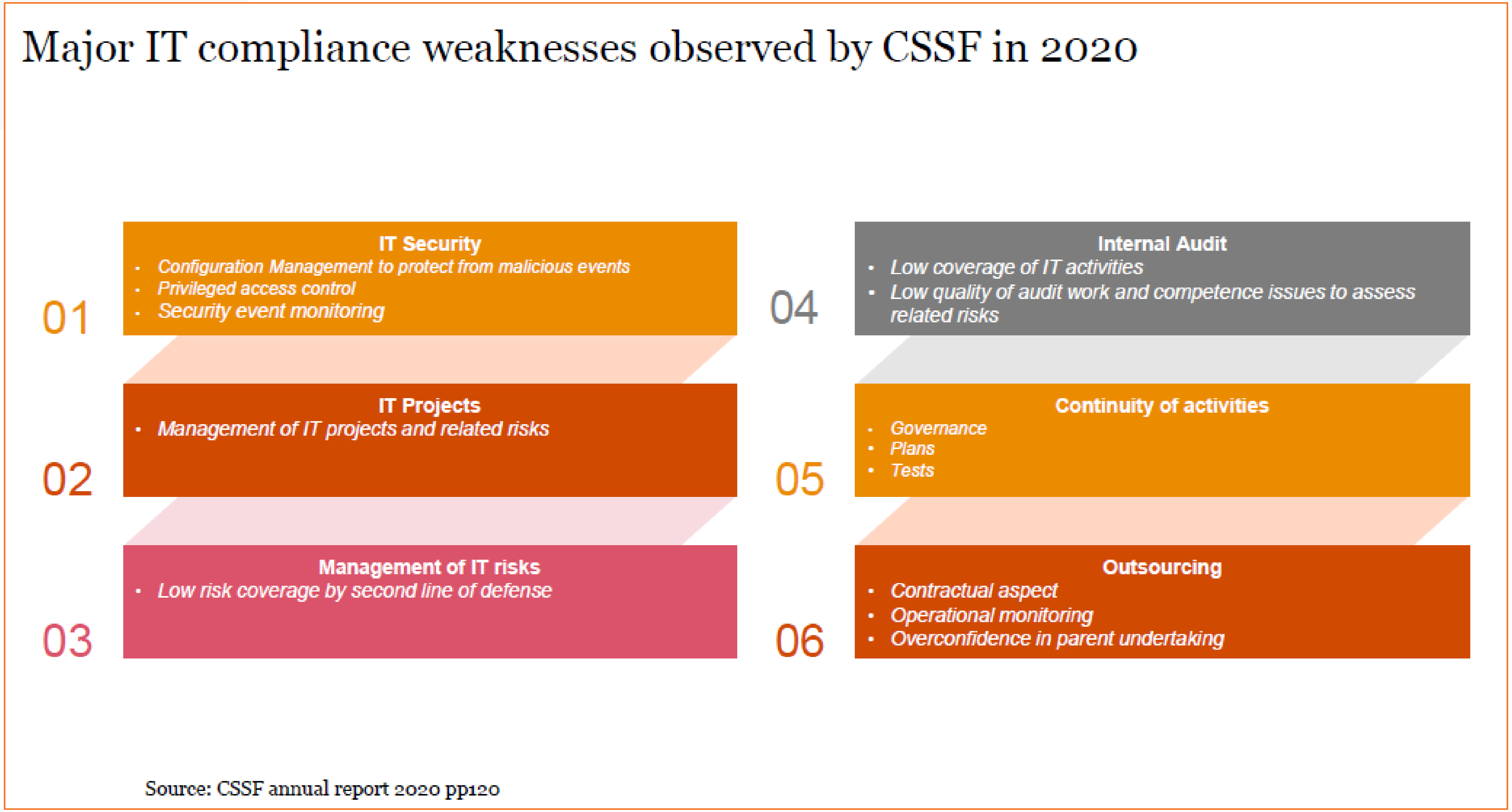
WALLIX
CYBERSECURITY SIMPLIFIED

SECURITY FORUM

Identity & Access Management: How to deal with compliance

By **Antoine Louveau**
Territory Manager
Belgium at WALLIX

CSSF Observations



Major IT compliance weaknesses observed by CSSF in 2020

01 **IT Security**
- *Configuration Management to protect from malicious events*
- *Privileged access control*
- *Security event monitoring*

02 **IT Projects**
- *Management of IT projects and related risks*

03 **Management of IT risks**
- *Low risk coverage by second line of defense*

04 **Internal Audit**
- *Low coverage of IT activities*
- *Low quality of audit work and competence issues to assess related risks*

05 **Continuity of activities**
- *Governance*
- *Plans*
- *Tests*

06 **Outsourcing**
- *Contractual aspect*
- *Operational monitoring*
- *Overconfidence in parent undertaking*

Source: CSSF annual report 2020 pp120

CSSF Observations

- More and more regulations, certifications or frameworks are being put in place to help IT, but also OT (industrial environments) to improve security by limiting the attack surface , cyberattacks, insider threats, etc…
- This is a must be and some frameworks can be helpful with recommendations of controls, actions, and solutions to put in place. Many companies are impacted by regulations all over the world from different verticals (finance, industries, governmental, etc…)
- Some concepts appeared thanks to those certifications, regulations or frameworks.

