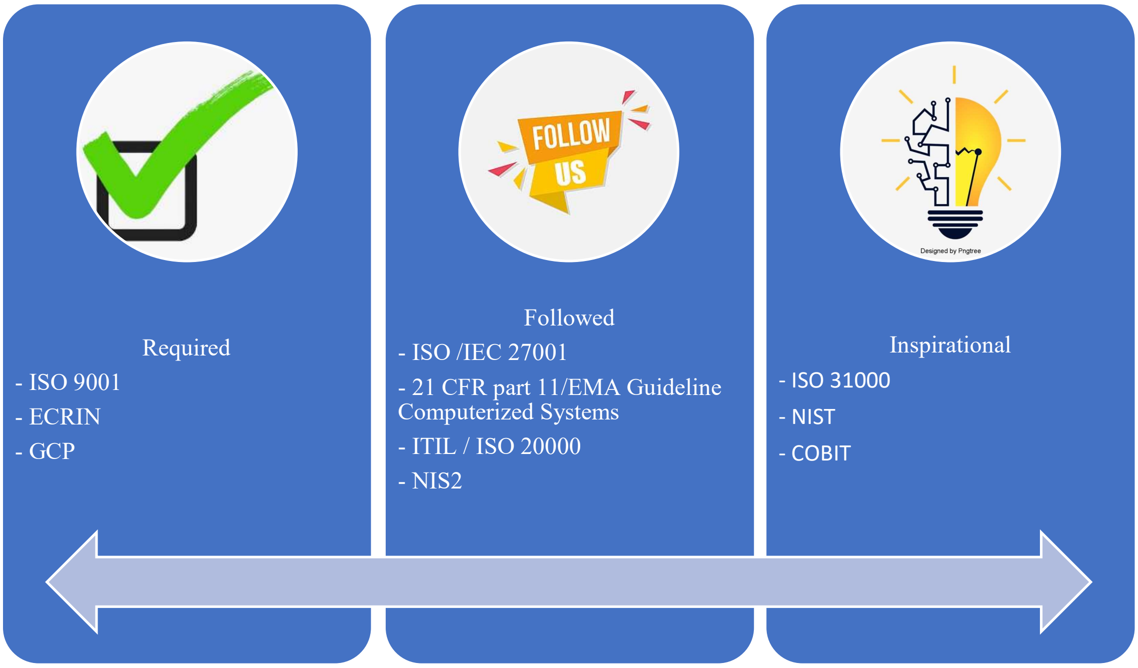


Figure 2 – Communication layers (Gartner model)

There are several differences between strict requirements, followed frameworks and inspirational contexts. As a certified institution, AIBILI will follow strictly ISO 9001 quality practices, ECRIN Data Centre and GCP[3] methodology. Those are mandatory and required in any of AIBILI’s certified activity. AIBILI will also follow other relevant standards, guidelines and regulations (e.g. ISO/IEC 27001, EMA Guidelines for computerized

[3] https://www.ema.europa.eu/en/

Systems, FDA 21CFR part 11[4] ,and other IT good practices (as ITIL[5] or ISO20000[6]) when performing Data Centre activities. Last, but not least, AIBILI has identified other referential that will be used, customized, and implemented as part of the implemented standard operational procedures, as reflected in the next figure.



Required
- ISO 9001
- ECRIN
- GCP

Followed
- ISO /IEC 27001
- 21 CFR part 11/EMA Guideline Computerized Systems
- ITIL / ISO 20000
- NIS2

Inspirational
- ISO 31000
- NIST
- COBIT

Figure 3 – Compliance model

AIBILI Quality Management Unit will be responsible for certification and compliance processes.

Ref. Doc: PGQ 01- Strategy Management, Planning and Performance Control; Context of the Organization, Relevant QMS Stakeholders

1.7. Secure System Principles

AIBILI should invest in people, security services and technology to operate the security operational center equally as increases the project IT dependency. It is critical to give IT personnel a sense of ownership in the operations

[4] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application[5]https://www.itlibrary.org/
[6] https://www.iso.org/standard/70636.html

and security program, ensuring there is a dedicated budget for recruitment, retention, and training of security expertise.

