



XNESEC


ALWAYS SECURE, NEVER AT RISK

Onesec Digital Identity





Diary

- Introduction
 - The Need for a Digital Identity Strategy
 - Service Strategy
 - Identity and Access Governance and Management
 - Solution process
- 

Introduction

ALWAYS SECURE, NEVER AT RISK.

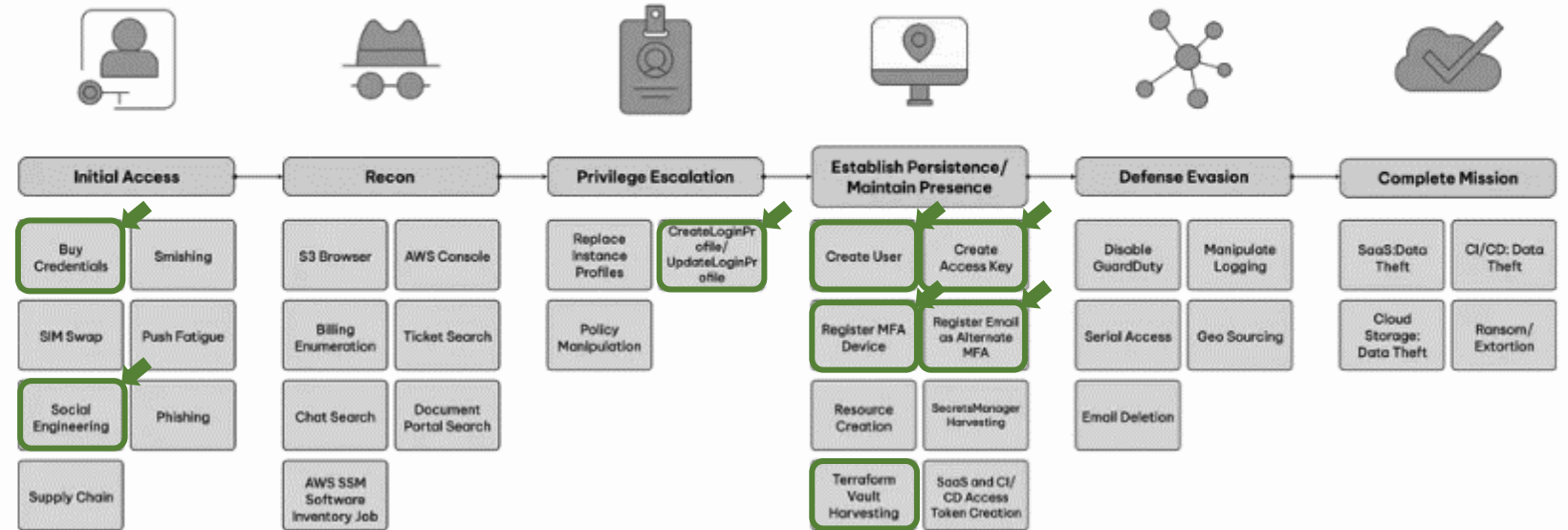




MGM: an Attack of the Modern Era

ATTACKER LIFECYCLE

LUCR-3: CHOOSE YOUR OWN ADVENTURE!



AWS Attacker Lifecycle

MGM faces \$100M loss from ransomware attack

MGM's Q4 filing revealed some personal customer data was stolen during the September attack and said the company expects cyber insurance to sufficiently cover the losses.

By Andrew Pollack, Wall Street Journal | October 11, 2023



MGM Resorts International said its third-quarter earnings were hurt by a \$100 million ransomware attack that cost the company \$100 million but said the amount will likely be covered by its cyber insurance policy.

The September 2023 ransomware attack, which guests reported issues related to room access, amenities and casino games that persisted for days, finally was resolved, according to MGM. The casino confirmed that MGM was one of many customers affected in a previously disclosed ransomware attack that caught other operators off guard and granted access to other organizations.

More information about the attack and remediation was revealed in an S-K-1 filing and update from MGM CEO William Herrstetter on Thursday, MGM confirmed it.



