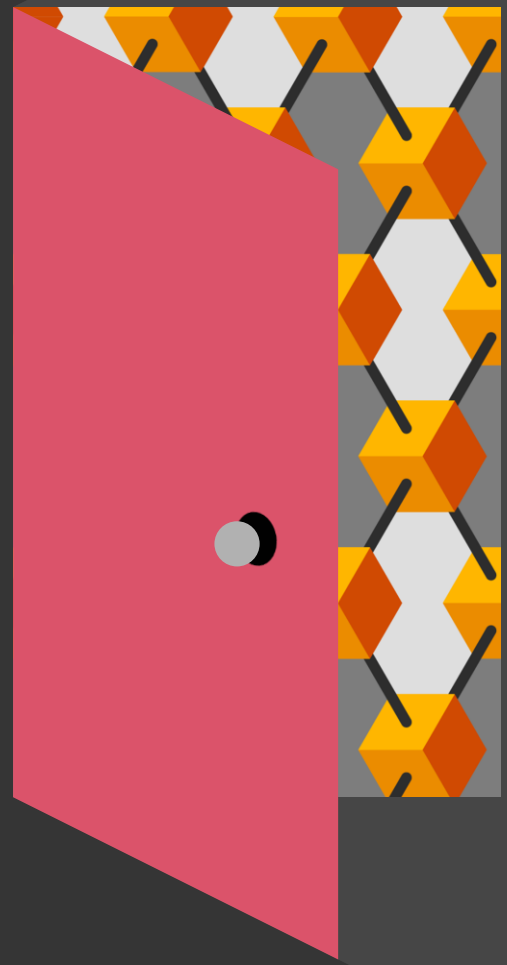
# NIS2 PAM

Præsentation af Lukas Pavka and Kim Buchwald Mikkelsen, PwC DK



pwc

# Table of contents



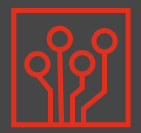
# The NIS2 Directive provides legal measures to boost the overall level of cyber security in the EU

## Why? State of the cyber threat

NIS was created in response to the increased digitization of the society and increasing number of incidents that poses an immense threat to our critical infrastructure. NIS2 repeals and replaces the Network and Information Systems Directive (EU) 2016/1148 (NIS1), aiming to achieve a high common level of cybersecurity across the EU, with a focus on protecting critical infrastructure.

## What? Extended scope

NIS2 expands the definition of critical sectors in society and imposes significantly heightened cybersecurity requirements on businesses and public authorities associated with these sectors.



## Obligations

NIS2 will be implemented as executive orders (bekendtgørelser) nationally in Denmark, which makes it obligatory for organisations and authorities to be compliant to the law. NIS 2 introduces cyber risk management, incident reporting, and information-sharing obligations for specific organizations across various sectors.

## Opportunity

It brings obligations, but it also creates opportunities for getting security initiatives into the roadmap and get funding approved with more management attention nowadays for the compliance with the NIS2 and other recent regulations.

# Main NIS2 requirements

## NIS2 introduces stricter cybersecurity & risk management requirements

NIS2 Article 21 directs member states to ensure that essential and important entities manage risk by implementing robust systems, policies and best practices covering a wide range of cybersecurity measures and disciplines including:

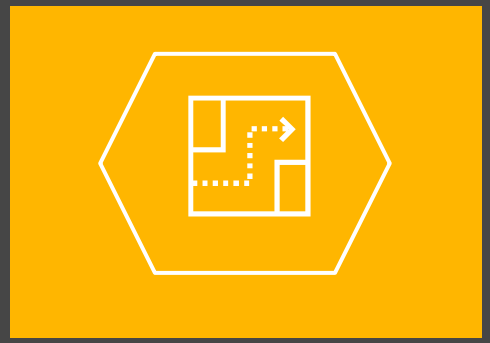
- Risk analysis and information system security
- Incident handling and reporting
- Business continuity, such as backup management and disaster recovery
- Crisis management
- Supply chain security
- Systems acquisition, development and maintenance security
- Basic cyber hygiene practices and cybersecurity training
- Cryptography and encryption technologies
- Human resources security, access control policies and asset management
- Zero Trust access (multifactor authentication, continuous authentication)

# Get ahead of the curve – Assess and plan

*”Organizations without a formal program will spend 40% more on IAM capabilities while achieving less than organizations with such programs.”* – Gartner

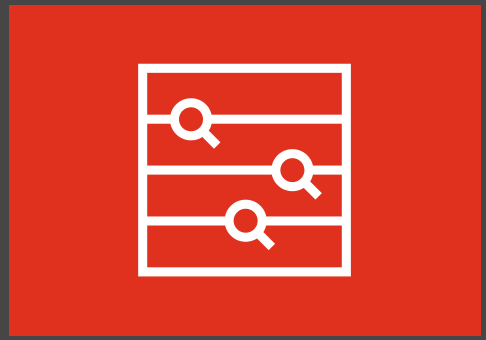
## Current state assessment

1. Conduct an As-Is assessment
2. Identify gaps against the requirements
3. Develop assessment methodology
4. Classify the gaps and map them to concrete parts of your organization
5. Develop an inventory and update it regularly with progress