AIBILI should use a pragmatic and realistic selection process for security tools, based on cost, threat modeling, and identified business risks. Layering multiple overlapping tools might give a stronger barrier, reducing the risk but will naturally increase costs. Therefore, this should be a balanced commitment among involved parties and documented in AIBILI's pluriannual investment plan.

The principles that must be respected, based on the basic dimensions of security, are the following:

• **Confidentiality**: property by which the information managed by Information Technology and Systems can only be accessed by whoever is authorized to do so, subject to identification, at the authorized time and by the authorized means.

• **Integrity**: property that guarantees the validity, accuracy, and completeness of the information managed by Information Systems and Technology, its content being that provided by those affected without any type of manipulation and allowing it to be modified only by whoever is authorized to do so.

• **Availability**: property that can be accessed and used at agreed intervals. The information managed by Information Systems and Technology is accessible and usable by authorized and identified customers and users at all times, guaranteeing its own persistence in the event of any foreseen eventuality.

Additionally, given that any Information Security Management System must comply with current legislation, the following principle will apply:

• **Legality**: in reference to compliance with the laws, rules, regulations, or provisions that govern Information Systems and Technology, especially regarding the protection of personal data.

1.7.1 Internal and external security audit

AIBILI must guarantee and verify, through internal and external security audits, the degree of compliance and the correct compliance and operation of the ISO/IEC 27001 standards and guidelines of this ISMS and related documents, taking responsibility for compliance with the corrective measures that may have been determined for the purposes of continuous improvement. For security operational purposes, independent audits are necessary to be possible to confirm that AIBILI is compliant with some of these standards or frameworks. This audit should follow ISO/IEC 27001 standards and should be performed by a qualified auditor.

For the internal audit, the internal general procedure PGQ10 – "Internal Audits" will be followed, apart from the compliance requirements, the technical controls from Annex A – "Information security controls reference" from ISO/IEC 27001 standards should be used, as reference. This internal audit may also be performed by external auditors, as a previously qualified vendor, according to PGQ 10 and IT 04-3 – "Qualification and Evaluation of External Suppliers."

AIBILI external audit will only be developed for certification or compliance with required or followed frameworks by other interested parties (e.g. customers, etc.).

Ref. Docs: PGQ10 – Internal Audits; IT 10-1 – Quality Internal Audits; IT 04-3 – Qualification and Evaluation of External Suppliers.

1.8. Risk management

Information Security Management within the context of Information Systems is risk-based, in accordance with the international standard ISO/IEC 27001 and ISO 9001.

It is articulated through a general assessment and management of the risk, which can potentially affect the security of the information pertaining to the services provided. The following information must be considered in the risk management methodology: 1) Acceptable level of risk; 2) Types of threat and risks; 3) Methodology adopted; 4) Classification for use of probability and impact; 5) Criteria used for the asset to be subject to the risk analysis process; 6) Risk management responsibilities; 7) Controls to be used for the risk treatment plan.

It generally consisting of:

- Identification of threats that will take advantage of vulnerabilities in the Information Systems that support, or on which the information security depends.
- Risk analysis based on the consequences if the threat materializes and the probability of its occurrence.
- Assessment of the risk against a previously established and approved level of risk
- Dealing with the risk through appropriate controls or safeguards.

This process is cyclical and must be carried out periodically, at least once every year or whenever justified. An owner will be assigned for each identified risk, and multiple responsibilities may fall on the same person.

Ref. Docs: IT 01-3 – Formalization of Service Provision; IT 19-1- Management of Data Centre Services; Risk Log (Imp. 01-3-4).