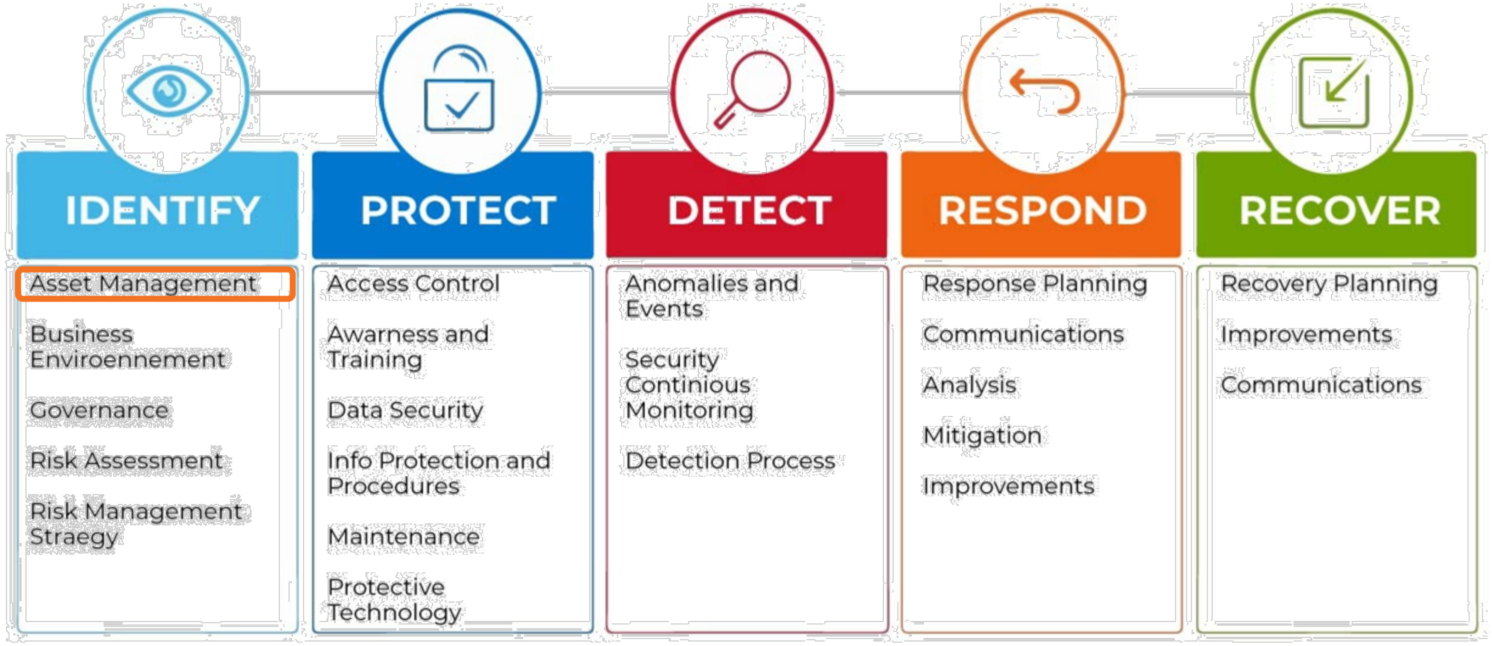
In 2021, compliance is the biggest board challenge: volume of regulatory change, instilling a culture of compliance, meeting regulatory expectations (Thomson Reuters source)

Legal

- GDPR
- NIS V1 for Digital Service Providers: SaaS, IaaS, PaaS, SecaaS (security), DaaS (data)
- NIS V2 for Providers of public electronic communication networks or services, Digital services such as social networking services and Data Centre Services
- PCI-DSS for banking data or PSF in Luxembourg
- HIPAA

Technical Framework

- ISO 27001/ ISO 27002 / 27017 / 27018
- CSA Cloud Security Alliance
- ISAE3402 / SSAE 16
- SOC 2 Trust Services
- NIST (General Access Control Guidance for Cloud Systems) & Zero Trust Architecture
- IEC 62443 (standards for Industrial Automation & Control Systems)
- HITECH-HIPAA



IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Enviroennement	Awarness and Training	Security Continious Monitoring	Communications	Improvements
Governance	Data Security	Detection Process	Analysis	Communications
Risk Assessment	Info Protection and Procedures		Mitigation	
Risk Management Straegy	Maintenance		Improvements	
	Protective Technology			

NIST FRAMEWORK & COMPLIANCE SAMPLE

ISO 27001

ISO 27k consists of **18 chapters**, the first 4 are introductions.