## Strategy and roadmap for closing the gaps

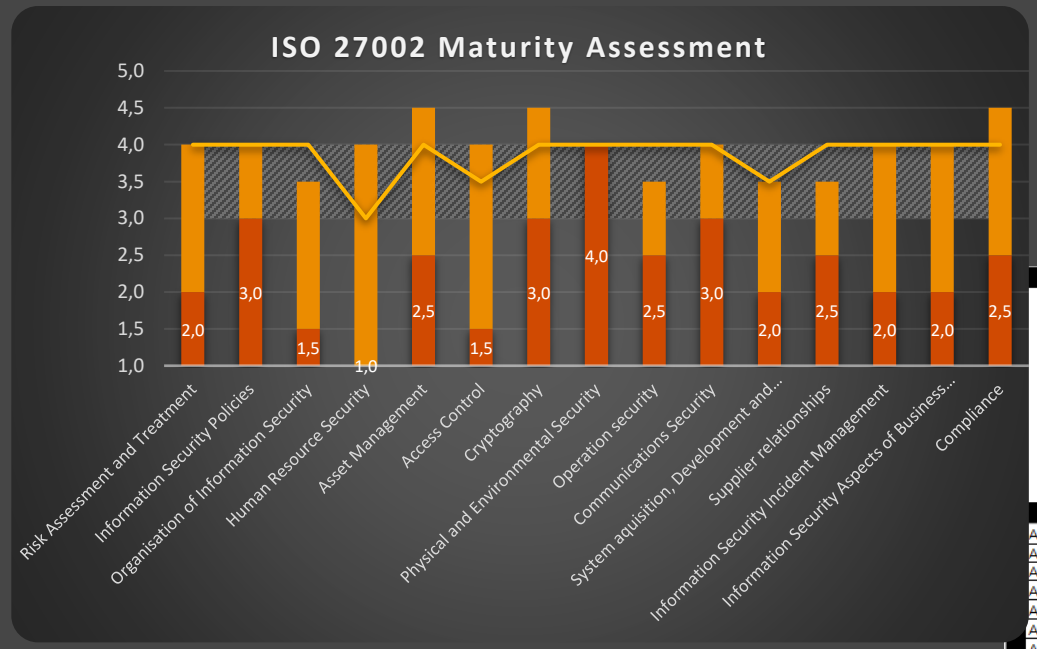
1. Analyze the identified gaps
2. Prioritize the findings based on risks, complexity to implement and importance against NIS2 requirements
3. Define the future state
4. Update Enterprise strategy
5. Gaps mitigation roadmap with timelines for each gap



## Continuous risk assessments

1. Define the process to continuously evaluate your risks
2. Regularly perform the assessments and document progression and new gaps identified
3. Document results of each iteration
4. Update Roadmap and Strategy accordingly

# Example assessment




| ISO 27001 Clauses: | | 4 | A5 | A6 | A7 | A8 | A9 | A10 | A11 | A12 | A13 | A14 | A15 | A16 | A17 | A18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Risk | Information security policies | Organisation of information security | Human resource security | Asset management | Access control | Cryptography | Physical and environmental security | Operations security | Communications security | System acquisition, development and maintenance | Supplier relationships | Information security incident management | Information security aspects of business continuity management | Compliance |
| NIS2 ref. | NIS 2 directive | | | | | | | | | | | | | | | |
| Art 11.5 | Requirements, technical capabilities and tasks of CSIRTS | | | X | | | | | | | | | | | | |
| Art 20.1 | Managment approval of cybersecurity risk-management measures | X | | X | | | | | | | | | | | | |
| Art 20.2 | Training and education of management | | | | X | | | | | | | | | | | |
| Art 21.2(a).1 | policies on risk analysis and i | X | | | | | | | | | | | | | | |
| Art.21.2.(a).2 | Information system security policies | | X | | | | | | | | | | | | | |
| Art.21.2.(b) | Incident handling | | | | | | | | | | | | | X | | |
| Art.21.2.(c).1 | Business continuity | | | | | | | | | | | | | | X | |
| Art.21.2.(c).2 | Backup management | | | | | | | | | X | | | | | | |
| Art.21.2.(c).3 | Disaster recovery/crisis management | | | | | | | | | | | | | | X | |
| Art.21.2(d) | Supply Chain Security | | | | | | | | | | | | X | | | |
| Art.21.2(e).1 | Network security (acquisition, development and maintenance) | | | | | | | | | | | X | | | | |
| Art.21.2(e).2 | Network security (vulnerability handling and disclosure) | | | | | | | | | X | | | | | | |
| Art.21.2.(f) | Policies and procedures to assess the effectiveness of cybersecurity risk ma | X | X | | | | | | | | | | | | | |
| Art.21.2.(g) | Basic cyber hygiene practices and cybersecurity training | | | | X | | | | | | | | | | | |
| Art.21.2.(h) | Policies and procedures regarding the use of cryptography | | | | | | | X | | | | | | | | |
| Art.21.2.(i).1 | Human resource security | | | | X | | | | | | | | | | | |
| Art.21.2.(i).2 | Access control policies | | | | | | X | | | | | | | | | |
| Art.21.2.(i).3 | Asset management | | | | | X | | | | | | | | | | |
| Art.21.2.(j).1 | Multi-factor authentication or continuous authentication solutions | | | | | | X | | | | | | | | | |
| Art.21.2.(j).2 | Secured voice, video and text communications | | | | | | | | | | X | | | | | |
| Art.21.2.(j).3 | Secured emergency communications systems within the entity, where appropriate | | | | | | | | | | | | | | X | |
| Art.23.1 | Report incident to competent authority/CSIRT | | | X | | | | | | | | | | | | |
| Art.32.2 | Supervision and enforcement measures in relation to essential entities | | | | | | | | | | | | | | | X |
| Art.33.2 | Supervision and enforcement measures in relation to important entities | | | | | | | | | | | | | | | X |
| Para 58 | The manufacturer or provider of ICT products or services should also put in place the necessary procedures to receive vulnerability information from | | | | | | | | | X | | | | | | |
| Para 77 | Responsibility of promoting and implementing cybersecurity risk managemen | X | | | | | | | | | | | | | | |
| Para 79 | Physical security | | | | | | | | X | | | | | | | |
| Para 82 | Cyber risk management measures should be proportionate to risk exposure | X | | | | | | | | | | | | | | |
| Para 85 | its relationship with its suppliers, such as providers of data storage and processing services or managed security services and software editors, is | X | | | | | | | | | | | X | X | | |

