ATRIA SOLUTIONS

Cybersecurity in Financial Institutions
The Good, the Bad and the Ugly

Cybersecurity Practice Leader

Tony Chebli - Brussels, Belgium

23 Years+ Industry Experience, CISSP, CMSA, PECB & TRECCERT Certified Trainer, PECB Certified Data Protection Officer, ISO/IEC 27001 Lead Auditor, ISO 27701 LI, ISO 27002 Lead Manager, PECB Cloud Manager, ISO 27005 Risk Manager and PECB Certified ISO/IEC 27032 Lead Cyber Security Manager.

Tony Chebli is the Cybersecurity practice leader at Atria Solutions in Europe and the Middle East. He led the cybersecurity practice at CGI Belgium, he was the head of the Information Security Department at Credit Libanais for 13 years. He holds several cybersecurity certificates, including CISSP (since 2001), PECB Certified Management Systems Auditor (CMSA), PECB Data Protection Officer (GDPR), ISO 27001 Lead Auditor, ISO 27701 LI, ISO 27002 Lead Manager, PECB Cloud Manager, ISO 27005 Risk Manager, ISO 27032 Lead Cyber Security Manager, PECB and TRECCERT Certified trainer, and other technical certifications.

Tony received the security award "CISO-100" (Chief Information Security Officer among the top 100 in the region) from the Middle East Security Awards (MESA) in Dubai, UAE, for three consecutive years.

He achieved PCI-DSS compliance for Credit Libanais (the first and still the only bank to be certified PCI-DSS in Lebanon), Netcommerce (an e-commerce site), IPN (a service provider), CCM (a service provider), and Credit International Bank in Senegal.

His experience in the field is extensive and has led him to perform the following:

- Providing consultancy for ISO 27001 certifications,
- Performing risk assessments based on ISO 27001

Agenda

- Definition
- The Bad
- Security news!
- Security Facts!
- Threats & vulnerabilities
- The Ugly
  - Pune Cosmos Bank cyber attack case
  - Bangladesh Bank heist case
  - Accenture security breach case
  - Capital One hack case
  - Apex Bank breach case
  - Experian breach case
  - State Farm Bank breach case
  - Equifax breach case
  - Tesco bank case
  - Heartland Payment Systems breach case
- The Good
- Security program
- ISO 27001 standard
- Ask me anything

Definition

Cyberspace is a concept describing a widespread, interconnected digital technology. "The expression dates back from the first decade of the diffusion of the internet. It refers to the online world as “apart,” distinct from everyday reality.

Definition

Cyberspace includes physical infrastructures and telecommunications devices that allow for the connection of technology and communication system networks, understood in the broadest sense (SCADA devices, smartphones/tablets, computers, servers, etc.).

Definition

"INFORMATION is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably PROTECTED"

"…...Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected"

Definition

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security.

Definition

Cyber-attack is an assault launched by cybercriminals using one or more computers against single or multiple computers or networks. A cyber attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks.

The Bad

"The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards.

Even then, I wouldn't stake my life on it."