The Need for a Digital Identity Strategy

ALWAYS SECURE, NEVER AT RISK.

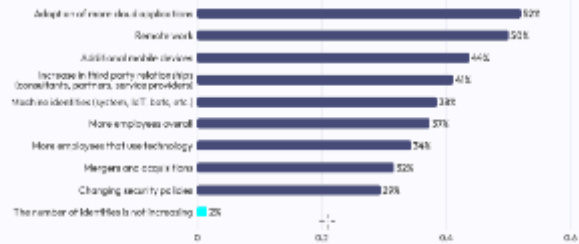




Trends in Cybersecurity related to Digital Identity

What factors are driving an increase in the number of identities at your company?

Choose all that apply.



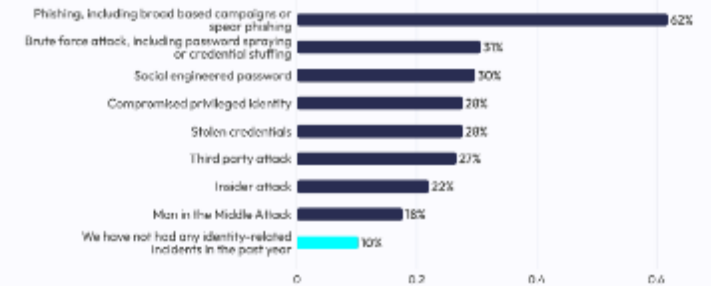
Did your company suffer any direct impact to business results as a result of identity-related incidents in the past year?

Choose all that apply.



What kind of identity-related incidents has your company had in the past year?

Choose all that apply.



The adoption of zero trust architectures is motivating organizations to strengthen their governance and identity and access management

EXHIBIT 10. ANTICIPATED CRITICALITY OF ZERO TRUST IN NEXT TWO YEARS

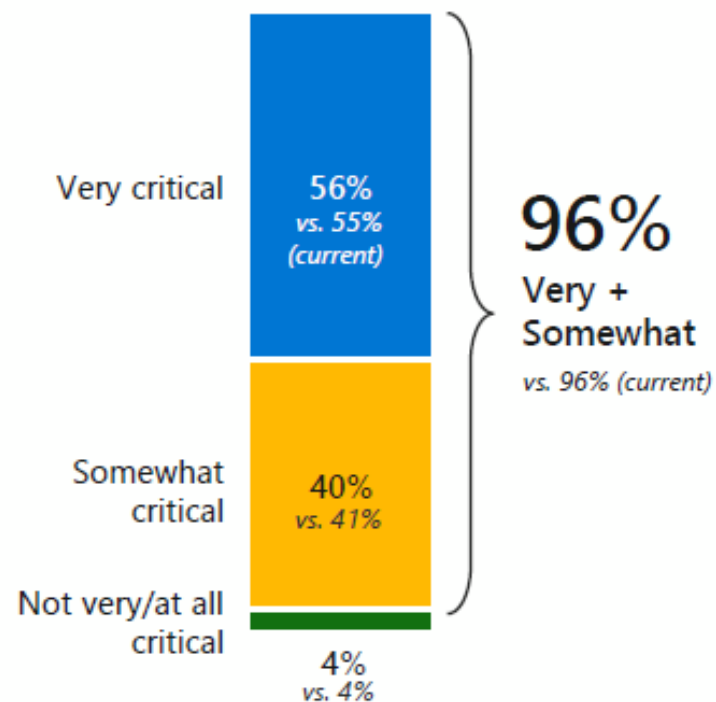
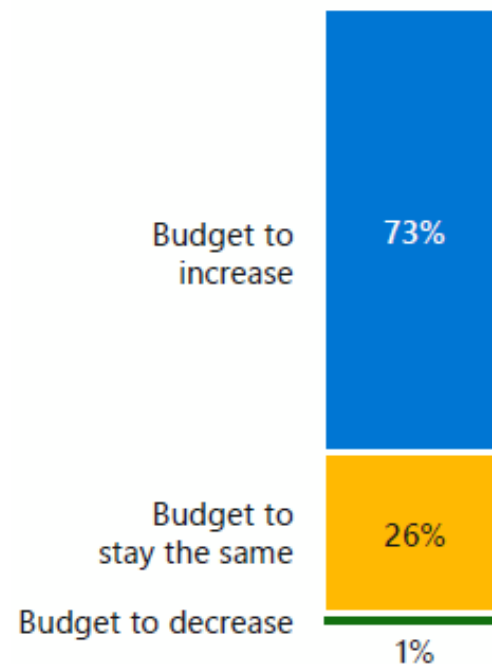
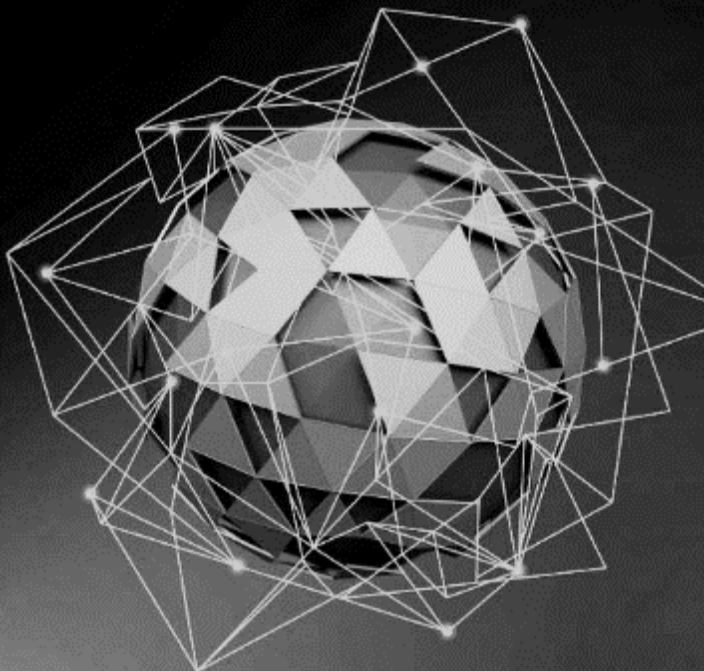