# IAM and PAM directly enhances an organizations ability to comply with the following ISO2700x controls

**Introduction to ISO2700x**

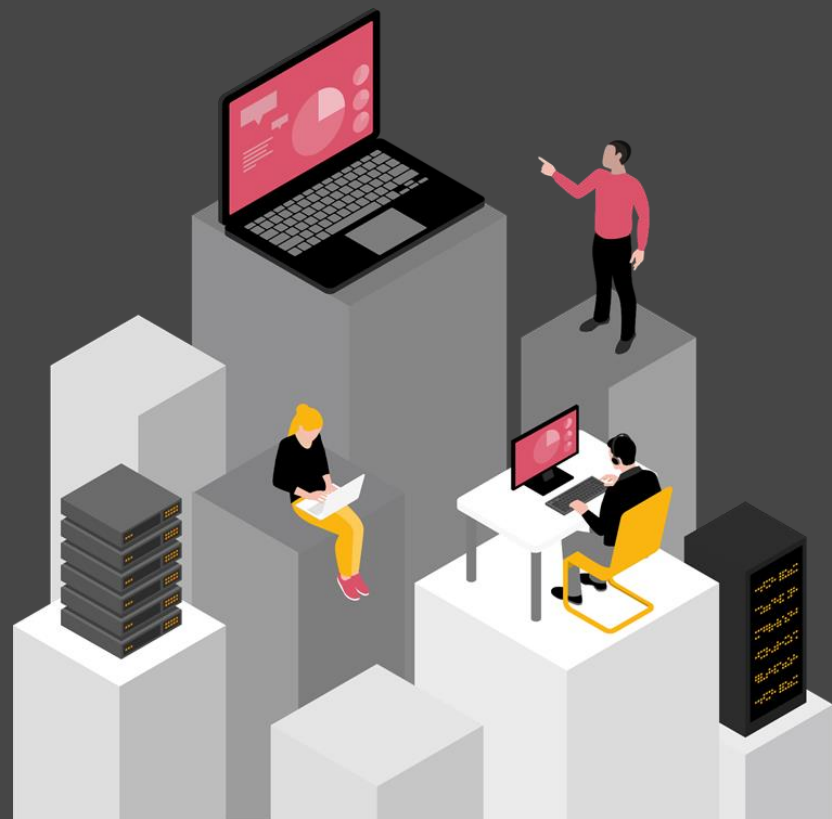
The use-case of ISO 2700X in relation to Identity and Access Management (IAM) and Privileged Access Management (PAM) is to provide a structured framework and guidelines for organizations to establish robust security controls, risk management processes, and continuous improvement practices to ensure the confidentiality, integrity, and availability of information assets related to identity and access management, including privileged accounts and access rights. It helps implementing the information security controls based on internationally recognized best practices

- ISO 27002:2022 5.3 - Segregation of Duties
- ISO 27002:2022 5.15 - Access Control
- ISO 27002:2022 5.16 - Identity management
- ISO 27002:2022 5.17 - Authentication information
- ISO 27002:2022 5.18 - Access rights
- ISO 27002:2022 8.2 - Privileged Access rights
- ISO 27002:2022 8.3 - Information Access restrictions
- ISO 27002:2022 8.5 - Secure authentication
- ISO 27002:2022 8.15 - Logging

