



Information Technology Auditing Cassa Depositi e Prestiti

Roma, 28/11/2023

Agenda

Internal Audit positioning and role

The Internal Control System – Three Lines Model
Nature, Responsibility & Duties of Internal Audit
Risk Assessment

Information Technology Audit

Definition

Primary objectives of IT Audit

Best practices

Main regulations on Information Technology

Analysis of the main known cyber attacks globally in the 2018-2022

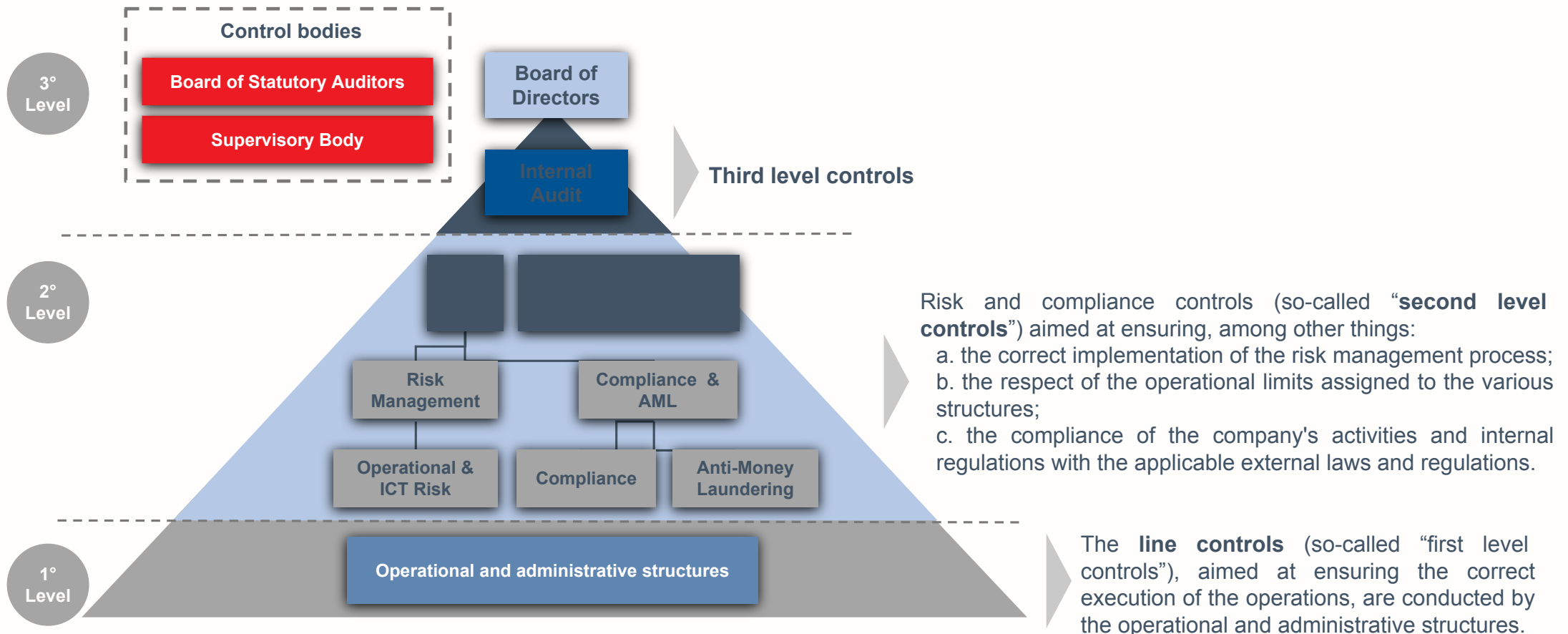
IT Audit Experience in Cassa Depositi e Presidi: our results

Main benefits in IT Governance & IT Management

Main benefits in IT Security

Internal Audit positioning and role

The Internal Control System – Three Lines Model



Internal Audit positioning and role

Nature, Responsibility & Duties of Internal Audit



Nature

Internal Audit is a permanent, independent and objective function which, through a professional and systematic oversight, pursues the **continuous improvement of the effectiveness and efficiency of CDP's governance, risk management and control processes**



Responsibility

- Continuous and independent monitoring, through third-level controls and a **risk-based approach**, on the regular performance of **governance, risk management and control processes**;
- Prevention or detection of anomalous and risky situations;
- Collaboration with the other company's structures and coordination with the other control functions.