EXHIBIT 11. ANTICIPATED ZERO TRUST BUDGET IN NEXT TWO YEARS



Microsoft Security

hypothesis



I-TRENDS 2023

MANDIANT SPECIAL REPORT

NESEC

Why do companies require a Digital Identity strategy?

SPECIAL REPORT | MANDIANT M-TRENDS 2023

77

Lessons Learned

The common thread between Lapsus and UNC3944 is simple; both groups realized the value in targeting credentials and accounts rather than endpoints. Despite the lack of maturity and sophistication on display, both groups were able to gain access to large entities with mature security organizations. Both groups ignored the idea of establishing a foothold on network, instead focusing on targeting the accesses and accounts of legitimate individual users.

Beyond the targeting of credentials rather than endpoints, there is another, more sinister thread that binds these actors together. UNC3944 and UNC3661 have both purposefully targeted executives and privileged administrators during intrusions with personal intent to threaten, coerce, or otherwise motivate these high priority employees to pay a ransom or submit to the actors' demands. This intentional willingness to target individual people with threats and other malicious activity constitutes an evolution of the attack surface; individual people and their families are now considered fair game for malicious actors in their efforts to monetize their intrusions. In response to this evolutionary leap, defenders should expand their definition of "attack surface," and consider that providing protection for their employees may become a necessary part of protecting your organization from malicious actors.

In the near term, organizations will have to contend with threat actors that find new ways to steal identities from users through a combination of social engineering and commodity information stealers alongside information gathering operations targeting their internal data stores. As MFA grew more commonplace, attackers sought novel means to bypass MFA without relying on malware. The same is to be expected of Identity and Access Management (IAM) systems in the near term as attackers and researchers alike explore the capabilities supplied by such platforms.



Why do companies require a Digital Identity Strategy?