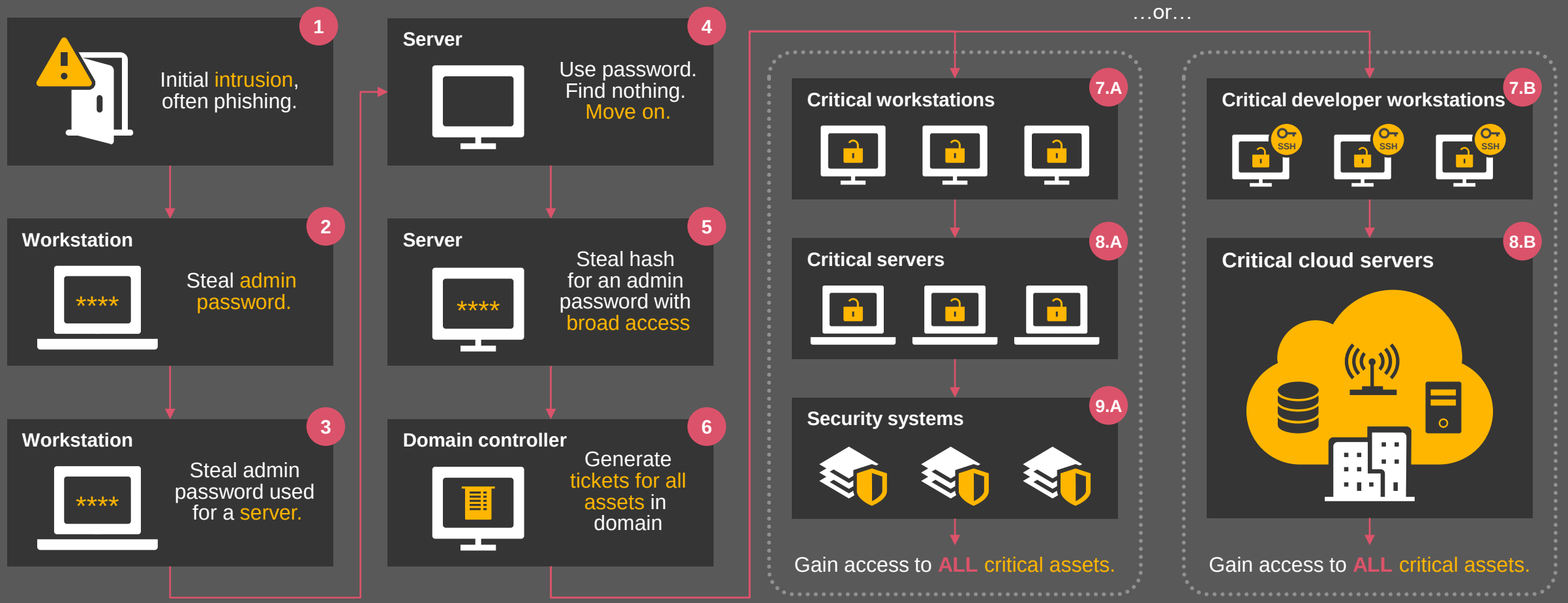
**IAM & IGA** – supporting most of the above policies, including segregation of duties, access control, access rights and identity management in general

**PAM** - supporting most of the above policies, including Information Access restrictions, secure authentication and logging

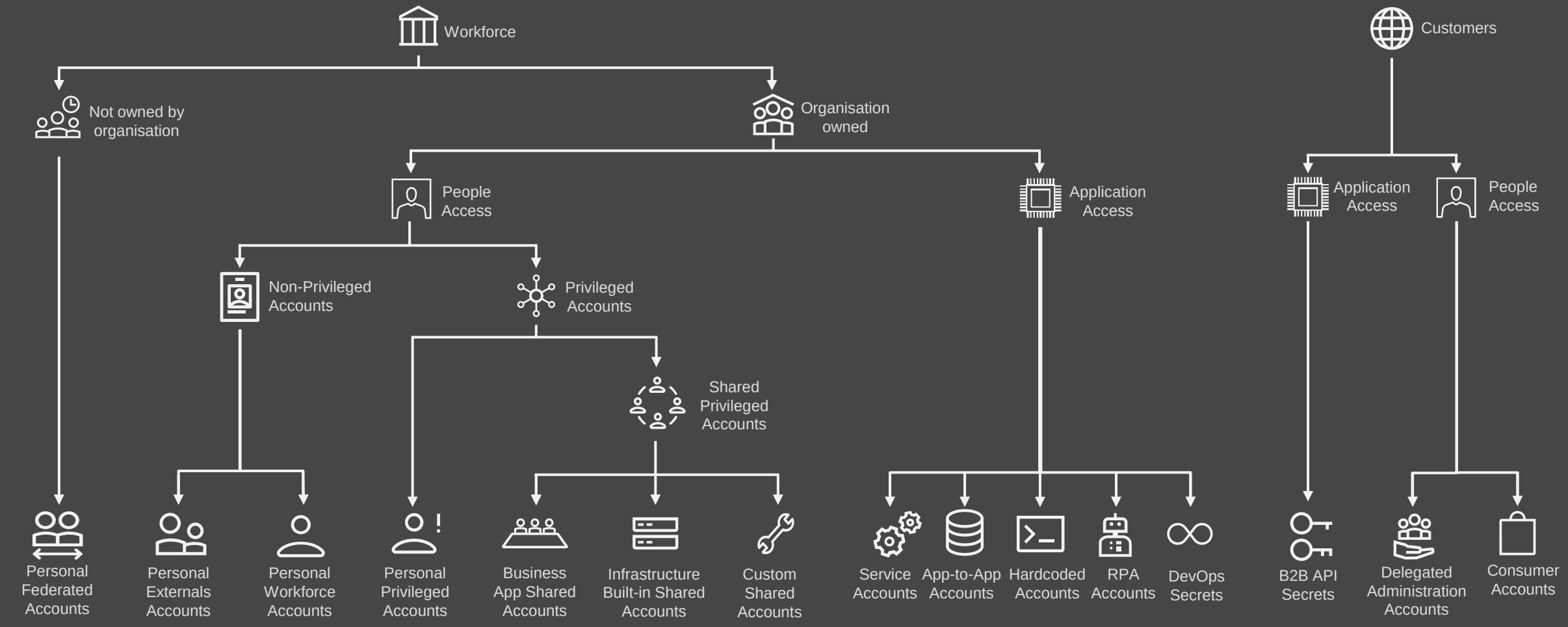
**Endpoint privilege management** - supporting segregation of duties, access control and information access restrictions, protect against ransomware and allow effective detection and reporting capabilities