ISMS – Information Security Management System

1.9. Security policy and objectives

AIBILI should continuously assess, measure and understand the asset value and risk to determine where the security operational team is on the correct roadmap journey, according to its functional and operational goals:

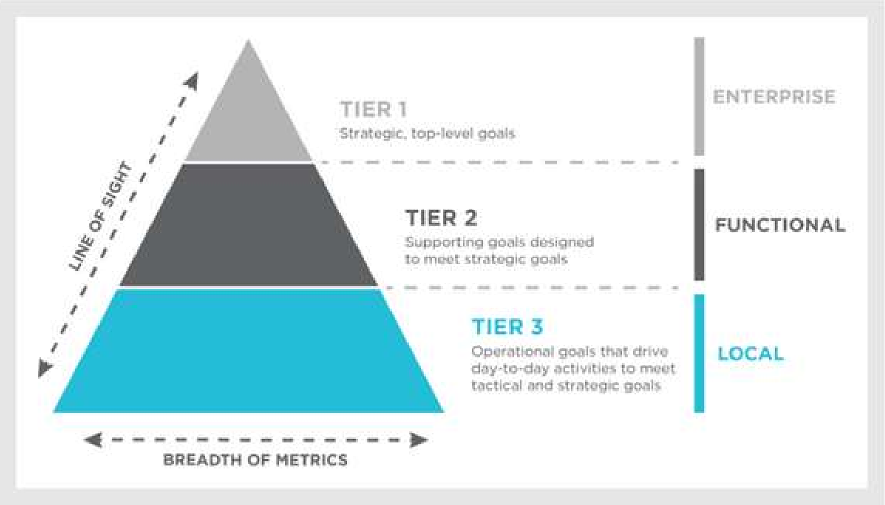

LINE OF SIGHT
TIER 1
Strategic, top-level goals
ENTERPRISE
TIER 2
Supporting goals designed to meet strategic goals
FUNCTIONAL
TIER 3
Operational goals that drive day-to-day activities to meet tactical and strategic goals
LOCAL
BREADTH OF METRICS

Figure 4 – Metrics and Reporting Hierarchy[7]

AIBILI has defined an Information Security Policy, strategic/global goals, as well as goals on a functional, local and operational level. AIBILI has established information security objectives consistent with the Information Security Policy. These objectives, as well as specific measurements are defined in the ISMS Objective and Metrics. Process Owners are assigned responsibility and authority for measurement collection and reporting. This analysis is documented and approved by the Management Committee during the Quality and Information Security Management System Review Meeting (annual meeting).

Information Security Policy

The Information Security Policy is segregated into a set of policies oriented towards information security, where each policy must have its classification according to its purpose (see section "Related Documents). Each policy should be defined with business requirements, relevant laws and regulations. The Information Security Policy expresses management concerns and establish the main objectives for information security management, considering AIBILI's requirements, mission and objectives. All documents within the scope of information security (policies, procedures and standards) are reviewed at planned intervals, at least once a year or when

[7] https://www.scottmadden.com/insight/security-operating-model-strategic-approach-building-secure-organization/

changes occur and are dully communicated to whom maybe concerned (e.g. employees and other interested parties (e.g. vendors/suppliers, Clients, etc.)).

Ref. Doc: IT 01-2- Planning, control and Revision by the Management Committee, ISMS Objective (Imp. 01-2-6) and Metrics (Imp.01-2-7); PGQ 01- Strategy Management, Planning and Performance Control; Context of the Organization - SWOT ANALYSIS- Strategic Direction, Objectives and actions.

1.10. Inventory of Assets

AIBILI asset documentation is distributed and stored on different platforms and locations. For IT assets, GLPI is used to document the required information for the user service desk. Other information (financial, logistics and contracts) are stored by each Unit or by Financial (SA) Unit (for instance, the institutional number of asset).

Critical assets (for Data Centre Services) are documented on the IT security management platform - MICKEY.

Ref. Doc: IT 05-1 - Documented Information System; IT security management platform - MICKEY

1.10.1. Acceptable use of Assets

AIBILI employees are responsible for ensuring compliance with the operational rules established and communicated in the intranet - Filedoc, specifically “ISMS Operational Rules”.