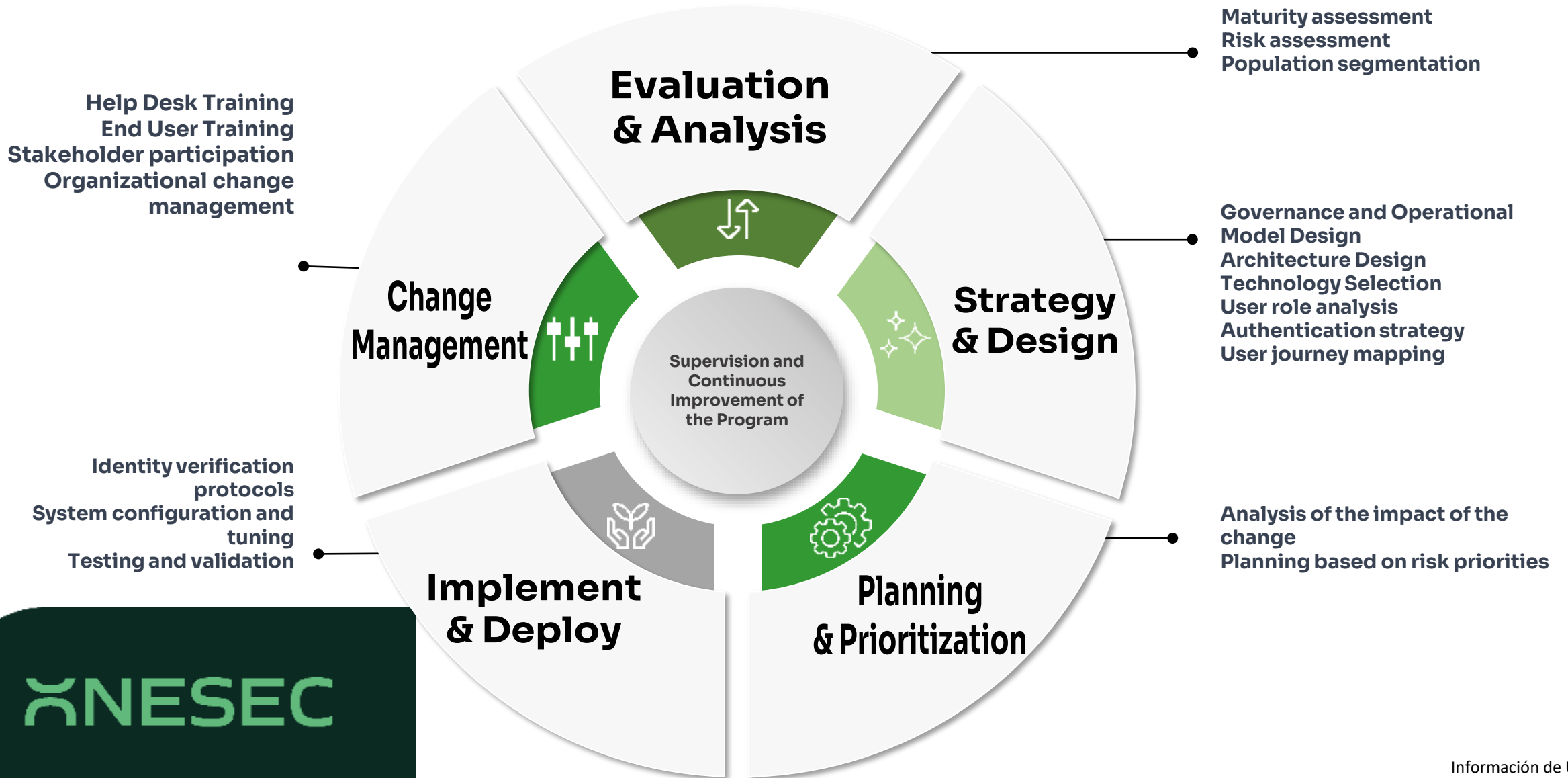


XNESEC

Our customers will get

- **Ability to defend against modern threats:** Organizations gain a robust defense against modern cyber threats, such as insider attacks and compromised credentials.
- **Increased ability to meet regulatory and compliance needs:** Customers achieve and maintain compliance with stringent industry regulations, minimizing penalty risks.
- **An end-to-end cybersecurity solution:** Zero Trust and IGA/IAM offer end-to-end security solutions, ensuring that all potential vulnerabilities are addressed.
- **Have an Adaptive Security Model:** With the adaptive nature of the Zero Trust model, customers can ensure security across a variety of environments (on-premises, cloud, hybrid).
- **Enhanced access management:** IGA/IAM provides granular control over who accesses what, reducing the risk of unauthorized data access or breaches.
- **Significant protection savings:** By preventing potential breaches and ensuring compliance, organizations can avoid hefty penalties and potential reputational damage, resulting in long-term savings.
- **Agility in human resources management processes:** IGA/IAM solutions streamline the process of granting and revoking access, simplifying HR and IT processes.
- **Transparent and auditable processes:** Organizations can easily track, audit, and report access and activities, improving transparency and accountability.

