How do I become compliant with Identity security

Presentation by **Martin Topgaard**
April 2024

New to NIS2
Where to begin?

It's about people and processes

1

The security efforts must be rooted in the management team – the management team must show that it takes responsibility for security and must be involved in the management of cybersecurity risks.

2

The company must ensure an appropriate level of security based on a risk-based approach – and it must be able to measure the risks it accepts.

3

Documenting the security effort – the company must document that the company is in control of security.

4

The company must be ready to handle cybercrises – and have a disaster recovery plan ready.

5

Focus on the security of suppliers – the company must be critical, ask questions and ask for documentation of suppliers' security.

6

The company must be able to handle a notification obligation on an equal footing with the GDPR – but already within 24 hours.

Important first steps

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

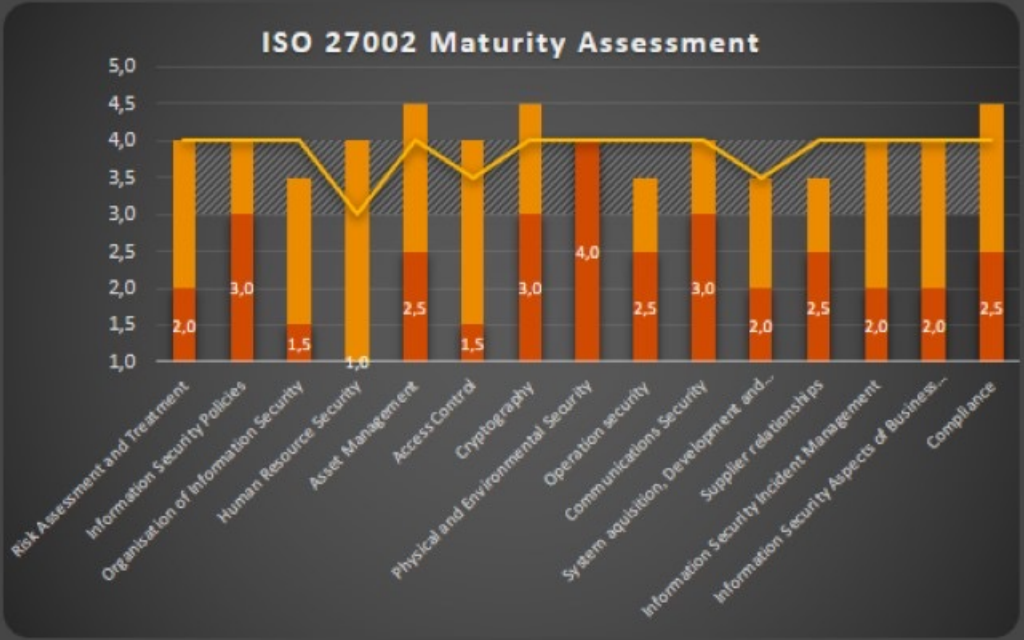
Strategy and roadmap for closing the gaps

