KPMG

# A world of privileges

**TIIME Workshop**

**Juan Manuel Zarzuelo Díaz**

**February 2020**

# Contents

# 1. Introduction

# Context

The know as **“Zero Trust” model** was establish on the market back in 2010, with the idea that every organization should not trust (automatically) any connection to its systems, coming from outside or inside. Everything must be verified. At that time, the infrastructure, data and the users were mostly inside the network, so the biggest efforts were done in **perimeter security**. Golden age of firewalls and VPNs. Also, the processes were quite manual, relying the activities on **human interventions**, so the typology of users and permissions was simpler.

Nowadays, on the cloud computing era, with the users working remotely in different locations and the incremental use of robots to automate manual processes, the ecosystem has changed entirely, increasing the attack surface and the risks due **the perimeter is undefined and the users are not anymore just humans**.

**It is the right moment to take control over the keys of our kingdom.**

KPMG

# 2. The privileged account landscape

# Types of privileged accounts

**There are 6 main different privileged accounts based on the usage and the scope:**


**Local administrative accounts** are non-personal accounts which provide administrative access to the local host or instance only

**Privileged user accounts** are named credentials which have been granted administrative privileges on one or more systems.

**Domain administrative accounts** have privileged administrative access across all workstations and servers within the domain.

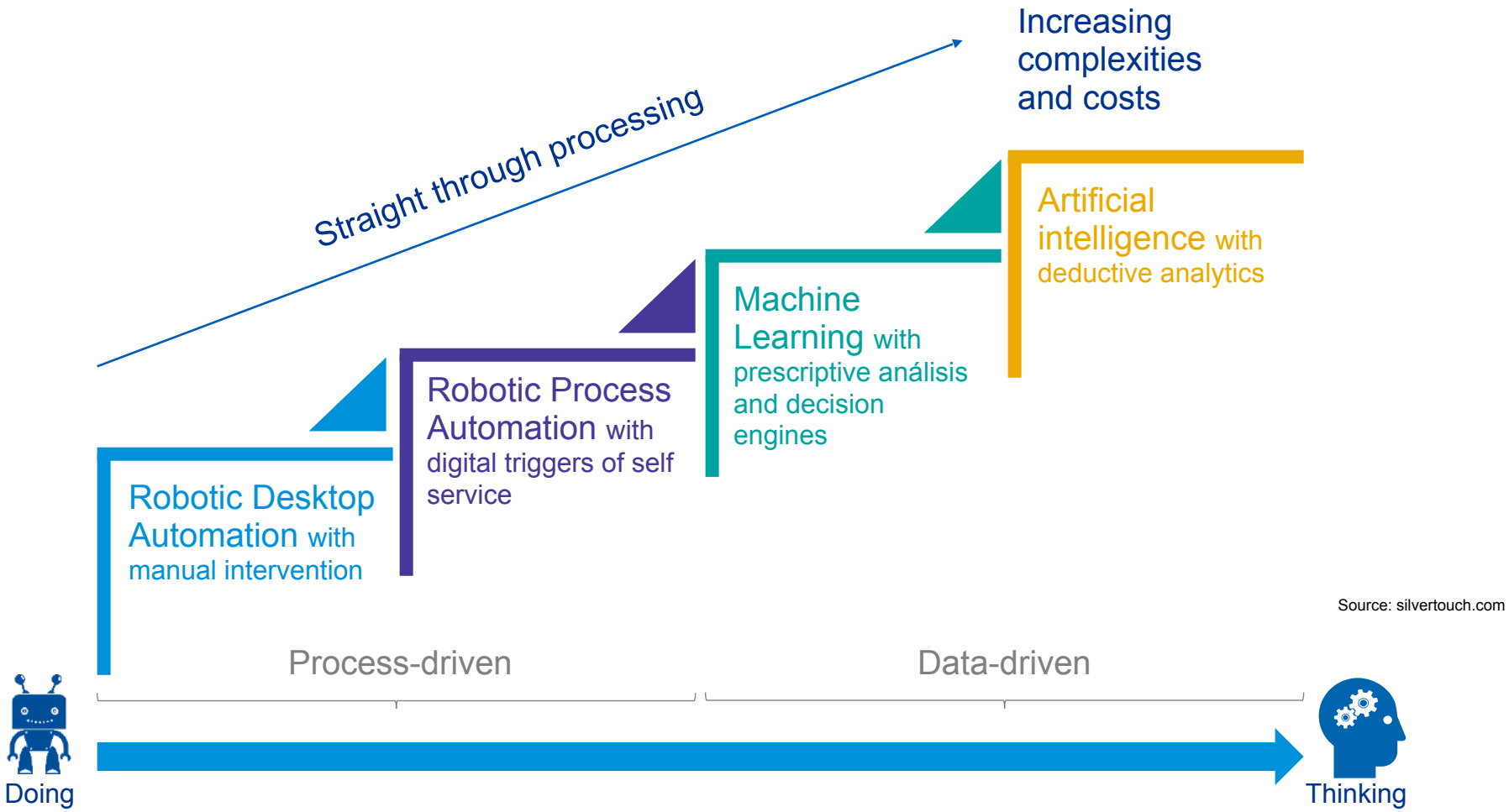
**Emergency accounts** provide unprivileged users with administrative access in the case of an emergency (firecall / breakglass).