Gene Spafford- Director, Computer operations, audit and Security Technology

(COAST)-Purdue University

Adversaries weapons

Phishing

Malware

Ransomware

DDOS

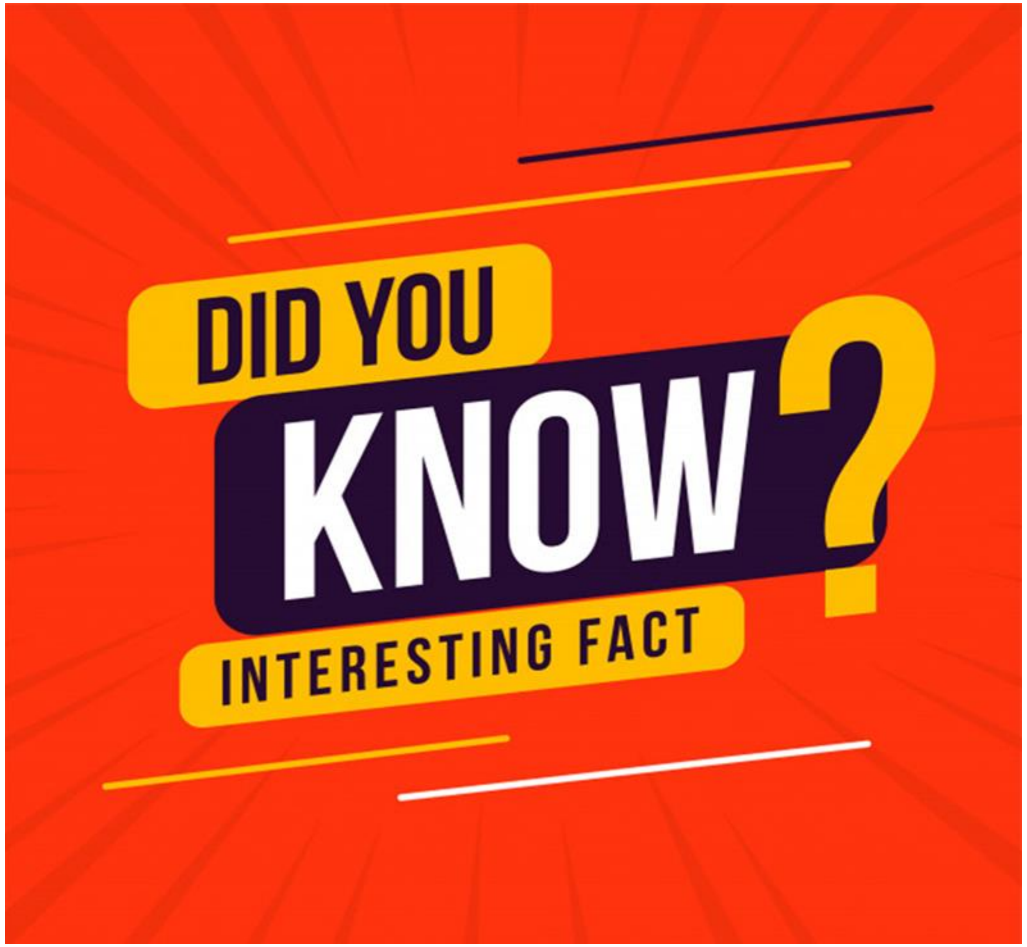
APTs

Cloud

IoT

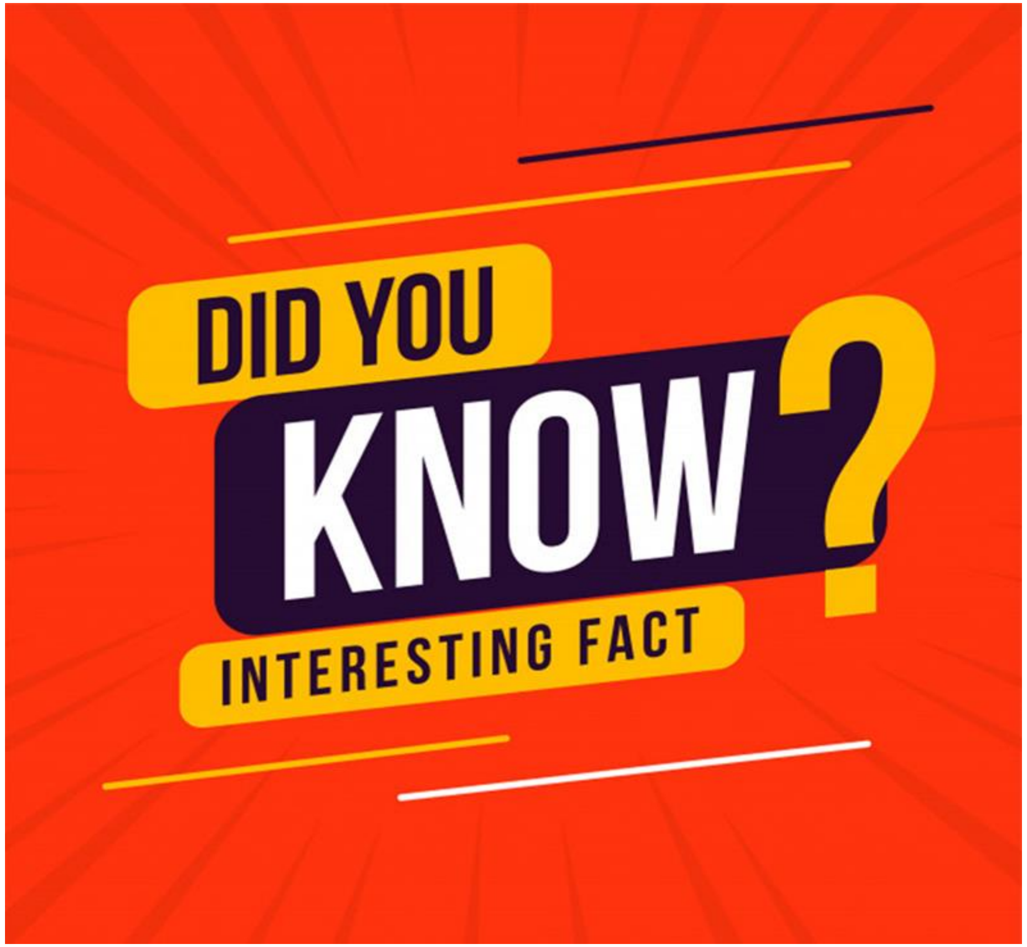
Insider Threats

Security news!



- Cybersecurity Ventures predicts cybercrime damages will cost the world $6 trillion annually
- Nearly 80 Percent of German Organizations Aren’t Prepared for a Cyber Security Incident
- Almost Half of Boards Lack a Real Understanding of Cyber Threats
- Business email compromise cost over $7 billion in 2023
- More than 50 Billion Devices are Vulnerable to Cyberattacks
- IoT: Hacker’s Wonderland in the Enterprise
- Lack of Skills Still Hamper Ability to Deliver Cybersecurity
- EU General Data Protection Regulation (GDPR) is Forcing Firms

Security news!



- Ransomware has continued its upward trend with an almost 25% increase in 2022
- Error continues to be a dominant trend and is responsible for 13% of breaches due to misconfigurations of Cloud storage
- 82% of breaches involved in the human element in 2023

Security Facts!