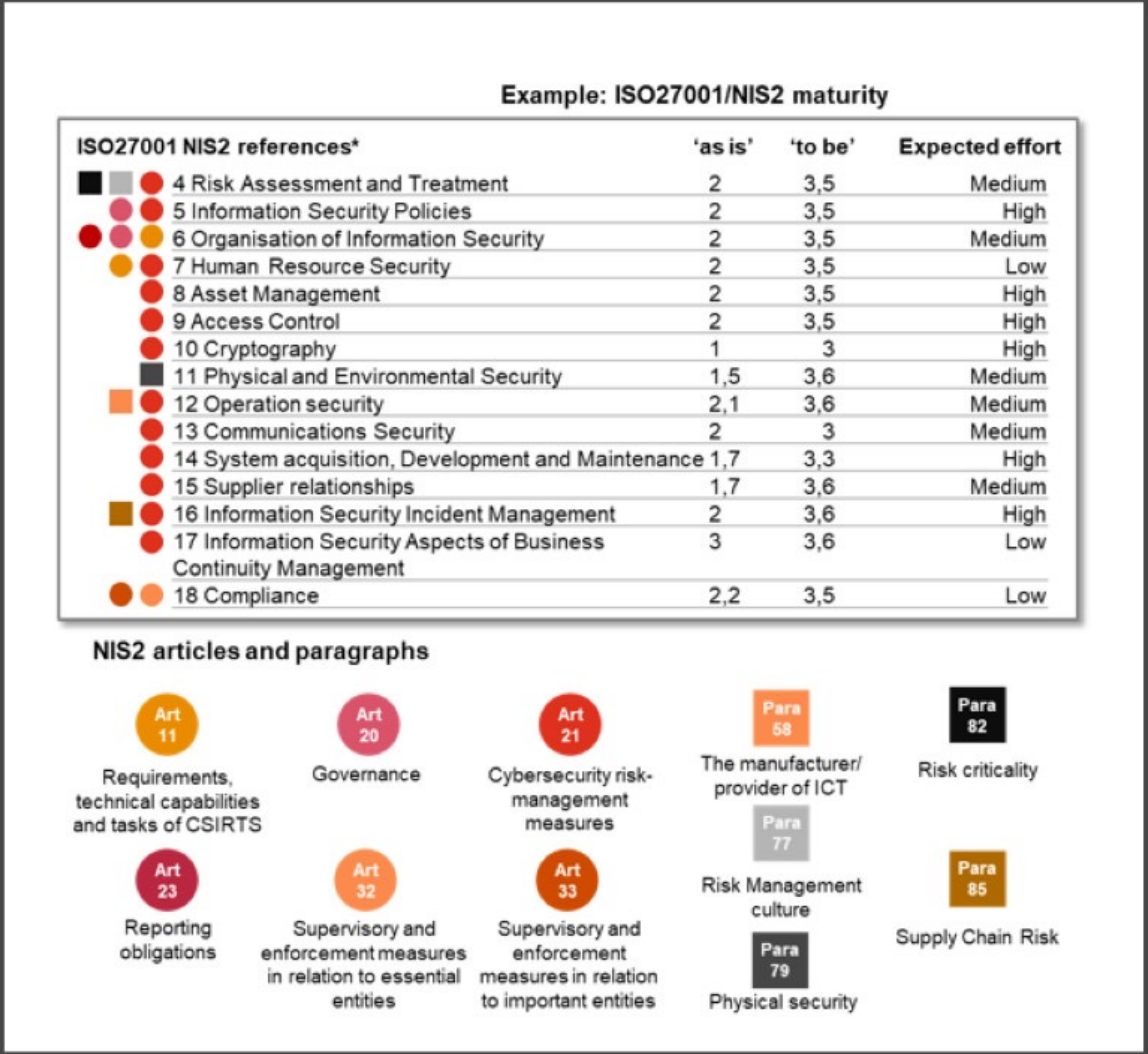
1. Analyze the identified gaps
2. Prioritize the findings based on risks, complexity to implement and importance against NIS2 requirements
3. Define the future state
4. Update Enterprise strategy
5. Gaps mitigation roadmap with timelines for each gap