**Generic accounts** are any account that is shared or is not tied to a specific user.

**Service accounts** can be privileged local or domain accounts that are used by an application or service to interact with the operating system, to access databases, run batch jobs or scripts, or provide access to other applications.

# What do we mean with robots?

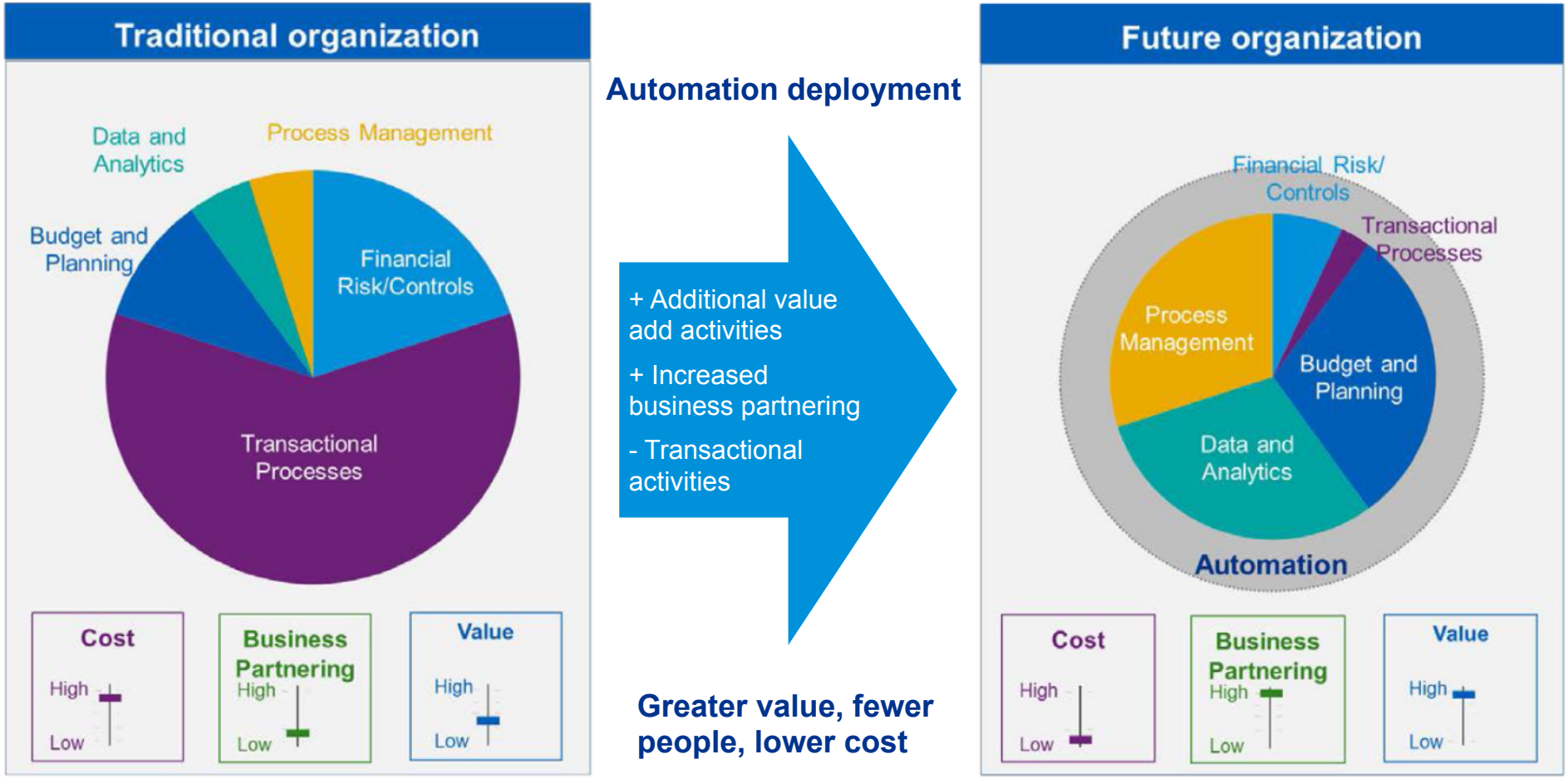
**There are 4 different types of automation:**