# The privilege pathway to the domain controller and beyond to the cloud

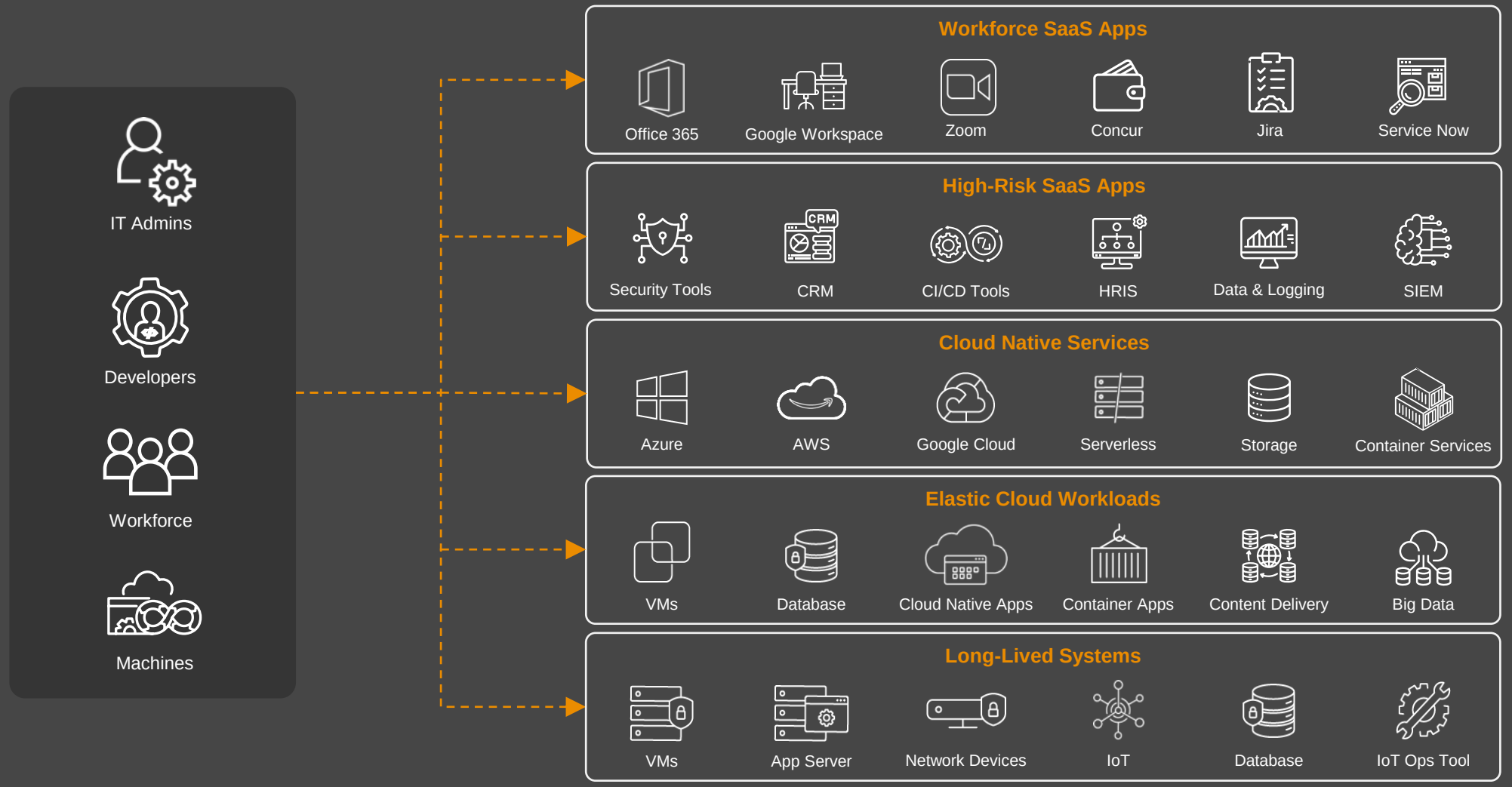


# Identities across organization



# Identities across Environments

## New identities, new environments, new attack methods



# Risk based approach

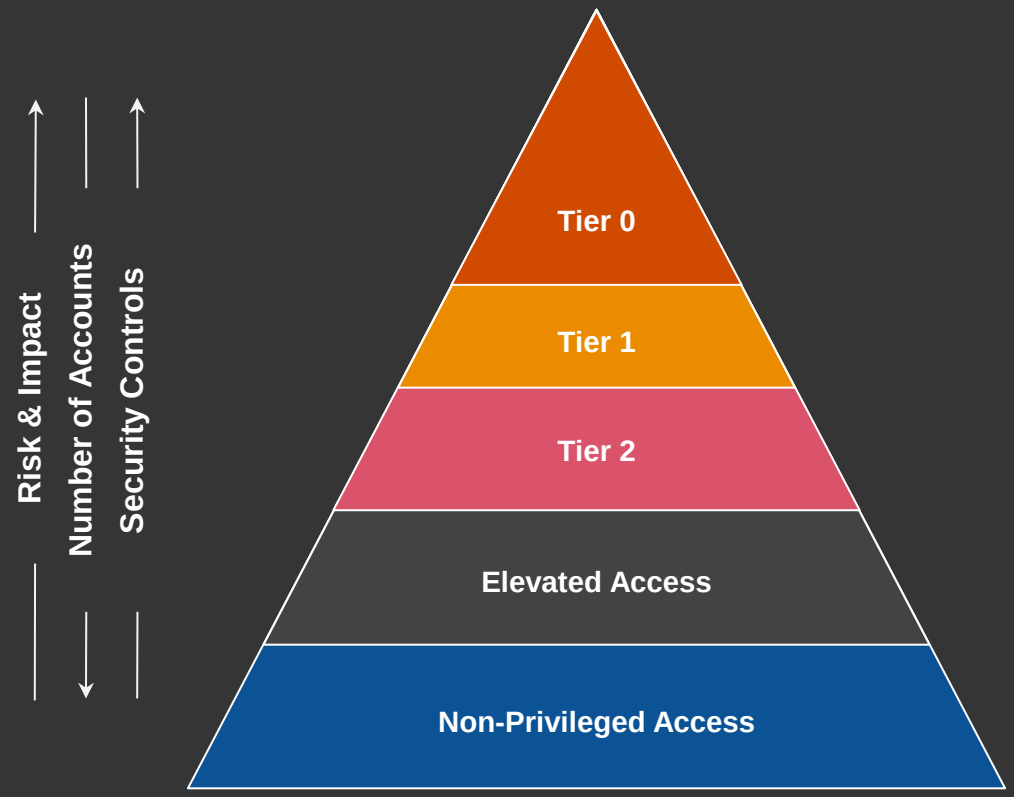
Almost every attack starts by taking over the identity of an account within the breached organization.

Having automated streamlined IAM processes is a key to protect your assets and to allow efficient work for your employees and to be compliant with all regulatory and audit requirements