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





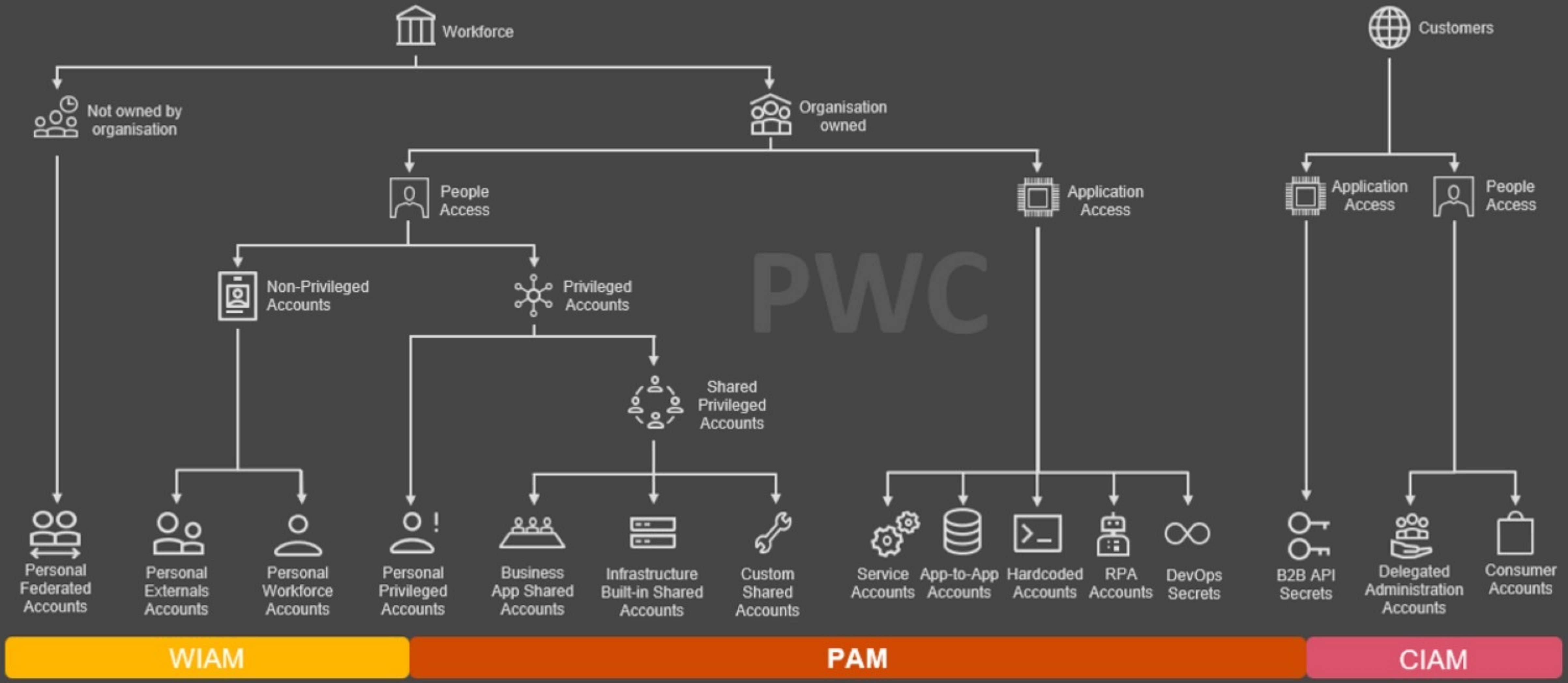
Example: ISO27001/NIS2 maturity

ISO27001 NIS2 references*	'as is'	'to be'	Expected effort
■ ■ ● 4 Risk Assessment and Treatment	2	3,5	Medium
● ● 5 Information Security Policies	2	3,5	High
● ● ● 6 Organisation of Information Security	2	3,5	Medium
● ● 7 Human Resource Security	2	3,5	Low
● 8 Asset Management	2	3,5	High
● 9 Access Control	2	3,5	High
● 10 Cryptography	1	3	High
■ 11 Physical and Environmental Security	1,5	3,6	Medium
■ ● 12 Operation security	2,1	3,6	Medium
● 13 Communications Security	2	3	Medium
● 14 System acquisition, Development and Maintenance	1,7	3,3	High
● 15 Supplier relationships	1,7	3,6	Medium
■ ● 16 Information Security Incident Management	2	3,6	High
● 17 Information Security Aspects of Business Continuity Management	3	3,6	Low
● ● 18 Compliance	2,2	3,5	Low