Source: silvertouch.com

# The future of finance

**Extreme process automation will allow finance to transcend its transactional role, resulting in enhanced business partnering and value delivery through insight generation.**



# Extreme automation

**The finance technology ecosystem will continue to evolve and be integrated.**

## Data Management

Data management will no longer be an aggregation of performance data; new data sources will be used to drive deeper prescriptive insights.

## Blockchain

Blockchain will accelerate transaction recognition and provide enhanced security, lesser storage requirements and shorter deliver cycle times.

## Cloud

Cloud technologies will bring the ability to select best-in-class application solutions, real-time data accessibility and business partnering capabilities.

## Robots

RPA will drive “extreme automation” within rules-based processes resulting in greater capacity for value-added activities.

## Machine learning

Adaptive technologies will radically change the work through the use of smart algorithms that can be leveraged to accomplish activities and tasks.

## Cognitive

Cognitive technologies will advance automation past execution, through the ability to infer trends and patterns from structured and unstructured data

## Natural language processing

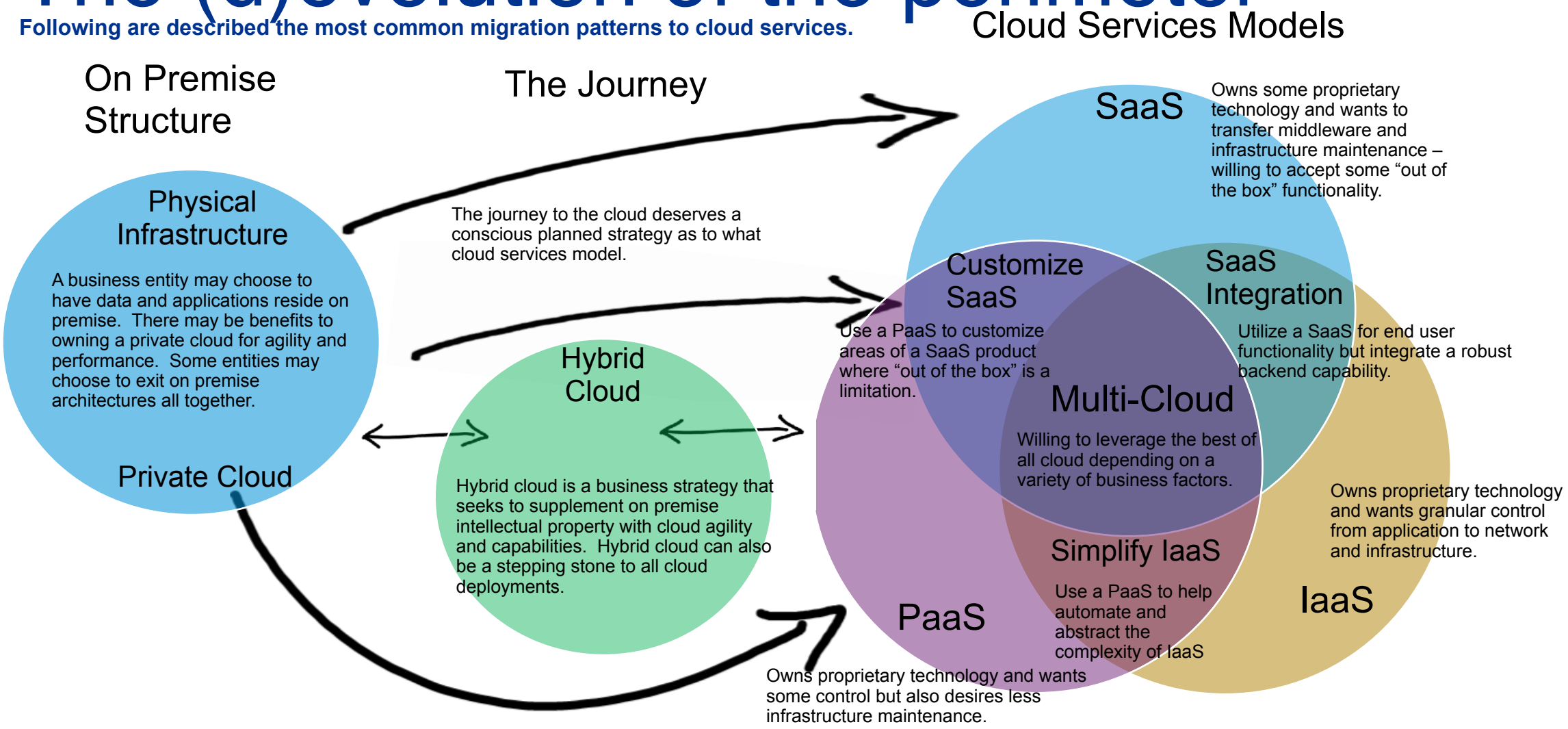
NLP will provide unconstrained, real-time information accesibility, beyond just the numbers.