- EU Digital Operational Resilience Act (DORA) is a new act for Financial Institutions to be applied by 2025.
- 135% increase in novel social engineering attacks across thousands of emails between Jan & Feb 2023 with the wide spread of ChatGPT
- A lost or stolen device like a smartphone or laptop causes 3.3 percent of confirmed security breaches and 15.3 percent of overall incidents.
- Document-related errors: i.e. forwarding sensitive information to incorrect recipients, publishing private data to public

Security Facts!

- Weak or stolen credentials lead to massive security breaches
- 50% of security breaches are caused by employees misusing access privileges
- Using outdated software and web browsers can cause serious security concerns
- 62% of cyberattacks in 2021 exploited the trust of customers in their suppliers

Threats & Vulnerabilities

Vulnerabilities

Lack of appreciation of threats

It won’t happen to us

E-mail and Internet access

Staff / Contractors / Employees

Physical Security

Outsourcing

Vulnerabilities

Remote working

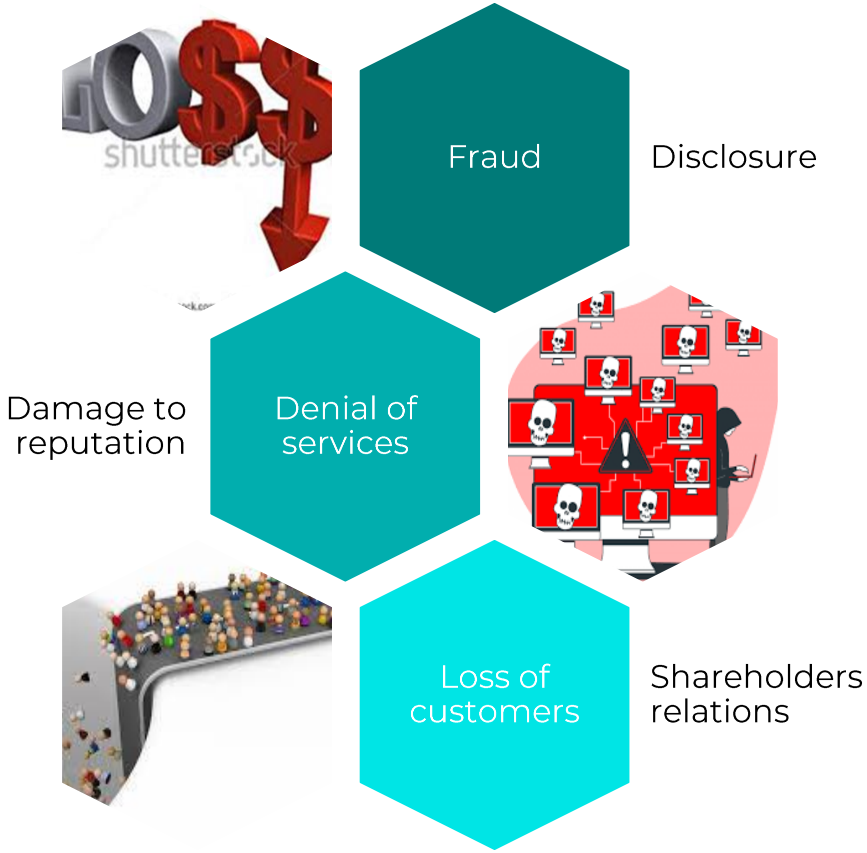
Rush to market

Absence of BCP/DRP

Low awareness of security

Poor controls

Threats



Fraud

Disclosure

Damage to reputation

Denial of services

Loss of customers

Shareholders relations

The Ugly

Pune Cosmos Bank cyber attack case

The 2018 Pune Cosmos Bank cyber attack

Cosmos Bank is a large cooperative bank in India with digital banking offerings.

- Hackers exploited the bank's ATM/debit card switch to gain unauthorized access.
- Hackers used malware to manipulate the switch transactions and disable incoming payment alerts. This allowed transactions to go undetected.
- The attack went unnoticed for several days.

With access to the payment switch, the hackers were able to initiate fraudulent ATM withdrawals totaling $13.5 million from 28 countries and siphon off $2.5 million via unauthorized money transfers. In total, hackers were able

Pune Cosmos Bank cyber attack case

The 2018 Pune Cosmos Bank cyber attack

Root cause analysis

The post-breach investigation found a lack of monitoring, network segmentation, and multi-factor authentication played a role.

Bangladesh Bank heist case

The 2016 Bangladesh Bank heist

Central Bank of Bangladesh with a SWIFT terminal for interbank messaging.

- Hackers compromised the bank's SWIFT credentials through a targeted phishing campaign aimed at bank employees.
- Having the SWIFT passwords allowed the hackers to send fraudulent money transfer requests from Bangladesh Bank to the Federal Reserve Bank of New York.

The hackers were able to successfully initiate over three dozen request messages totaling almost $1 billion in fraudulent transfers.

Bangladesh Bank heist case

The 2016 Bangladesh Bank heist

Root cause analysis

Investigations found the bank's security deficiencies including:

- Lack of proper network segmentation
- Weak system logging and audit functions enabled the large-scale theft.
- Limited multi-factor authentication and oversight of SWIFT activity also contributed to hackers evading detection for an extended period.