Duties

Verifies the functioning, effectiveness and efficiency of **processes**, including those outsourced, and compliance with internal and external regulations;

Monitors the evolution of the organization in order to identify **new risk profiles**;

Assesses:

- the adequacy, overall reliability and security of the **information system** (ICT audit), as well as the adequacy of the disaster recovery plan;
- the levels of logical and physical security, the availability and integrity of the information systems and the **confidentiality of information**;

Internal Audit positioning and role

Risk Assessment

SCOPE



The **Risk Assessment** activity normally carried out on at least an annual basis is aimed at **evaluating** the riskiness of company processes, to **give priority** to the interventions to be planned, **focusing** on what is most risky and strategic for the Company

ASSESSMENT



For each Audit Area, an assessment of the associated risks is carried out at an **inherent** and **residual** level, i.e. based on the assessment of internal controls

SUPPORTING INFORMATION



The evaluation is based on:

- **knowledge** acquired through previous audit activity;
- **information flows** from the other control functions (Risk Management, Compliance, Anti-Money Laundering), from the external auditor, from the Supervisory Authority;
- information available within the Company;
- ad hoc interviews and meetings with company process managers

Information Technology Audit

Definition

What is an Information Technology (IT) audit?

An Information Technology audit is the examination and evaluation of an organization's information technology infrastructure, applications, data use and management, policies, procedures and operational processes against recognized standards or established policies. Audits evaluate if the controls to protect information technology assets ensure integrity and are aligned with organizational goals and objectives.

(Harvard University)

Traditionally, the term “IT audit” suggests certain familiar procedures such as ensuring the functionality and integrity of an entity’s tools, systems and networks; testing and monitoring the security of IT systems against intrusion or misappropriation; and providing assurance around the compliance of IT activities with relevant enterprise policies, industry best practices and government laws and regulations.

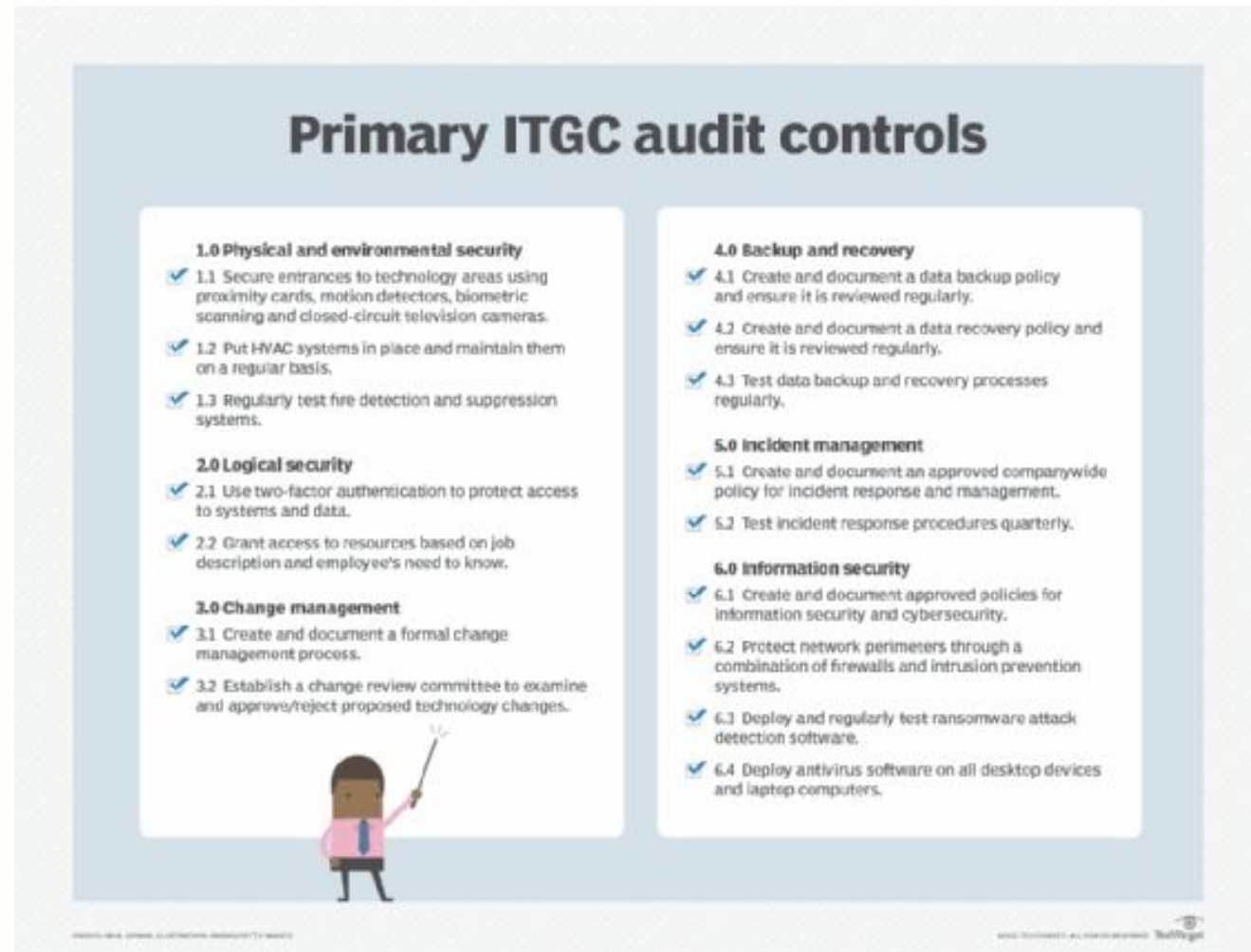
However, the archetype of IT audit is changing. As society in general becomes more data driven and organizations increasingly look to leverage data to power processes, inform business decisions and generate value, IT audit must, in turn, provide business leaders with more timely and actionable risk assessments and input for effective governance of data and other IT assets.