## Digital analytics and delivery

Results will be delivered real-time, driving accelerated decisión-making capabilities, influencing positively business outcomes.

# The (d)evolution of the perimeter

**Following are described the most common migration patterns to cloud services.**



# 3. Main triggers and concerns

# Top 5 CISO priorities and Top 10 Security projects

As the feedback offer by CISOs on different reports, the ecosystem evolution is the tri[illegible] mo[illegible] important concerns CISOs have. F[illegible] 5 are listed:

1. **Identity Manag[illegible]ment in a Mu[illegible]**
2. **Protecting As[illegible]ts w[illegible]h Encr[illegible]on and Zer[illegible] Trust**
3. **The Rise of DevSecOps**
4. **Responding to "Alert Fatigue“**
5. **Educating Employees to Think Like a CISO**

On the other hand, as the market studies performed by researchers, the following are the top 10 security projects for the following year:

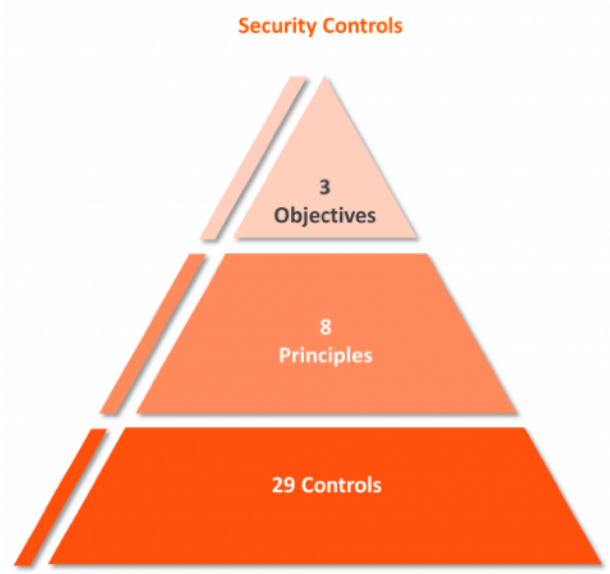
1. **[illegible]ged [illegible] management (PAM)**
2. **[illegible] [illegible]de[illegible]it [illegible]anagement**
3. **[illegible]e[illegible]ng[illegible]on**
4. **[illegible]oud [illegible]ess [illegible]uri[illegible] b[illegible]ke[illegible] (C[illegible]SB)**
5. **Cloud security posture management (CSPM)**
6. **Business email compromise**
7. **Dark data discovery**
8. **Security incident report**
9. **Container security**
10. **Security rating services (SRS)**

# SWIFT Customer Security Programme

The growing threat of cyberattacks has never been more pressing. Recent instances of payment fraud in SWIFT customers' local environments demonstrate the necessity for industry-wide collaboration to fight against these threats.

**SWIFT customers are individually responsible for the security of their own environments**, however, the security of the industry as a whole is a shared responsibility. As an industry cooperative, SWIFT is committed to playing an important role in reinforcing and safeguarding the security of the wider ecosystem.