Also, they are committed to this Information Security Management System (ISMS) and to escalate any anomaly or violation of these rules and procedures:

- It is not allowed to connect any equipment not belonging to AIBILI to the corporate network and systems (e.g.: laptops, switches, routers, wireless routers) except in relation to the wireless network for visitors.
- All AIBILI equipment must be inventoried by financial services with a unique identification code (among the respective serial number). The IT team registers and updates the list of the IT equipment / assets in GLPI to provide effective helpdesk.
- Any unauthorized connection to AIBILI´s network and systems may be disconnected without notice; Any exception must be previously authorized by the IT security team.
- Users with authorized access to AIBILI´s equipment, systems and networks have a duty to protect them from unauthorized access and misuse.
- It is the responsibility of all users to ensure the confidentiality of information that is on removable storage (media) regardless of its classification.

- AIBILI equipment's are available only for work purposes except Wireless Guest network that is available for internet access to be temporarily used.

Ref. Docs: ISMS Operational Rules.

1.11. Access control Policy

The request for access to rooms, systems and software must be approved by the Unit Director, using IT Helpdesk, FILEDOC or other approved mechanism according to the related internal procedures.

Ref. Docs: IT 03-1 – "Recruitment and Integration of new employees"; IT 06-2 – "Restricted access"; IT 03-3 – Human Resources - Management of Competences; IT 19-3 – "Security and Access Management".

1.12. Operating Procedures for IT Management

More than written policies, the management and use of best practices should be verified constantly, in the daily basis operations. Therefore, continuous support and on-job training should be in place to ensure technicians are using the best practices in the management activities.

IT management procedures might include but are not limited to:

- Systems Administration and Delegation of Competencies
- Software and System Installation, management and access
- Network management and VLAN segmentation
- Network Shares and encryption
- Backup management
- Service Desk
- Antivirus and update services
- Intrusion detection and response
- Monitoring and alarmistic management
- Printing and paper document management

Ref. Doc: IT 06-05- Accessibility, Management and Maintenance of the IT Network

1.13. Supplier security policy

AIBILI has a formal qualification procedure, to identify and select suppliers. This procedure defines the requirements associated with the qualification and periodic evaluation of AIBILI's external suppliers. When applicable, security requirements and tests might be included,

These requirements and tests will depend on the vendor/supplier risk assessment, the information required, and the product/service provided.

Ref. Doc: IT 04-03 – "Qualification and Assessment of External Suppliers/Vendors"

1.14. Business Continuity Plan

AIBILI Business Continuity Plan and Disaster Recovery documents communication responsibilities and channels in case of incident, crises or disaster. This is well defined on PGQ19 – "DC activities", IT 19.4 – "Business Continuity Plan and Disaster Recovery". AIBILI understands that RPO and RTO are relative to specific pre-established SLAs (either from vendors and also for clients) and they should always be documented in specific documents for each study or protocol. By default, for regular projects the maximum RPO will be 24 working hours and the RTO should be less than 3 working days.

1.15. Continuous improvement

As said before, when it comes to managing AIBILI cybersecurity performance, a risk-based and outcome-driven approach should be taken. To reduce cyber risk, targeted measurement, continuous monitoring, detailed planning and forecasting efforts should exist. To support this continuous cycle, AIBILI developed a web platform - MICKEY, that addresses:

a) Assets, including their lifecycle (validation, production and retirement).
b) Security agents applied or related to any critical asset.
c) Critical data stored or processed by assets.
d) Risks, vulnerabilities and mitigation controls.
e) Incidents.

This continuous improvement cycle is fully supported by ISO/IEC 27001 and ISO 9001 requirements, terminologies and recommendations and also follows the internal procedure PGQ07 – "Non-Conformities and Improvement" where applicable.

Ref. Docs: PGQ07 – "Non-Conformities and Improvement; MICKEY

1.16. Institutional Communication between AIBILI and employees and other interested Parties

To make sure that ISMS and related Policies are well known and communicated within the organization, they are available in the intranet-Filedoc and internal training is regularly performed, as well as communicated to other interested parties, when applicable.

References

NISTIR 8286B Prioritizing Cybersecurity Risk for Enterprise Risk Management

https://csrc.nist.gov/publications/detail/nistir/8286b/final

Related Documents

ISMS - Operational Rules