The remaining 14 chapters cover different subjects from Information Security Policies, to Supplier Relationships to Compliance.

A **PAM solution** can help with some controls and with indirect aspects of the ISO 27k.

ISO 27K: **Some direct aspects**

Section A.9 Access Controls

Section	Subject	Objective/Control	Role of PAM in the Control Execution
A.9.2.1	User registration and de-registration	Control: A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	A PAM solution facilitates user registration and de-registration to provide high visibility over access rights and active privileged users.
A.9.2.2	User access provisioning	Control: A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	The PAM solution provides a centralized management interface to grant or revoke privileged access rights to critical systems.
A.9.2.3	Management of privileged access rights	Control: The allocation and use of privileged access rights shall be restricted and controlled.	The PAM solution restricts and controls privileged access rights.
A.9.2.5	Review of user access rights	Control: Asset owners shall review users’ access rights at regular times.	Asset owners can specify privileged usage rights to the PAM system manager, who then implements the policies to ensure that only administrators approved by the asset owners are allowed privileged access. All access rights can also be managed in a centralized platform directly built in the PAM solution.
A.9.2.6	Removal or adjustment of access rights	Control: The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	The PAM solution allows super admins to smoothly modify their privileged of users or groups of users, thereby facilitating the termination or reduction of employee rights.

ISO 27K: **Some direct aspects**

Section A.9 Access Controls

Section	Subject	Objective/Control	Role of PAM in the Control Execution
A.9.4	System and application control	Objective: To prevent unauthorized access to systems and applications	A PAM solution bans direct access to critical systems, which can only be reached through the solution itself.
A.9.4.1	Information access restriction	Control: Access to information and application system functions shall be restricted in accordance with the access control policy.	A PAM solution provides administrators with the possibility to apply the principle of least privilege by granting different privileges according user groups and subgroups.
A.9.4.2	Secure log-on procedures	Control: Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	A PAM solution offers the possibility to maximize access security by enhancing access control over critical resources with an approval workflow. A PAM solution also provides rule configurations to detect malicious activity and block users from running programs or commands.
A.9.4.3	Password management system	Control: Password management systems shall be interactive and shall ensure quality passwords.	A PAM solution combining a vault and password management functionalities such as periodic password rotation, SSH key encryption, AAPM, cache mechanisms, etc. enable the enforcement of password policies related to privileged access.
A.9.4.4	Use of privileged unity programs	Control: The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	A PAM solution helps control and block when necessary, applications and programs running on target machines through extensive session monitoring.

ISO 27K: **Other direct aspects**

Section A.11 Physical and Environmental Security

Physical and environment security might seem far from system access management issues. However, the two topics are closely linked. Control A.11.1 Secure Areas, has the objective, “To prevent unauthorized physical access, damage and interference to the organization’s information and information processing facilities.” Physical access can easily translate into data and systemic access. Unauthorized physical access to a system exposes an organization to the risk of improper administrative actions, such as deleting accounts or reconfiguring security settings.

A PAM solution with a password vault lets privileged users do whatever they need to do without requiring any physical access to the hardware itself. In many traditional IT environments, admins had to manually reset servers, so physical access was expected. The practice created risk, though, which PAM mitigates.

Section A.15 Supplier Relationships

In many modern enterprises, supplier personnel may need privileged system access. While it’s rare for a supply chain partner to need this kind of access, with IT vendors, the arrangement is quite common. Outsourced IT vendors, some of whom might be on different continents, may need to have “root” access to critical systems. Control A.15.1 Information Security in Supplier Relationships, acknowledges this reality. The control objective for A.15.1 is, “To ensure protection of the organization’s assets that is accessible by suppliers.”
To protect an organization’s IT assets from unauthorized access by suppliers, the PAM solution can define and enforce agreed-upon access policies.

The PAM solution should also provide auditability that enables both supplier and client to verify that the policies are being followed. Controls A.15.1.1. and A.15.1.2 both address the requirement for establishing security policies in supplier relationships and agreements. PAM makes it possible to be specific about policies and prove compliance.