Accenture security breach case

The 2021 Accenture security breach

Accenture is a major global professional services firm that provides technology and consulting services to financial institutions.

In 2021, malicious actors compromised Accenture's systems and gained access to customer banking data.

The extent of the banks' data loss included transaction records, login credentials, and customers' personal information.

Accenture security breach case

The 2021 Accenture security breach

Root cause analysis

- The initial access point was traced to an exposed Accenture password on the dark web, indicating password reuse or phishing may have been the root cause.
- Once inside Accenture's network, the hackers were able to move laterally and access sensitive customer banking data and passwords stored on Accenture servers.
- Weak internal segmentation allowed the breach to access over two dozen major banks' data that was being managed by Accenture as a services provider.

Capital One hack case

The 2019 Capital One Hack

Capital One suffered a major data breach that impacted 106 million credit card customers and applicants. Once inside the network, the hacker was able to pull large amounts of sensitive customer financial data and credit card transaction logs.

Root cause analysis

- The attack was perpetrated by a hacker who exploited a misconfigured Web Application Firewall (WAF).
- The WAF misconfiguration allowed the hacker to use an SQL injection on Capital One’s public-facing APIs to gain unauthorized access.

Capital One hack case

The 2019 Capital One Hack

- The weakly configured WAF allowed the SQL injection against the API to succeed and did not trigger any alerts.
- Capital One's APIs also lacked proper rate limiting, allowing the hacker to make a very large number of queries to extract maximum data.
- The incident revealed API vulnerabilities stemming from poor WAF configurations, SQL injection flaws, and lack of restrictive rate limiting.

Apex Bank breach case

The 2018 Apex Bank Breach

Apex Bank was a U.S. community bank that suffered a security breach impacting thousands of customer records.

In total, the personal and financial data of over 5,000 customers were compromised.

As a result, Apex Bank was forced to notify and offer credit monitoring to impacted customers.

The breach resulted in $2 million in costs for notification, credit protection services, and legal fees.

Root cause analysis

- Initial investigations revealed that an employee fell victim to a phishing email which allowed the attackers'

Apex Bank breach case

The 2018 Apex Bank Breach

- Once inside the network, the attackers were able to move laterally undetected and access databases with customer names, account details, Social Security numbers, and other personal data.
- Inadequate network segmentation and privilege management allowed wider access.

Experian breach case

The Experian Breach in 2015

Experian is a large credit bureau that suffered a data breach impacting over 15 million T-Mobile customers.

The breach was enabled by an Experian employee who exceeded authorized access to download sensitive customer data including names, addresses, Social Security numbers and other personal info.

Once discovered, the insider breach required Experian to notify millions of affected individuals whose personal information was compromised.

Experian faced over $200 million in costs related to the breach including legal settlements, credit monitoring services, and other liabilities.

Experian Breach

The Experian Breach in 2015

- Experian's controls and monitoring failed to detect unauthorized access and large-scale data exfiltration by the insider.
- The compromised employee credentials and unchecked access allowed the insider threat to operate undetected for months.

State Farm Bank breach case

StateFarm

The 2018 State Farm Bank Breach

State Farm Bank suffered a data breach that impacted 1.4 million customer records.

Once inside the bank's network, the hacker accessed sensitive customer data including names, addresses, phone numbers, account details and Social Security numbers.

As a result of the breach, State Farm Bank spent millions in notification costs, credit monitoring services, and legal fees.

Root cause analysis

- An investigation revealed the root cause was an unpatched Web server

State Farm Bank breach case

The 2018 Sacca v. State Farm Bank Breach

- State Farm Bank did not have an established penetration testing program to proactively identify such vulnerabilities.

Equifax breach case

The 2017 Apache Struts Breach at Equifax

Equifax suffered a massive data breach that exposed the personal information of 143 million US consumers.

Hackers were able to exploit this vulnerability to access sensitive Equifax databases containing consumer names, Social Security numbers, birth dates, addresses and other personal data.

In total, the records of nearly half the U.S. population were exposed in the Equifax breach.

Equifax faced over $1 billion in costs related to legal fees, notification expenses, and a settlement with the Federal Trade Commission

Equifax breach case

The 2017 Apache Struts Breach at Equifax

- The vulnerable Struts version contained a flaw that allowed attackers to execute malicious code through a lack of proper input validation.
- This left the web application vulnerable to remote code execution via the unvalidated input.

Tesco Bank case

The 2016 Apache OFBiz XSS Attack on Tesco Bank

Tesco Bank, a UK-based financial institution, was the victim of a cyber attack that exploited an XSS vulnerability on their login page. Over 9000 customer accounts were compromised before Tesco Bank halted the attack.

Tesco Bank had to refund affected customers and spent millions in remediation costs related to the breach.

Root cause analysis

- The login page was powered by Apache OFBiz, which contained a flaw allowing the injection of malicious scripts into the web application code.

Tesco Bank case

The 2016 Apache OFBiz XSS Attack on Tesco Bank

- With the stolen credentials, the attackers gained access to customer accounts and initiated unauthorized transfers totaling over $3 million dollars.
- The XSS vulnerability allowed the script injection due to a lack of proper input validation on the login form fields.