ONESEC Digital Identity Consulting Services

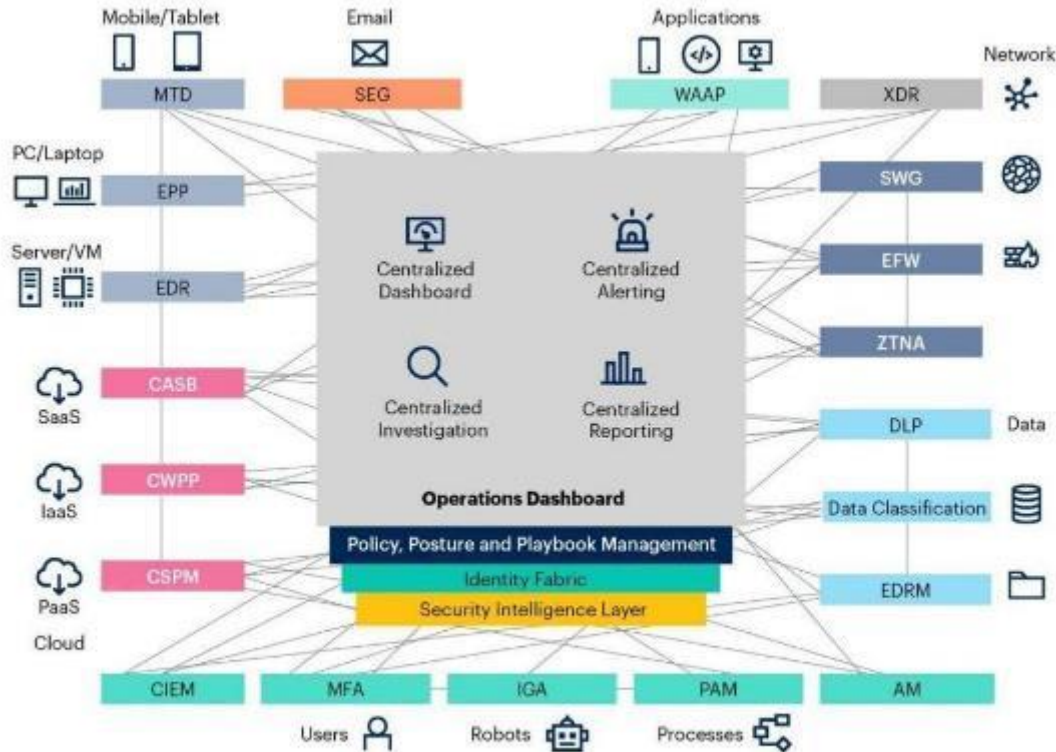


Government Services Strategy and Identity and Access Management



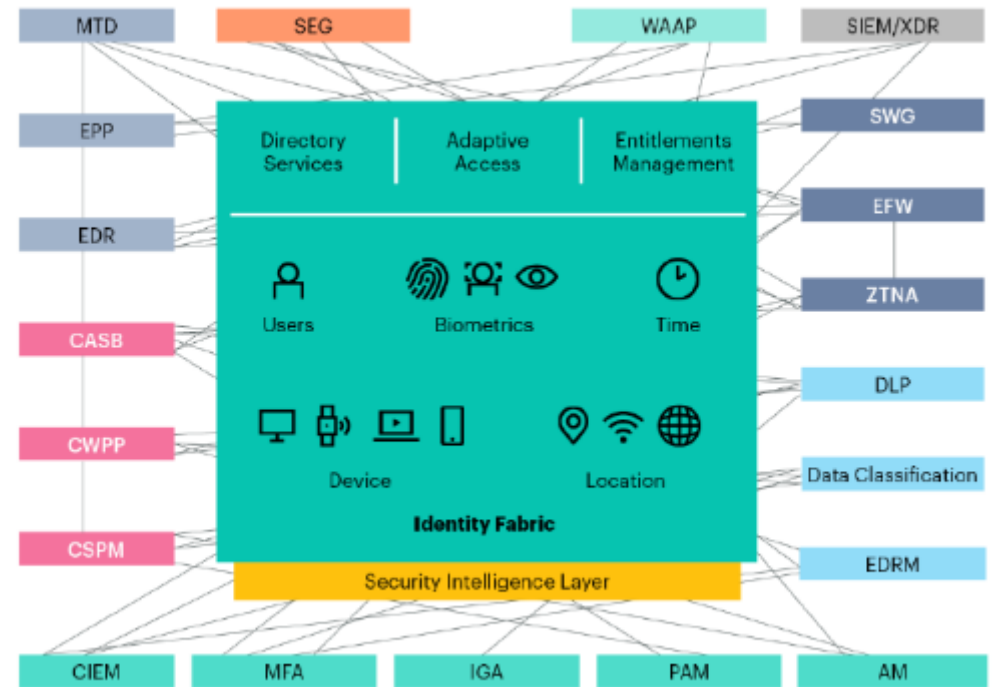
In what strategic context is the ONESEC Identity Services Blueprint located?