Some Indirect aspects of PAM in ISO 27K

Section A.5 Information Security Policies

Section	Subject	Objective/Control	Role of PAM in the Control Execution
A.5.1	Management direction for information security	Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	PAM ensures proper definition and enforcement of security policies related to privileged access.
A.5.1.1	Policies for information security	Control: A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	A PAM solution can produce reports of systems covered by PAM rules and document how those rules are implemented. This capability facilitates the definition of thorough security policies.
A.5.1.2	Review of the policies for information security	Control: The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	PAM reporting of access rules are helpful for gauging how security policies should be changed periodically, e.g. if a system changes from on-premises to cloud hosting, the privileged access policies may need to change along with it.

Some Indirect aspects of PAM in ISO 27K

Section A.12 Operations Security

Section	Subject	Objective/Control	Role of PAM in the Control Execution
A.12.1.2	Change management	Control: Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	PAM's session and activity tracing and recording should be used as a tool to monitor all change management work carried out to help troubleshoot issues that may show up after the change management. PAM also carries access validation workflows to ensure the control of processes.
A.12.1.3	Capacity management	Control: The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	A PAM solution provides a clear and concise view of targetuses along with information regarding the storage status and the number of concurrent connections.
A.12.4.1	Event logging	Control: Event logs recording user activities, exceptions, faults and information security events shall be produced, kept, and regularly reviewed.	A PAM solution traces and records all privileged users' activity to give administrators complete visibility over the actions that occur on their systems and equipment.
A.12.4.2	Protection of log information	Control: Logging facilities and log information shall be protected against tampering and unauthorized access.	All accesses should be logged into the system including unauthorized access. A PAM solution should differentiate the system administrator from the root user to protect against tampering. The WALLIX Bastion separates the administrator from the system's root user, thereby making the root user the only one able to access to logs files, protecting them against tampering. All access logs are also closely monitored.
A.12.4.3	Administrator and operator logs	Control: System administrator and system operator activities shall be logged and the logs protected regularly.	All operations realized by administrators should be logged through a syslog system. This includes information such as administrator connection, user creation by the administrator, password modification etc.

ISO 27K: **Other indirect aspects**

Section A.16 Information Security Incident Management

PAM figures into information security incident management, which is addressed by control A.16. For example, control A.16.1 Management of Information Security Incidents and Improvements, aims, “To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.” A PAM solution that can provide security managers with accurate information about privileged account sessions thanks to high traceability and monitoring capacities. A lack of detail about how and why a security incident occurred can impede a rapid, effective solution to the problem.

A PAM solution that can provide instant reporting on any administrative sessions that took place on targeted systems can give security managers a working narrative of the incident. Of course, the PAM solution has to be able to report on session details. Not all do this.

Section A.18 Compliance with Internal Requirements

The controls specified in A.18 cover compliance with internal requirements. These requirements may be driven by internal policy as well as by legal and contractual requirements (A.18.1) or regulatory schemes (A.18.1.1). The objective of A.18.1 is “To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.” PAM can play an important role in ensuring this sort of compliance.

Privileged access management may be directly required by compliance programs. In American healthcare and credit card privacy regulations, for example, organizations must demonstrate control over back end system access. Compliance usually requires documentation. PAM enables the organization to document how it defines and enforces privileged access controls.

PAM also provides logs of privileged sessions for use in compliance audits.

Why Privilege Access Management?

(on other regulations)

- **GDPR** Article 29 requires data controllers to only have access to the data they need to perform their tasks)
- **HIPAA** requires restricted access and used of healthcare data based on user function)
- **PCI-DSS** requires that users have privileged access to only the minimum data required to perform their functions)

WALLIX PAM4ALL

Unified Privilege Solution to Secure, Control and Manage any ACCESS for every:

- User
- Session
- Asset
- Endpoint

At just the right time. Anywhere.

Managed services

Paris
Headquarters

2003
Operate since

11 patents
Innovation

2020
clients served

300
distributors & integrators

90
countries

> € 23 m
2021 turnover

Euronext
ALLIX

220
Employees

Gartner

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

ANSSI
CSPN

A solution with unified privilege management components for **SOLVING ACCESS CHALLENGES**!

WALLIX
PAM4ALL
On premise / Hybrid / SaaS

Multi-Factor Authentication

Enhance Security

Neutralize the risk

Session Management

Advanced session monitoring

Maintain compliance

Remote Access Management

Manage privileged remote access

Seamless experience for employees & vendors

Password Management

Control and manage secrets, passwords and credentials

Prevent exposure

Least Privilege Management

Least privilege, dynamic elevation, grant the right privilege

Remove local admin rights & block lateral movement

WALLIX
CYBERSECURITY SIMPLIFIED

ANY QUESTION?

WALLIX
CYBERSECURITY SIMPLIFIED

WALLIX

Thank you!

250 bis, rue du Faubourg Saint-Honoré
75008 Paris, France

+33 1 53 42 12 81
info@wallix.com