Information Technology Audit

Primary objectives of IT Audit

The primary objectives of an IT audit include the following:



- Evaluate the **systems** and processes in place that **secure** company **data**.
- Verify that IT controls are being regularly practiced and maintained.
- Determine risks to a company's **information assets** and identify methods to minimize them.
- Ensure **information** management processes are in **compliance** with IT-specific laws, policies and **standards**.
- Determine inefficiencies in IT systems and associated management.



Interno – Internal

Financial Regulatory Framework

Main regulations on Information Technology

	Banking & Payments Markets	Investment Services	Asset Management	Insurance
 Normativa UE	CRD/CRR	MiFIR	UCITS IV	Solvency II
	PSD2	EMIR	AIFMD	IDD
	EMD2	MiFID2		IORP II
	EBA Guidelines	ESMA Guidelines		EIOPA Guidelines
	NIS Directive			
	GDPR			
	DORA			
	TIBER EU Framework			
 Normativa Nazionale	TUB	TUF		CAP
	Bol Circ. 285	Regolamento Emittenti		IVASS Reg. 38
	Bol Circ. 288	Regolamento Intermediari		IVASS Reg. 40
	Disp. Vig. IMEL	Reg. attuato art. 4-undecies TUF		IVASS Reg. 41
	Perimetro Nazionale di Sicurezza Cibernetica			

Circolare 285/2013: regulation that provide financial intermediaries with general requirements for the development and management of the information system.

EBA Guidelines: the guidelines on “ICT and security risk management” establish requirements for credit institutions, investment firms and payment service providers (PSPs) on the mitigation and management of their information and communication technology (ICT) risks.

GDPR (General Data Protection Regulation): regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

DORA (Digital Operational Resilience Act): regulation that establishes a binding and comprehensive framework regarding ICT risk management for the EU financial sector. It establishes the technical standards that financial entities and their critical third-party technology service providers must implement in their ICT systems.

TIBER EU: framework for threat intelligence-based ethical red-teaming. It provides comprehensive guidance on how authorities, entities, and threat intelligence and red-team providers should work together to test and improve the cyber resilience of entities by carrying out controlled cyberattacks.