Heartland Payment Systems breach case

The 2008 Heartland Payment Systems Breach

Heartland Payment Systems was a credit card payment processor that suffered a major breach impacting 130 million cards. In total, the attackers successfully extracted data for over 100 million cards over several months before being detected.

The breach resulted in major costs for Heartland including legal fees, fines, and acquisition by another provider.

Root cause analysis

- The initial foothold gained by attackers was through the exploitation of a buffer overflow flaw in

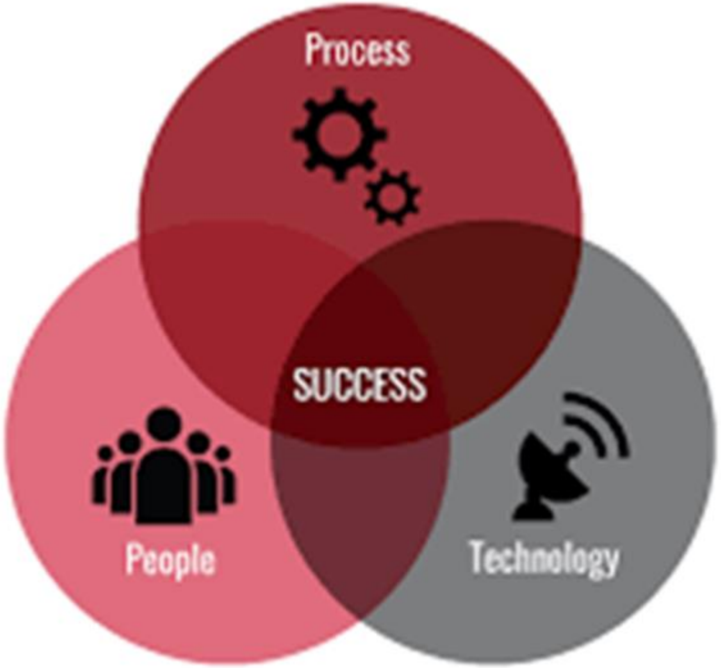
Heartland Payment Systems breach case

The 2008 Heartland Payment Systems Breach

- By exploiting this buffer overflow, the attackers were able to compromise the firewall and pivot internally to install sniffing malware on payment processing servers.
- This malware allowed them to intercept credit card numbers, expiration dates, and other track data as it was sent to Heartland for processing by retailers.

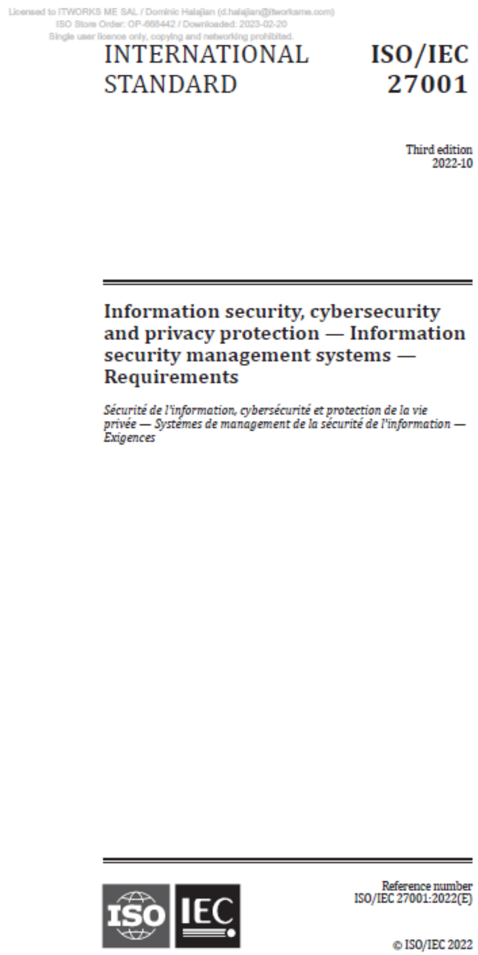
The Good

Security program



A security program is a set of policies, procedures, and technologies designed to protect an organization's assets, including its data, intellectual property, employees, and physical infrastructure, from various security threats.