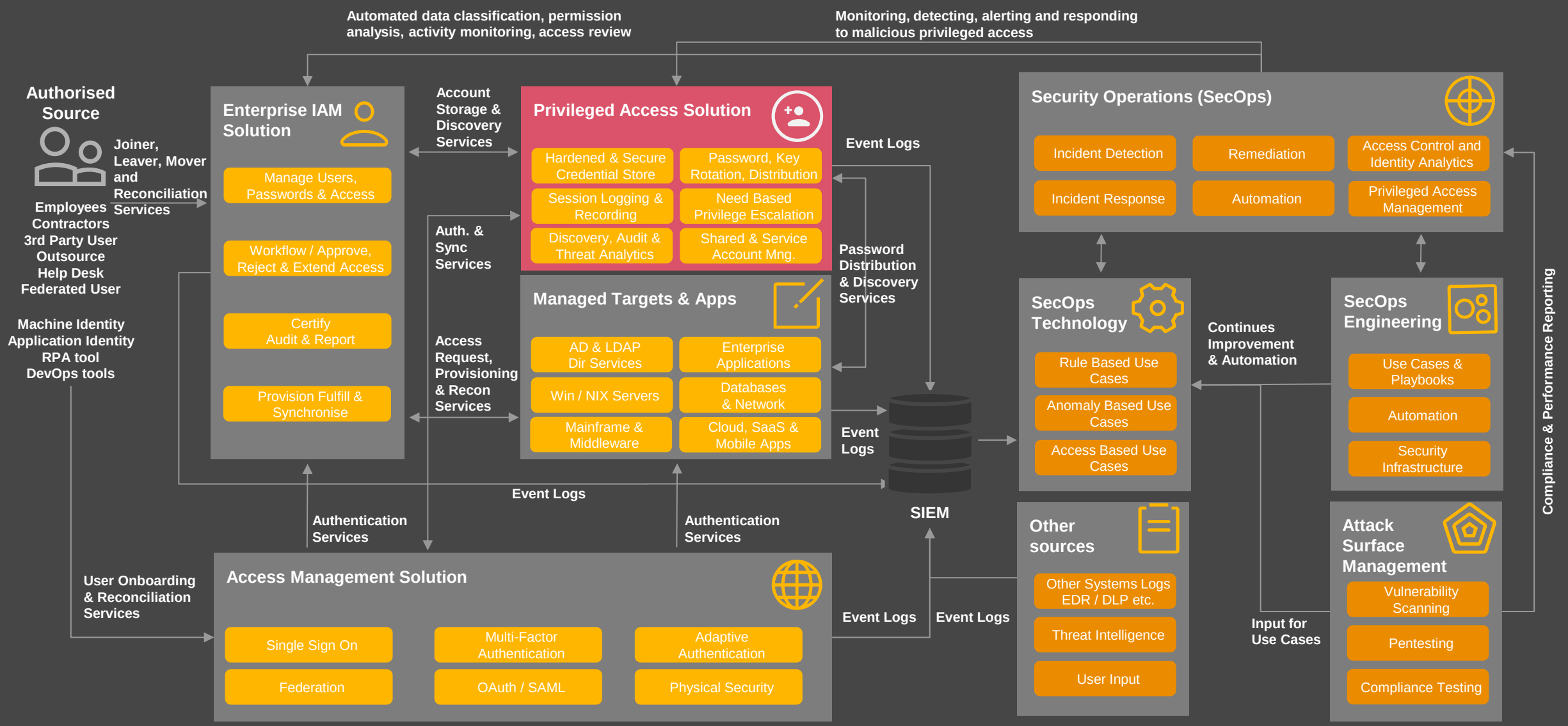
## Before enforcing controls

Below are some key considerations to be made before enforcing controls:

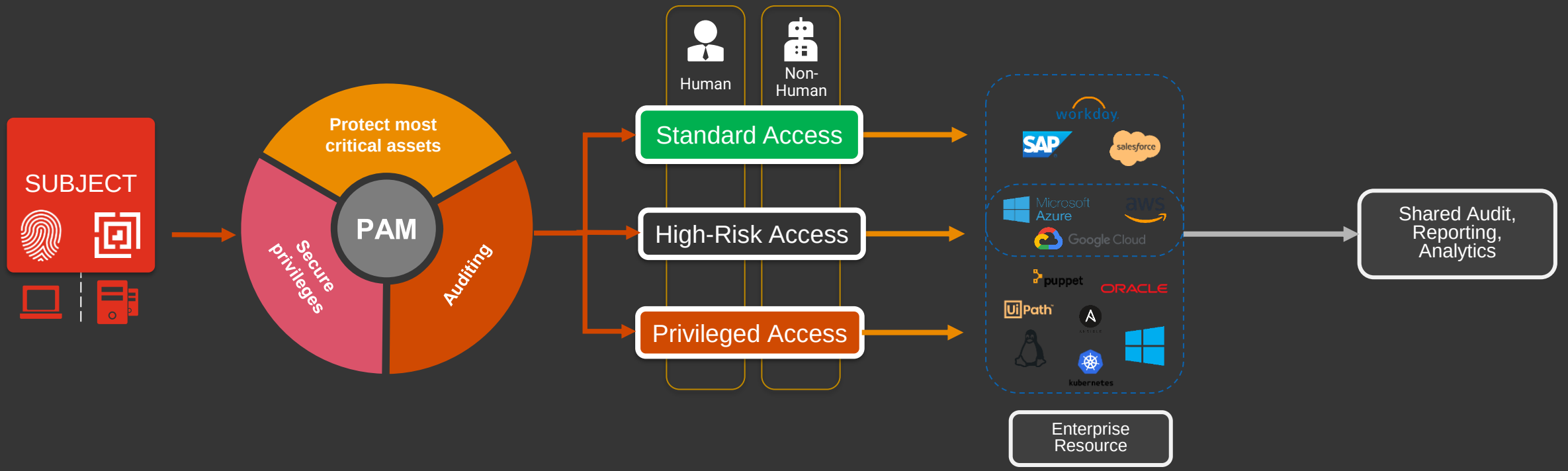
- Discovery of privileged access
- Identification of tiers based on tiering matrix
- Hygiene Exercise on accounts
- Updating the controls model to meet the standards
- Finalizing the tools for enforcing controls
- Setting up necessary integrations to allow enforcement



# Integrated Identity Security



# Identity security enabling zero trust




### STRONG ADAPTIVE VERIFICATION

- Establish Device Trust
- Adaptive Multi-Factor Authentication
- Adaptive Single-Sign On
- Endpoint Privilege Protection

### CREDENTIAL & AUTHENTICATION PROTECTION

- Protect Authentication Tokens
- Protect Credential Caches
- Manage Local Admin Credential

### CONTINUOUS APPROVAL AND AUTHORIZATION

- Identity Provisioning
- Approval Processes
- Life Cycle Management
- Automated Provisioning