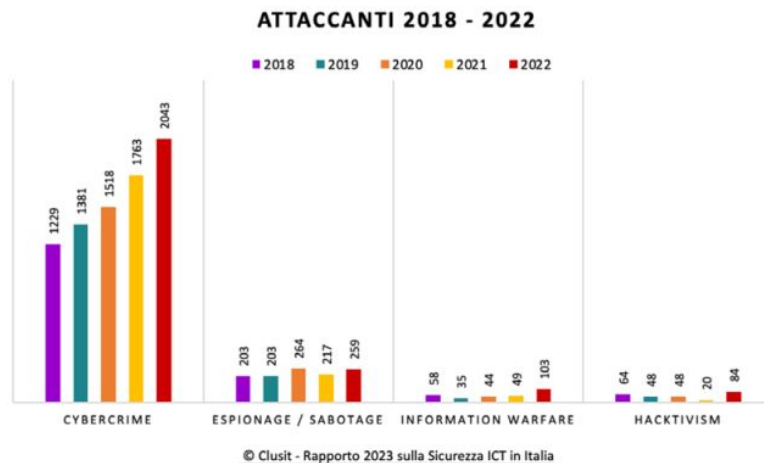
Information Technology Audit

Analysis of the main known cyber attacks globally in the 2018-2022



In the period between January 2018 and December 2022, a total of 9,633 cyber attacks occurred.

This number represents 58.4% of the total incidents classified in 12 years, with an overall average of 161 attacks per month over the entire period (there were 39 in 2011, 130 in 2018, and 207 in 2022).



In the last year, 2,489 accidents were recorded, the highest number ever and it is interesting to note how in 2022 the reality has exceeded the predictions indicated in gray by the trend line.

Information Technology Audit

Best practices



COBIT (Control Objectives for Information and Related Technologies) is a globally recognized framework and set of guidelines for governing and managing information technology (IT) and related services within an organization. COBIT provides a structured approach to IT governance, risk management, and compliance, and it is designed to align IT activities with the strategic goals and objectives of the business.

ITIL (Information Technology Infrastructure Library) is a framework and set of best practices that provides guidance for managing and delivering IT services within an organization. ITIL offers a structured approach to IT service management (ITSM) and is designed to help organizations align their IT services with their business needs and objectives. It defines a series of processes, procedures, tasks, and checklists that can be adapted and customized to suit an organization's specific requirements.



ISO/IEC 27001 is an international standard for information security management systems (ISMS). It provides a systematic and structured approach to managing and protecting sensitive information within an organization. ISO/IEC 27001 outlines a framework for establishing, implementing, maintaining, and continually improving an ISMS, which is designed to ensure the confidentiality, integrity, and availability of information while managing information security risks effectively.

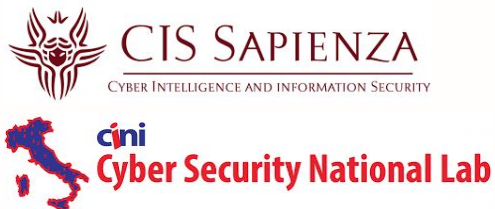
Information Technology Audit

Best practices



The **National Institute of Standards and Technology (NIST)** provides comprehensive guidance on cybersecurity through a framework that is widely adopted in the United States and around the world. NIST's approach to cybersecurity is widely recognized and adopted, and it provides a structured and risk-based framework for organizations to manage and improve their cybersecurity posture. The NIST Cybersecurity Framework, specifically NIST Special Publication 800-53 and NIST Special Publication 800-171, serves as a valuable resource for organizations to enhance their cybersecurity practices and meet regulatory requirements in various industries.

Framework Nazionale per la Cybersecurity e la Data Protection



The “**Framework Nazionale per la Cybersecurity e la Data Protection**”, inspired by the Cybersecurity Framework created by NIST (National Institute of Standards and Technology), provides an operational tool for organizing cybersecurity processes suitable for public and private organizations of any size. Compared to the NIST framework, it also includes a series of new elements aimed at guiding the correct management of personal data, with specific reference to their security in the face of possible cyber attacks.