Applicability



INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

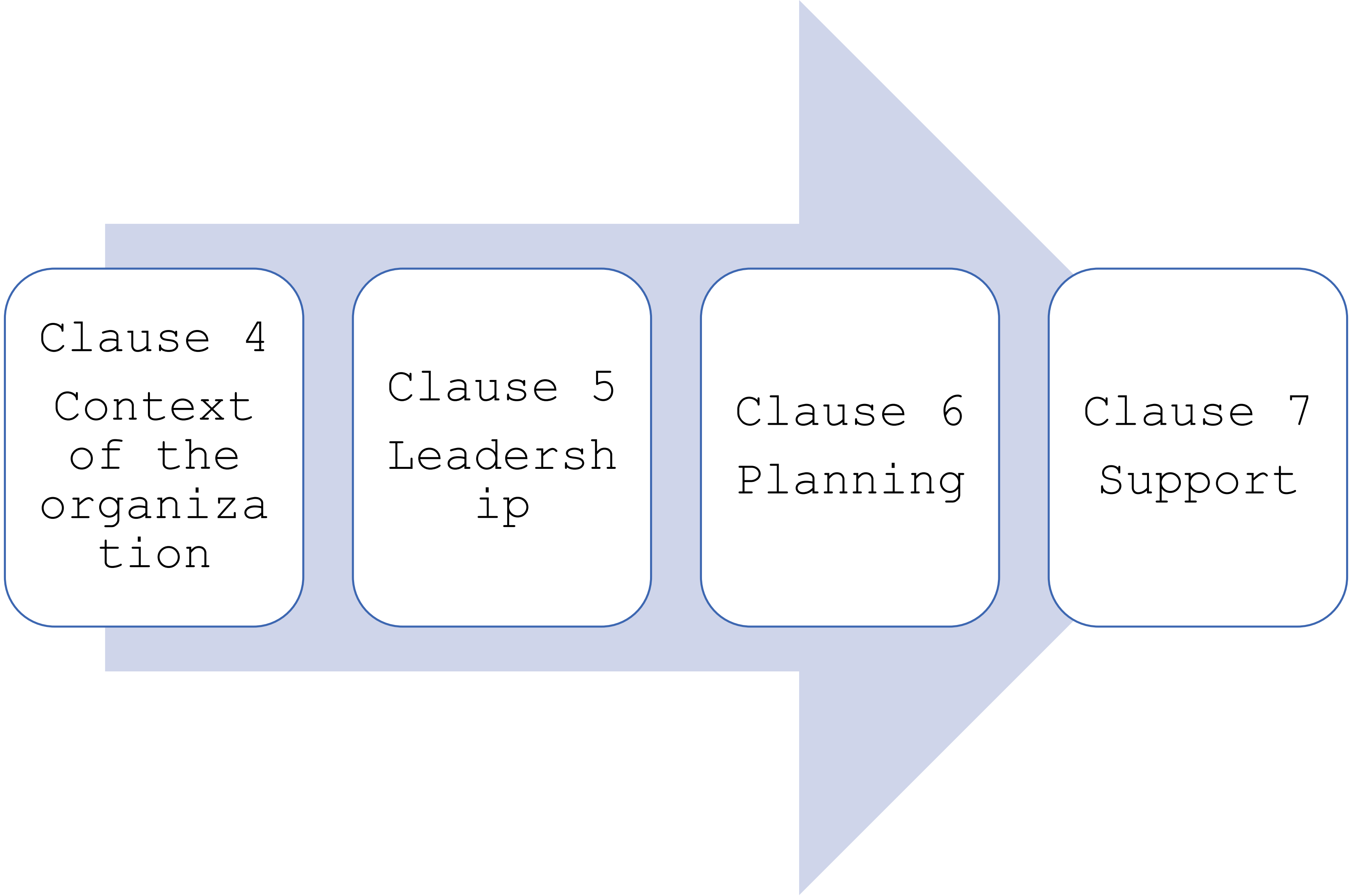
Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

ISO IEC

Reference number
ISO/IEC 27001:2022(E)