SWIFT have therefore launched the Customer Security Programme (CSP), which aims to improve information sharing throughout the community, enhance SWIFT-related tools for customers and provide a customer security control framework. Through the programme, best practices are shared for fraud detection and enhance support by third party providers.

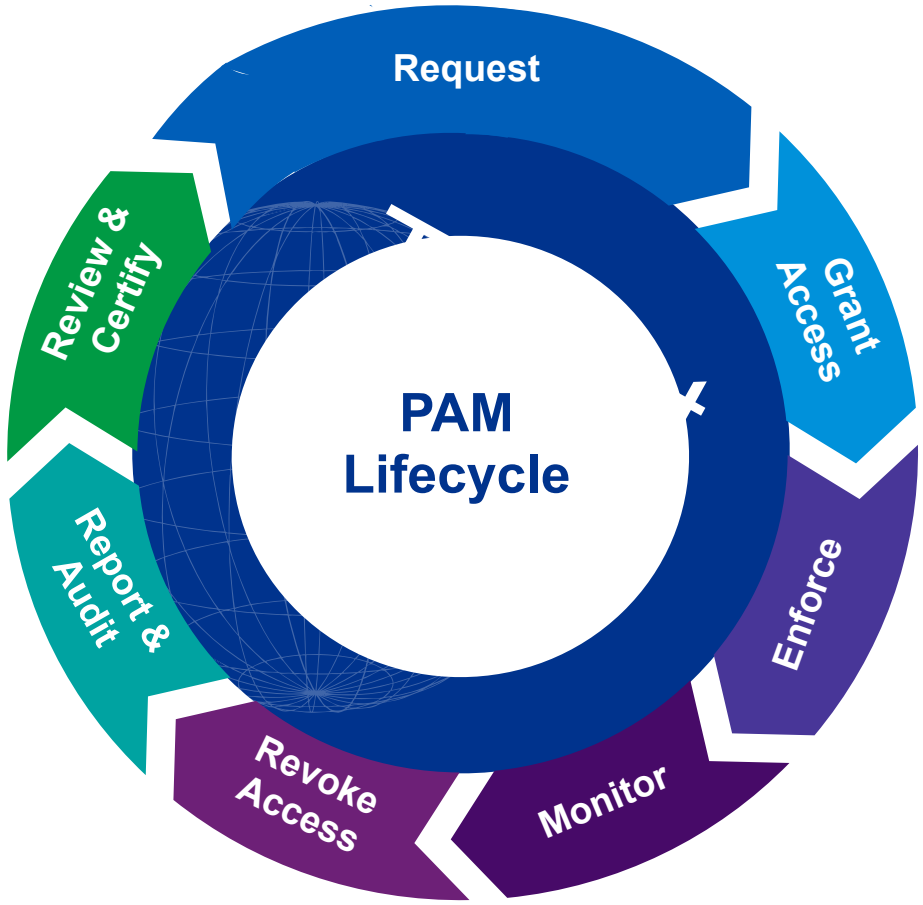



| CSP Security Controls Framework (combines 1 & 2) | | |
|---|---|---|
| Secure Your Environment | 1. | Restrict Internet access |
| | 2. | Segregate critical systems from general IT environment |
| | 3. | Reduce attack surface and vulnerabilities |
| | 4. | Physically secure the environment |
| Know and Limit Access | 5. | Prevent compromise of credentials |
| | 6. | Manage identities and segregate privileges |
| Detect and Respond | 7. | Detect anomalous activity to system or transaction records |
| | 8. | Plan for incident response and information sharing |

# SWIFT Customer Security Programme

| Objectives | Principles | Security Controls |
|---|---|---|
| **Secure your Environment** | 1. Restrict Internet Access and Protect Critical Systems from General IT Environment | **1.1 SWIFT Environment Protection**<br>**1.2 Operating System Privileged Account Control**<br>1.3A Virtualisation Platform Protection |
| | 2. Reduce Attack Surface and Vulnerabilities | 2.1 Internal Data Flow Security<br>2.2 Security Updates<br>2.3 System Hardening<br>2.4A Back Office Data Flow Security<br>2.5A External Transmission Data Protection<br>**2.6 Operator Session Confidentiality and Integrity**<br>2.7 Vulnerability Scanning<br>2.8A Critical Activity Outsourcing<br>2.9A Transaction Business Controls<br>2.10A Application Hardening |
| | 3. Physically Secure the Environment | 3.1 Physical Security |
| **Know and Limit Access** | 4. Prevent Compromise of Credentials | **4.1 Password Policy**<br>**4.2 Multi-factor Authentication** |
| | 5. Manage Identities and Segregate Privileges | **5.1 Logical Access Control**<br>**5.2 Token Management**<br>**5.3A Personnel Vetting Process**<br>**5.4 Physical and Logical Password storage** |
| **Detect and Respond** | 6. Detect Anomalous Activity to Systems or Transaction Records | 6.1 Malware Protection<br>6.2 Software Integrity<br>6.3 Database Integrity<br>**6.4 Logging and Monitoring**<br>**6.5A Intrusion Detection** |
| | 7. Plan for Incident Response and Information Sharing | 7.1 Cyber Incident Response Planning<br>7.2 Security Training and Awareness<br>7.3A Penetration Testing<br>7.4A Scenario Risk Assessment |