NIS2 articles and paragraphs

● Art 11	Requirements, technical capabilities and tasks of CSIRTS
● Art 20	Governance
● Art 21	Cybersecurity risk-management measures
■ Para 58	The manufacturer/ provider of ICT
■ Para 82	Risk criticality
● Art 23	Reporting obligations
● Art 32	Supervisory and enforcement measures in relation to essential entities
● Art 33	Supervisory and enforcement measures in relation to important entities
■ Para 77	Risk Management culture
■ Para 79	Physical security
■ Para 85	Supply Chain Risk

Identities across organization



Workforce

Not owned by organisation

Organisation owned

People Access

Application Access

Non-Privileged Accounts

Privileged Accounts

Shared Privileged Accounts

Customers

Application Access

People Access

Personal Federated Accounts

Personal Externals Accounts

Personal Workforce Accounts

Personal Privileged Accounts

Business App Shared Accounts

Infrastructure Built-in Shared Accounts

Custom Shared Accounts

Service Accounts

App-to-App Accounts

Hardcoded Accounts

RPA Accounts

DevOps Secrets

B2B API Secrets

Delegated Administration Accounts

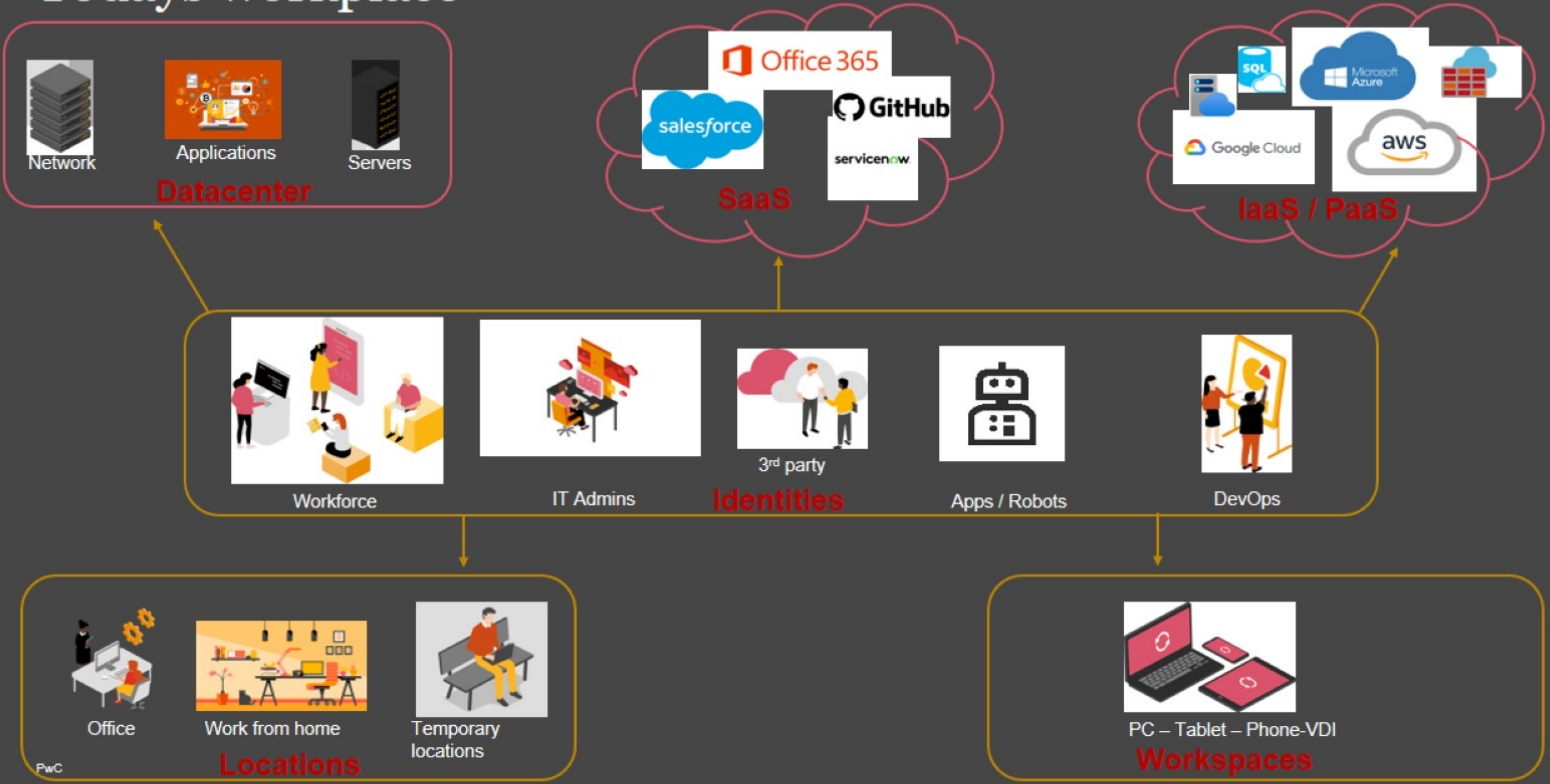
Consumer Accounts

WIAM

PAM

CIAM

Todays workplace



Datacenter

Network

Applications

Servers

SaaS

IaaS / PaaS

Identities

Workforce

IT Admins

3rd party

Apps / Robots

DevOps

Locations

Office

Work from home

Temporary locations

Workspaces

PC – Tablet – Phone-VDI

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

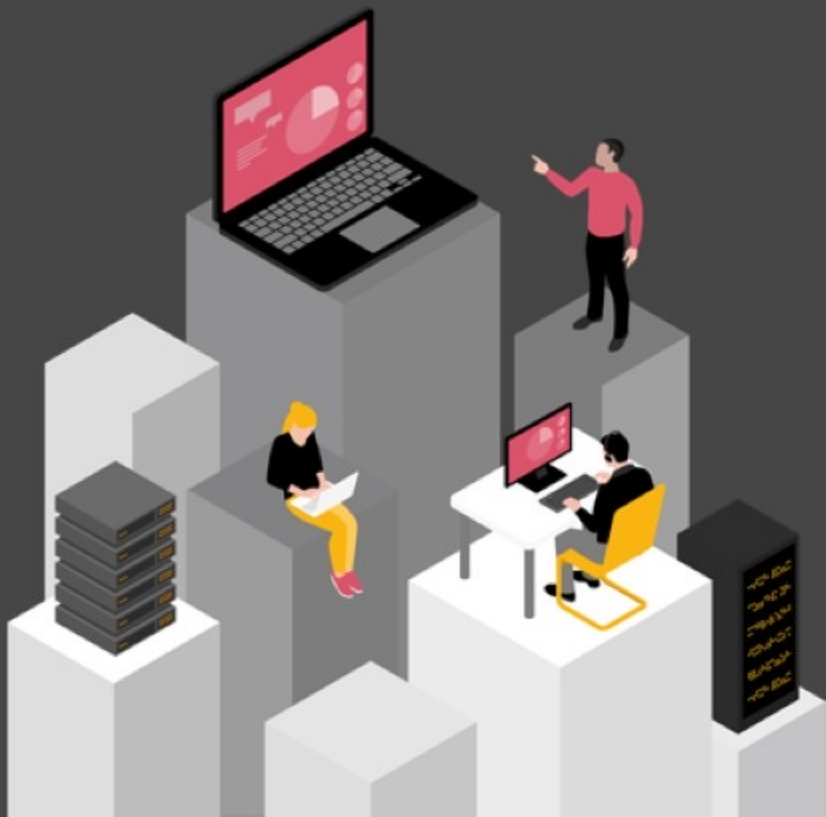
NIS2 articles

- Art.21.2(g) Basic cyber hygiene practices and cybersecurity training
- Art.21.2(i).3 Asset management
- Art.21.2(i).2 Access control policies
- Art.21.2(i).1 Multi-factor authentication or continuous authentication solutions
- Art.21.2(d).Supply chain security

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.