ISO 27001

ISO 27001 standard



Clause 4

Context of the organization

Clause 5

Leadership

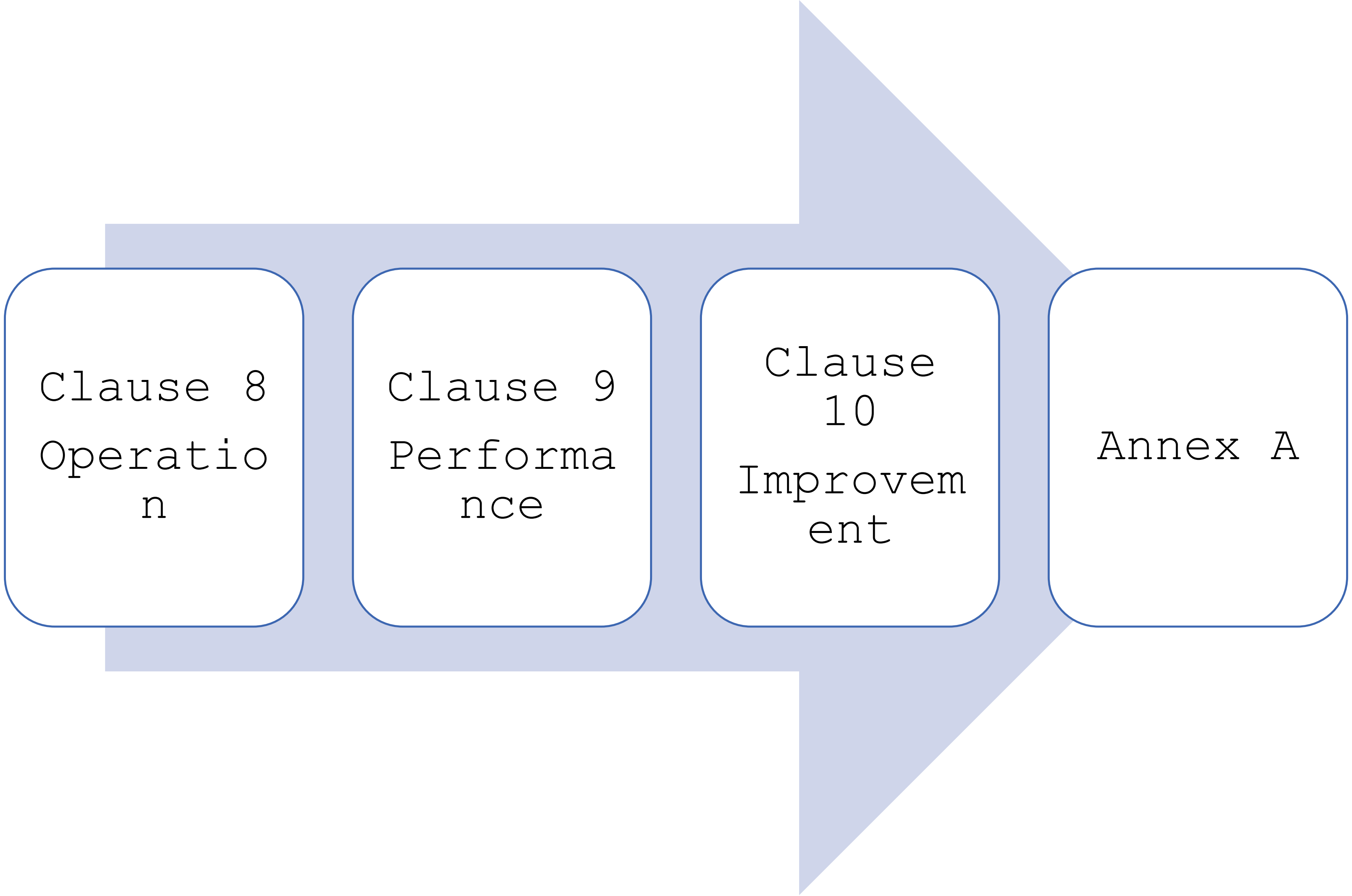
Clause 6

Planning

Clause 7

Support

ISO 27001 standard



Clause 8

Operation

Clause 9

Performance

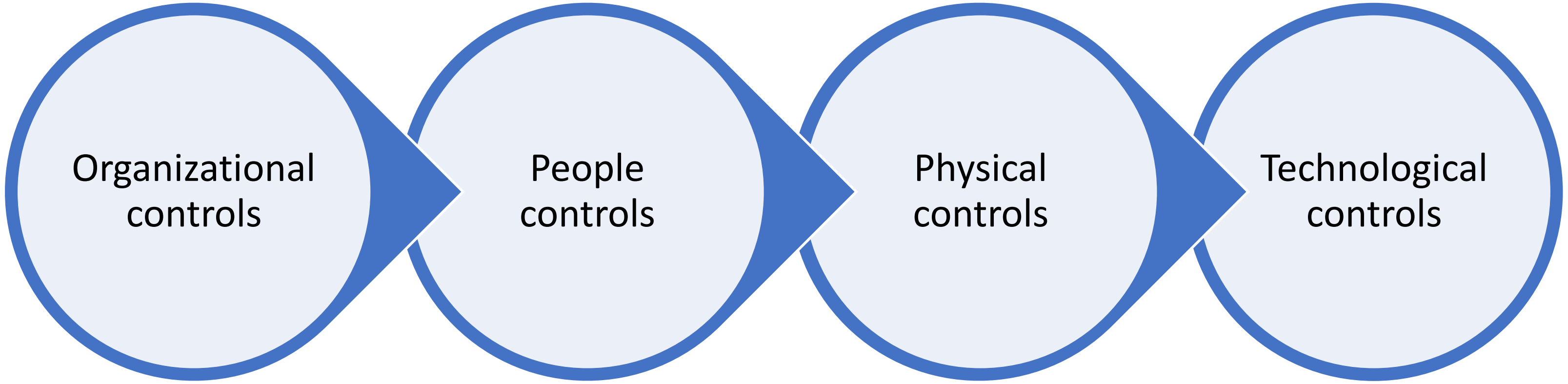
Clause 10

Improvement

Annex A

Annex A

93 information security controls total, grouped in 4 categories



5. Organizational controls

5.1 Policies for information security	5.2 Information security roles and responsibilities	5.3 Segregation of duties	5.4 Management responsibilities	5.5 Contact with authorities
5.6 Contact with special interest groups	5.7 Threat Intelligence	5.8 Information security in project management	5.9 Inventory and other associated assets	5.10 Acceptable use of information and other associated assets
5.11 Return of assets	5.12 Classification of information	5.13 Labeling of information	5.14 Information transfer	5.15 Access control
5.16	5.17	5.18	5.19	5.20

5. Organizational controls

5.21 Managing information security in ICT supply chain	5.22 Monitoring, review and change management of supplier services	5.23 Information security for cloud services	5.24 Information security incident management planning and preparation	5.25 Assessment and deacon on information security events
5.26 Response to information security incidents	5.27 Learning from information security incident	5.28 Collection of evidence	5.29 Information security during disruption	5.30 ICT readiness for business continuity
5.31 Legal, statutory, regulatory and	5.32 Intellectual property rights	5.33 Protection of records	5.34 Privacy and protection of PII	5.35 Independent review of informatio