# Governance – PAM lifecycle




| | |
|---|---|
| **Request** | User ask for access to a determinate system to do a privileged action |
| **Grant access** | After approval , user account is provision or granted with determinate privileges in the target system |
| **Enforce** | Ensure privileged account policies are properly applied |
| **Monitor** | Control and record of privileged sessions and/or actions |
| **Revoke access** | Access/ Permission requested for user is ended (end of session, permissions revoke...) |
| **Report & audit** | Send privileged account information to SOC / SIEM team |
| **Review & certify** | Verification of appropriated access/ permission is granted to authorized user |
| **Threat analytics** | Detect, alert, and respond to anomalous privileged activity indicating an in-progress attack. |

# 4. The PAM journey

# Program benefits

**Secure your credencials**
Use the vault to store your credencials creating a proper role model

**Automatic password rotation**
Rotate your credentials based on policies that fits each different asset

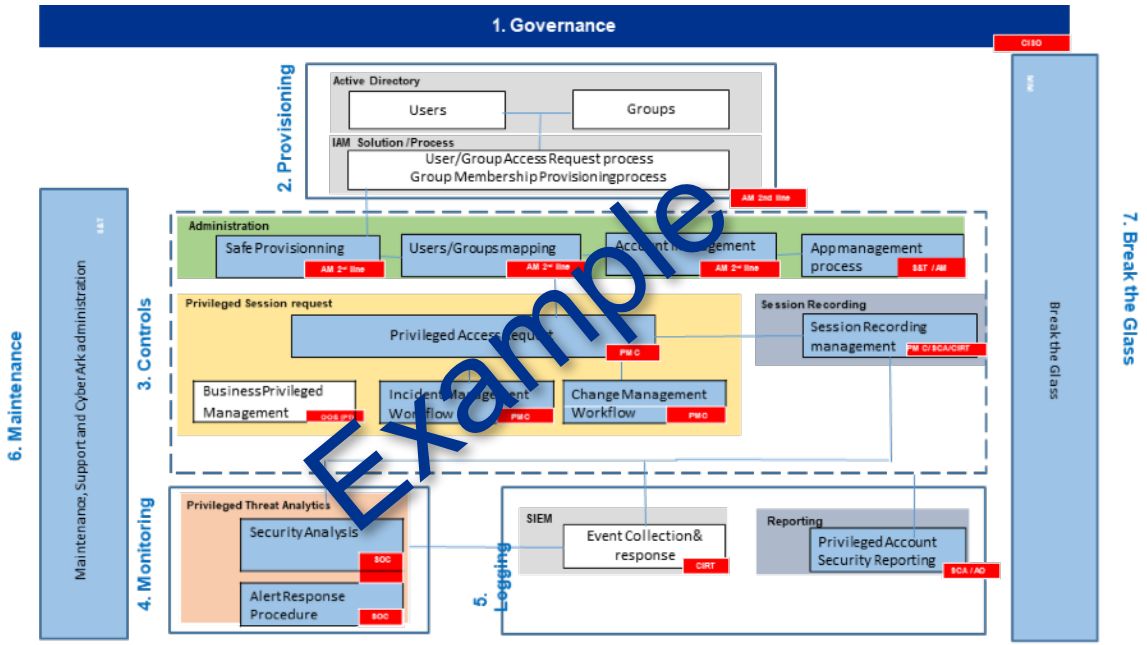
**Secure session isolation**
Offer secure channels to privileged users to register and monitor activity