### SECURED, LEAST PRIVILEGE ACCESS

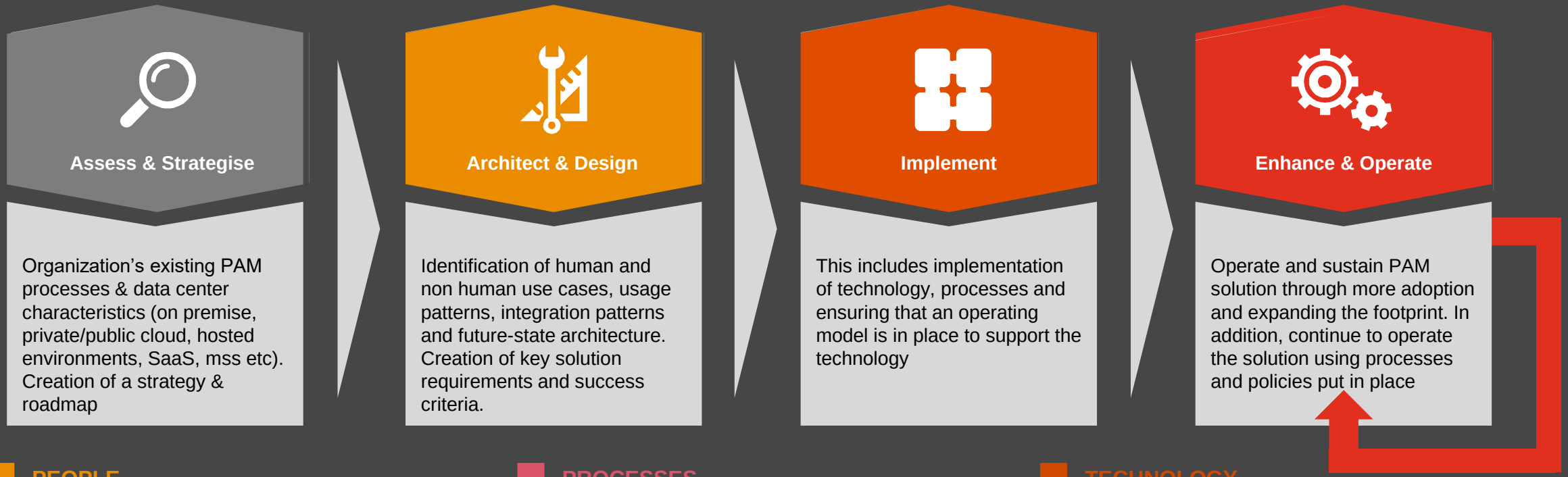
- Just in Time Access
- Just Enough Privileges
- Brokered Admin Access
- Credential Management

### CONTINUOUSLY MONITOR AND ATTEST

- Session Recording
- Activity Audit
- Threat Analytics

# People, Process & Technology (PPT)

While technology is a critical factor in any PAM program, the **people and processes** supporting the technology should be considered equally as important and must be **taken into consideration in every phase of the process** in order to create a sustainable and cost effective PAM service.




**PEOPLE**

- Organisation and team structure
- Target Operating Model
- Roles & Responsibilities
- Operational Runbook Review
- Communications

**PROCESSES**

- Policies
- PAM Controls
- Process guides
- Operational effectiveness
- Training material

**TECHNOLOGY**

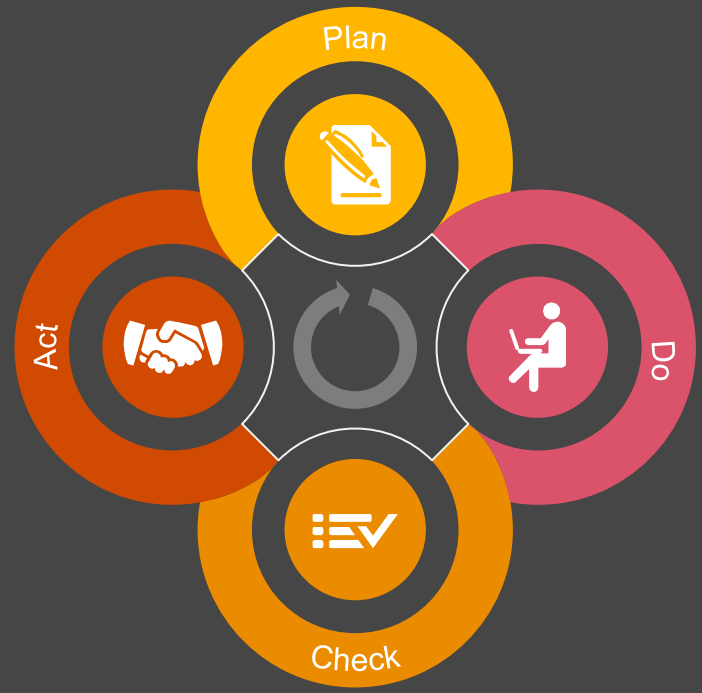
- Tool sets used for managing privileged access
- Key technology use cases & usage patterns
- Privileged access account types
- Monitoring, Audit and Recording tool set

# Execute towards the plan

## Compliance & Security is a journey, not a destination

Today’s threat landscape is ever changing, and organizations also evolve over time and thus the compliance and security cannot be a one-time goal

- Understand the impact and requirements on your organization
- Be concrete with your milestones and timelines, to execute roadmap efficiently
- Set up regular checkpoints for verifying the path you are on is still leading towards NIS2 compliance
- Define metrics to help you continuously measure and identify further potential gaps or issues along the way
- Perform regular user educations in the areas of security, especially in regards to NIS2 requirements
- Test your strategies and implemented processes regularly
    - Especially the ITDR, backup, emergency and DR processes



# Open discussion

# Thank you!

www.pwc.dk

Success skaber vi sammen…