- ISO/IEC 27001: A.9.2.1 - Access control policy
- ISO/IEC 27001: A.9.2.2 – User access management
- ISO/IEC 27001: A.9.2.3 – User responsibilities
- ISO/IEC 27001: A.9.2.4 – System and application access control
- ISO/IEC 27001: A.9.2.5 – User password management
- ISO/IEC 27001: A.9.2.6 – User identification and authentication
- ISO/IEC 27002: 9.2.6 – User roles and responsibilities
- ISO/IEC 27002: 9.2.7 – Management of privileged access rights



Protect Identities across organization

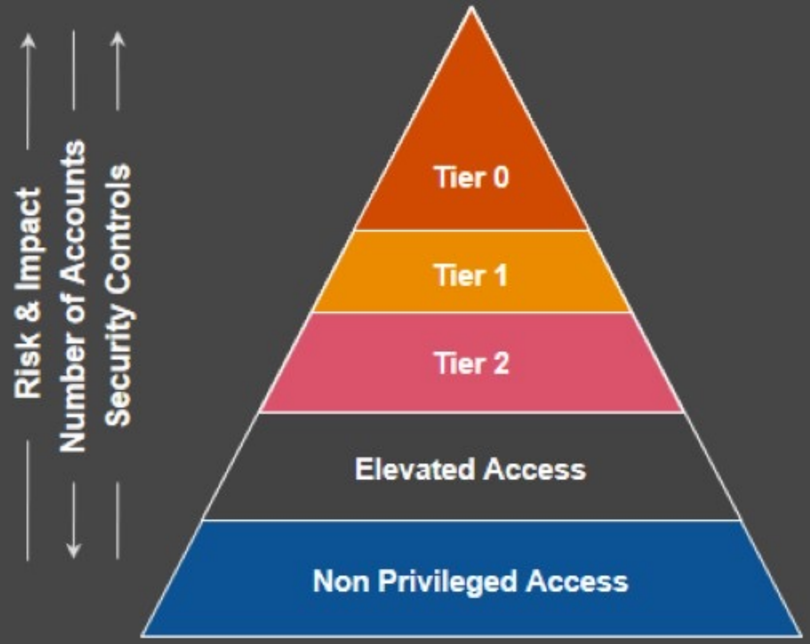
Almost every attack starts by taking over identity of an account within the breached organization.