IT Audit Experience in Cassa Depositi e Presiti: our results

Main benefits in IT Governance & IT Management

Definition of a **ICT Strategical Plan** and **Operational Plan** aligned with the Corporate Industrial Plan

Definition of the following processes and adoption of supporting instruments:

- **Demand** Management
- **Service** Management (Service Level Agreement definition and monitoring, definition of a Service Catalog and implementation of a CMDB)
- **Capability** and Availability Management
- **Business Continuity** Management
- **Change** Management
- **Incident** and **Problem** Management

Identify

IT Audit Experience in Cassa Depositi e Presiti: our results

IT Security Governance



Third-party security risk management



Protect

Access Management (implementation of an Identity Governance & Intelligence tool)

Secure Development Lifecycle



Hardening of individual computing devices



Hardening of backup process

Hardening of network and remote connection

Hardening of email

Implementation of Multi Factor Authentication

Security training

Detect

Real-time monitoring of security events

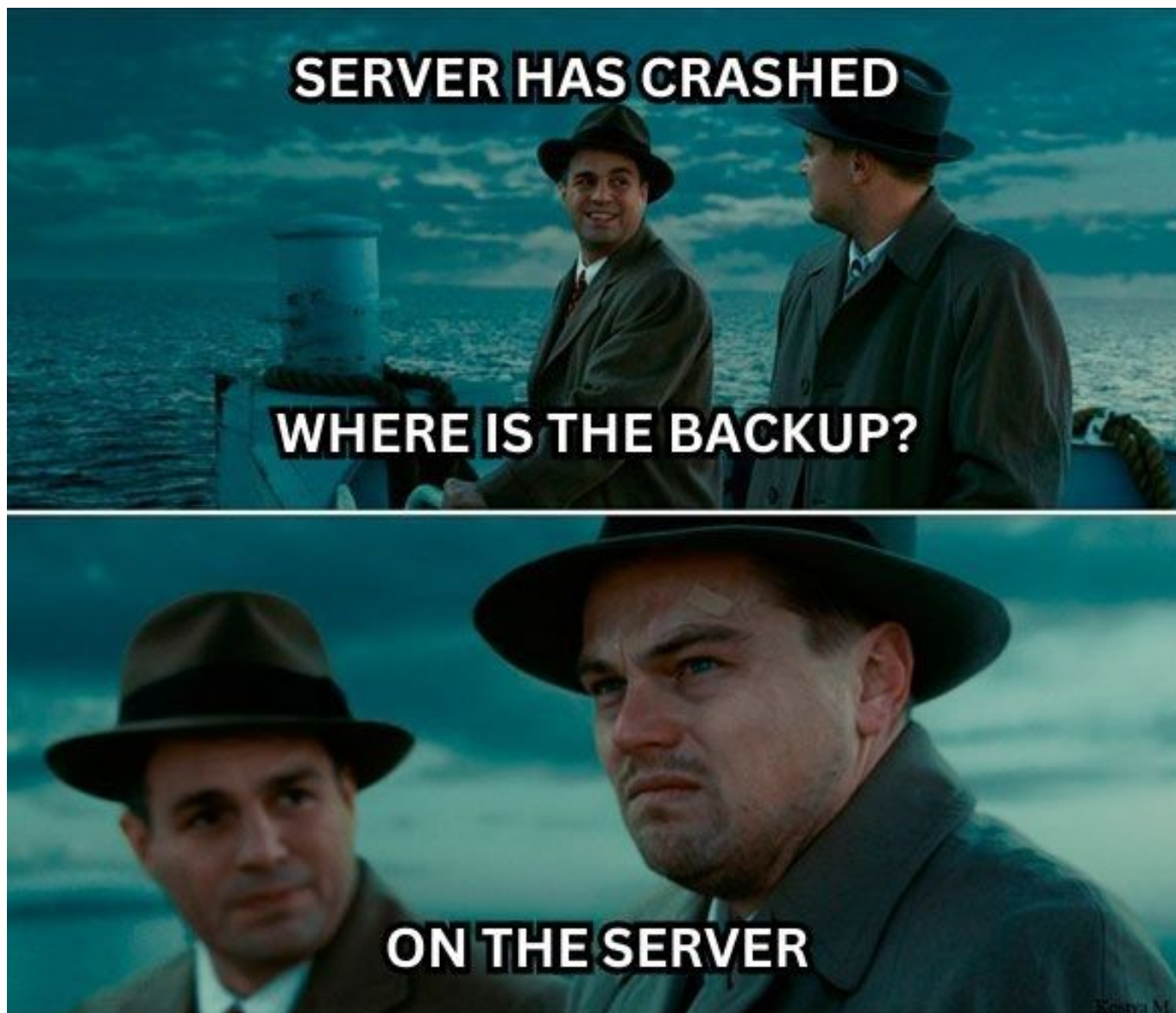
Security Operations Center (SOC)

BACKUP





Interno – Internal



Interno – Internal