6. People controls

<table>
<tr><td>6.1 Screening</td><td>6.2 Terms and conditions of employment</td><td colspan="2">6.3 Information security awareness, education, and awareness</td><td>6.4 Disciplinary process</td></tr>
<tr><td colspan="2">6.5 Responsibilities after termination or change of employment</td><td>6.7 Remote working</td><td colspan="2">6.8 Information security event reporting</td></tr>
</table>

7. Physical controls

7.1 Physical security perimeters	7.2 Physical entry	7.3 Security offices, rooms, and facilities	7.4 Physical security monitoring	7.5 Protecting against physical and environmental threats
7.6 Working in secure areas	7.7 Clear desk and clear screen	7.8 Equipment sitting and protection	7.9 Security of assets off premises	7.10 Storage media
7.11 Supporting utilities	7.12 Cabling security	7.13 Equipment maintenance	7.14 Secure disposal or re-use of equipment	

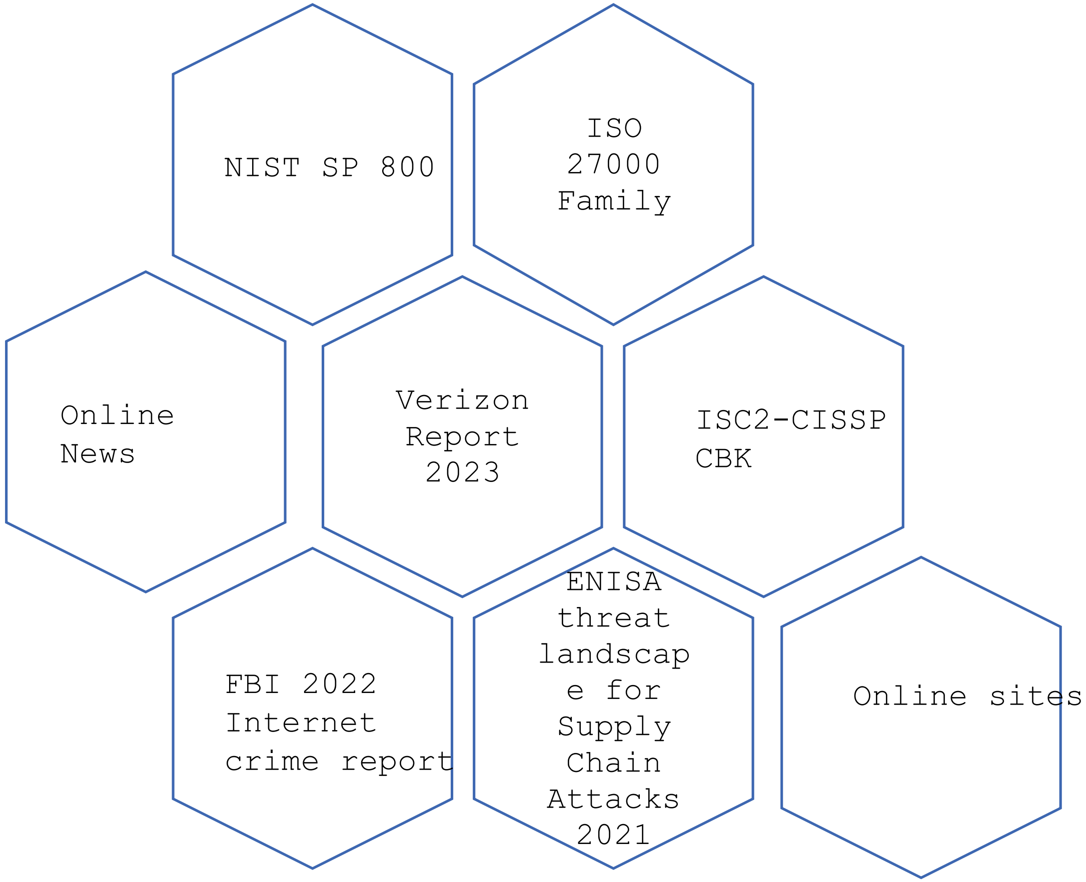
8. Technological controls

8.1 User end point devices	8.2 Privileged access rights	8.3 Information access restrictions	8.4 Access to source code	8.5 Secure authentication
8.6 Capacity management	8.7 Protection against Malware	8.8 Management of technical vulnerabilities	8.9 Configuration management	8.10 Information deletion
8.11 Data masking	8.12 Data leakage prevention	8.13 Information backup	8.14 Redundancy of information processing facilities	8.15 Logging
8.16 Monitoring	8.17 Clock synchroniz	8.18 Use of	8.19 Installati	8.20 Networks

8. Technological controls

8.21 Security of network services	8.22 Segregation of networks	8.23 Web filtering	8.24 Use of cryptography	8.25 Secure development lifecycle
8.26 Application security requirements	8.27 Secure system architecture and engineering principles	8.28 Secure coding	8.29 Security testing in development and acceptance	8.30 Outsourced development
8.31 Separation of test, development, and production environments	8.32 Change Management	8.33 Test information	8.34 Protection of information systems during audit testing	

References



NIST SP 800

ISO 27000 Family

Online News

Verizon Report 2023

ISC2-CISSP CBK

FBI 2022 Internet crime report

ENISA threat landscape for Supply Chain Attacks 2021

Online sites

?
ASK ME
ANYTHING