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

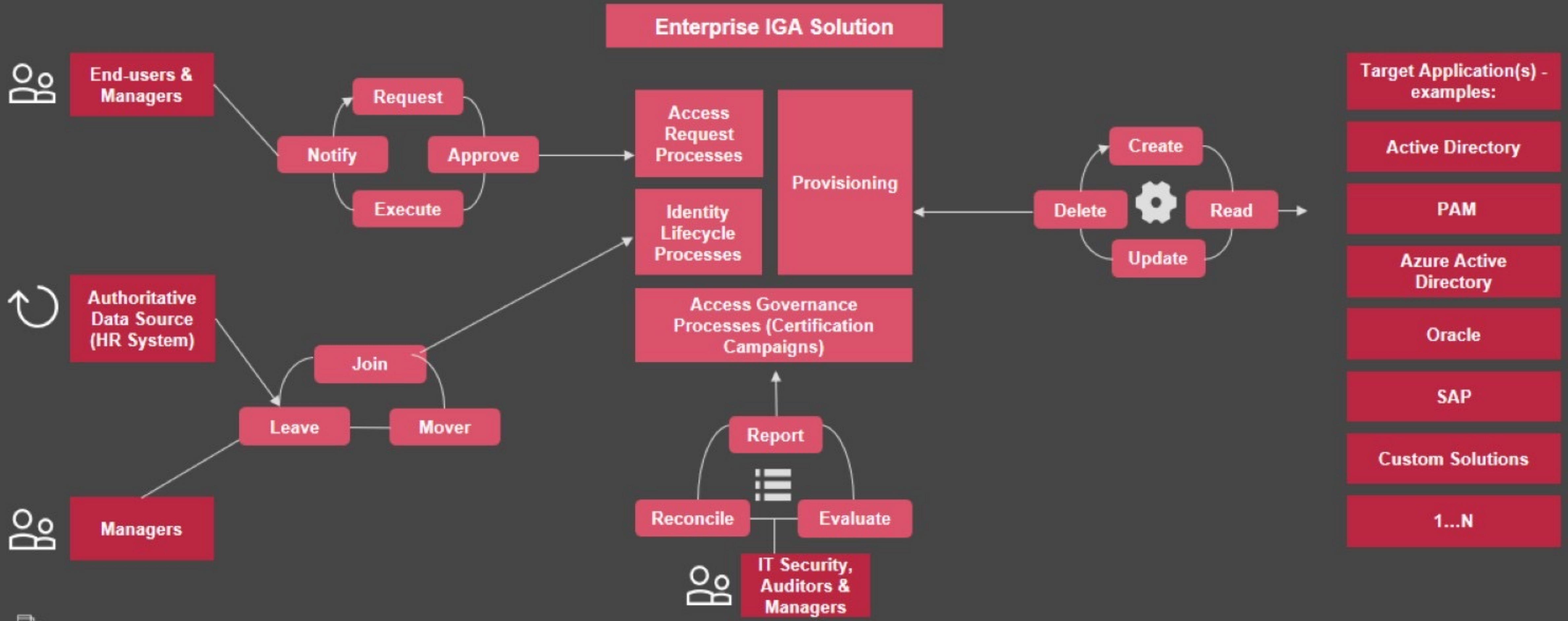
Below are some key considerations to be made before enforcing controls:

- 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

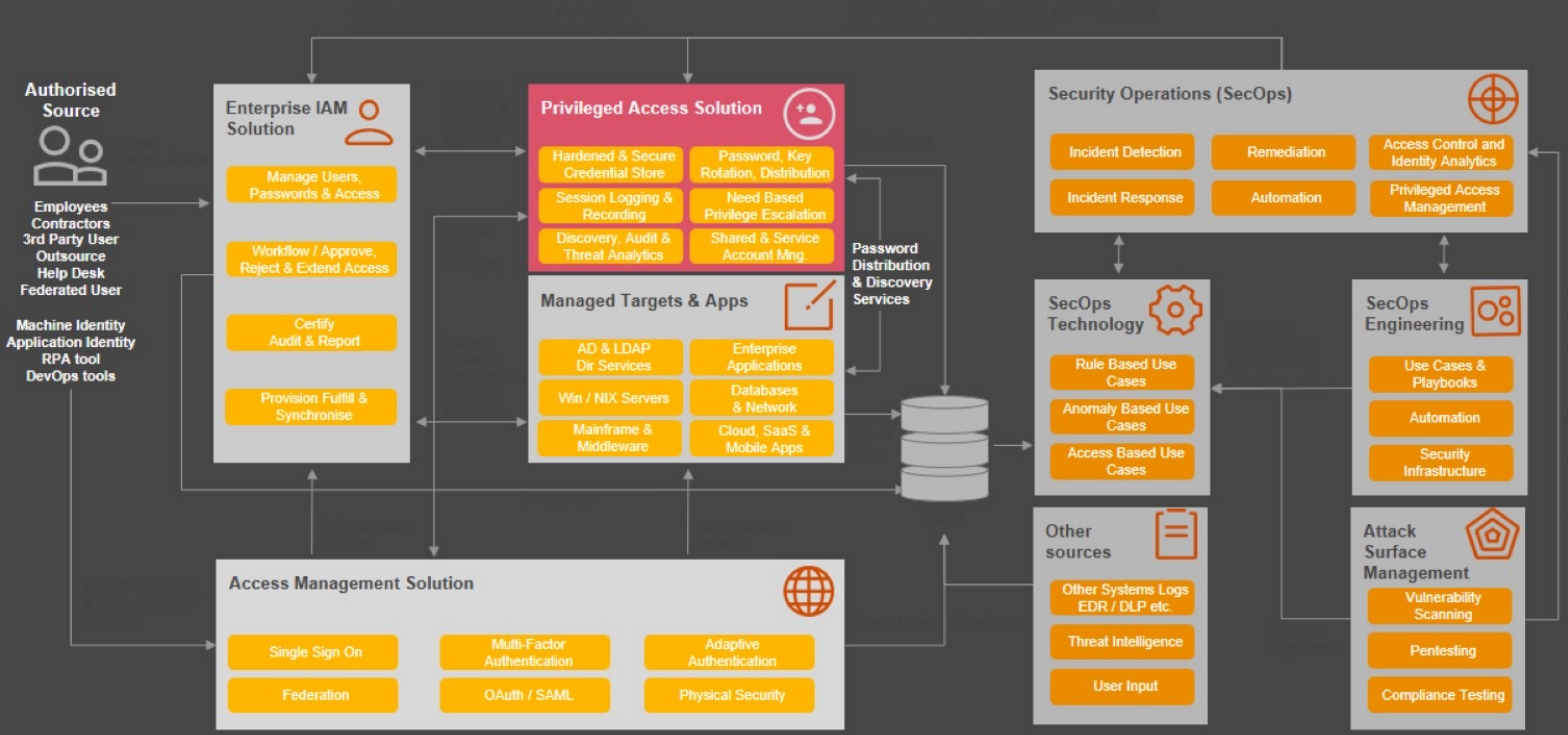


Leveraging IGA processes integrated with PAM

Enterprise IGA solutions support a set of standard processes using PAM module



Integrated Identity Security



Authorised Source

Employees
Contractors
3rd Party User
Outsource
Help Desk
Federated User

Machine Identity
Application Identity
RPA tool
DevOps tools

Enterprise IAM Solution
- Manage Users, Passwords & Access
- Workflow / Approve, Reject & Extend Access
- Certify Audit & Report
- Provision Fulfill & Synchronise

Privileged Access Solution
- Hardened & Secure Credential Store
- Password, Key Rotation, Distribution
- Session Logging & Recording
- Need Based Privilege Escalation
- Discovery, Audit & Threat Analytics
- Shared & Service Account Mng.

Managed Targets & Apps
- AD & LDAP Dir Services
- Enterprise Applications
- Win / NIX Servers
- Databases & Network
- Mainframe & Middleware
- Cloud, SaaS & Mobile Apps

Password Distribution & Discovery Services

Access Management Solution
- Single Sign On
- Multi-Factor Authentication
- Adaptive Authentication
- Federation
- OAuth / SAML
- Physical Security

Security Operations (SecOps)
- Incident Detection
- Remediation
- Access Control and Identity Analytics
- Incident Response
- Automation
- Privileged Access Management

SecOps Technology
- Rule Based Use Cases
- Anomaly Based Use Cases
- Access Based Use Cases

SecOps Engineering
- Use Cases & Playbooks
- Automation
- Security Infrastructure

Other sources
- Other Systems Logs EDR / DLP etc.
- Threat Intelligence
- User Input

Attack Surface Management
- Vulnerability Scanning
- Pentesting
- Compliance Testing

It all starts with people

It all starts with people

- Even with best possible security solutions, controls and policies, people will be involved and will be the weak link, unless you train them

Explain why

- Tell your people not only what is important to do, but also why
- Understanding why certain processes needs to be followed helps people to comply with them

Implement proper Cybersecurity Hygiene program

- Prepare the plan
- Share it accordingly to increase awareness

Thank you

www.pwc.dk

Together we succeed…

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.