**Threat analytics and intelligence**
Integrate the PAM solution with the SIEM will bring great benefits

**Cloud security and service accounts protection**
Protect cloud assets (IaaS) and accesses to cloud services (SaaS/PaaS). Onboard service accounts in the vault and establish rotation policies to avoid hard-coded credentials

# Program governance

## Target Operating Model (TOM)




## PAM Main Processes

1. **Privileged access request (change request):** requesting a Privileged Account in a timely manner, for the realization of a registered and accepted change request, in a specific target system. The process involves the responsible of the asset as approver and a timeframe.
2. **Privileged access request (incident)**: describes the steps necessary for an administrator to obtain a Privileged Account required to resolve an incident. It is primary to reduce the time required to obtain the account, monitoring for a correct use.
3. **Privileged account management (create/delete/modify)**: indicates the right workflows and approvals for the lifecycle management of a Privileged Account.
4. **Users and groups mapping**: aims to avoid duplication in the creation of groups so the administration is more efficient.
5. **Access model**: based on the previous mapping, definition of the rights and permissions on the different groups.
6. **Disaster recovery:** details the steps to follow when the PAM solution does not respond and its backup must be used, making the information available again at the shortest time.
7. **Break the glass:** instructions to follow in case of a critical incident in which the PAM solution is not available and the Disaster - Recovery process cannot be applied.

# Top 5 warning signs of failed PAM programs

1. Lack of an executive level sponsor and a governance structure
2. PAM is not accepted as a critical business function
3. Key decisions avoided or postponed, not followed through or not driven by business strategy and risk
4. Limited or no user adoption
5. Limited or no understanding of ongoing nature of PAM controls

# PAM guidelines for success

1. **Develop a strategy** that is aligned to the needs of the business and considers people, processes and technology issues
2. **Don't think of PAM as an IT-only initiative**, especially when it addresses business usage and regulatory requirements
3. **Be strategic**, not tactical, when planning and designing a solution
4. Because PAM is pervasive, be prepared for objections and concerns during any transformation process
5. Avoid the **Big Bang** approach; use a risk-based, phased implementation approach to ease the integration and adoption of PAM changes
6. **Don't rush to buy** and implement a tool without first considering the necessary business and process transformation requirements
7. **Create an inventory** of applications, systems and definition of business friendly access roles (profiles) (this will take longer than expected)

KPMG

# 5. Ready to success

# The value from working with KPMG

**The selection of a partner for your Cyber programmes is crucial and one that will have a significant influence on determining your success. We have set out below the value you will gain from working with KPMG.**

**The following slides describe our capabilities and illustrate a sample approach to a successful end to end delivery.**

## Trusted brand

- We are a **recognised and trusted brand** to your board and this will install confidence that your programme will deliver the required outcomes and business benefits.
- We have **relationships with senior stakeholders** across many organisations and can be influential around the board table to ensure key messages are clearly communicated and understood.
- We will have **credibility with business stakeholders** and this will enable us to deliver the required change.
- We are an **award winning cyber security consultancy** and take great pride in being recognised by Forrester **as a leader in the market**. We have achieved this through delivering to high quality standards and you can be assured our deliverables will be delivered to these standards.

## Track record of delivery

- We have successfully delivered projects in privileged access management, data privacy, identity access management, and Network security to clients **across all sectors**.
- We have **refined tools and methodologies** with key artefacts such as tailored questionnaires, data analysis techniques, planning tools and costing templates.
- Our methodologies and tools have been used on multiple projects, have evolved through this experience and as a result have helped illicit rapid Business benefit.
- We understand the complexities involved in projects of this nature and our methodologies will help you **navigate the pitfalls upfront and throughout**, making sure you get the right high level implementation plans.

## insights

- We have a **dedicated cyber security and privacy transformation practice** focused on helping our clients to fix their most complex and challenging issues.
- We have facilitated a cyber security benchmark study for several insurance and global banking clients. Through **our i-4 organisation** we also have access to the approaches being taken by clients across a range of industries and will capture these in our advice.
- Our **People and Change practice** ensures that technology programmes have a human face, encompassing the impact of change on all those affected, ensuring organisations plan, communicate, educate and support their staff to drive successful adoption.

KPMG

# Contacts

# Contacts

**The contacts at KPMG in connection with this document are:**

**Juan Manuel Zarzuelo**

Technology Risk

Director, KPMG Asesores S.L.
M: +34 618 899 666
E: jzarzuelo@kpmg.es

kpmg.es