Cybersecurity Mesh Architecture Complete



Source: Gartner
754315_C

Identity Fabric Layer



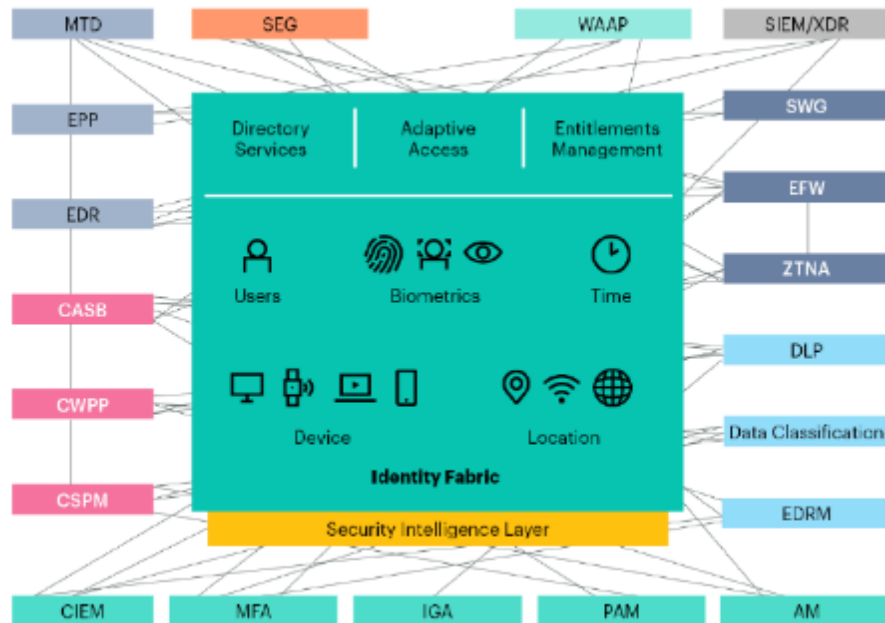
Source: Gartner

Gartner

ONESEC

In what strategic context is the ONESEC Identity Services Blueprint located?

Identity Fabric Layer



Source: Gartner



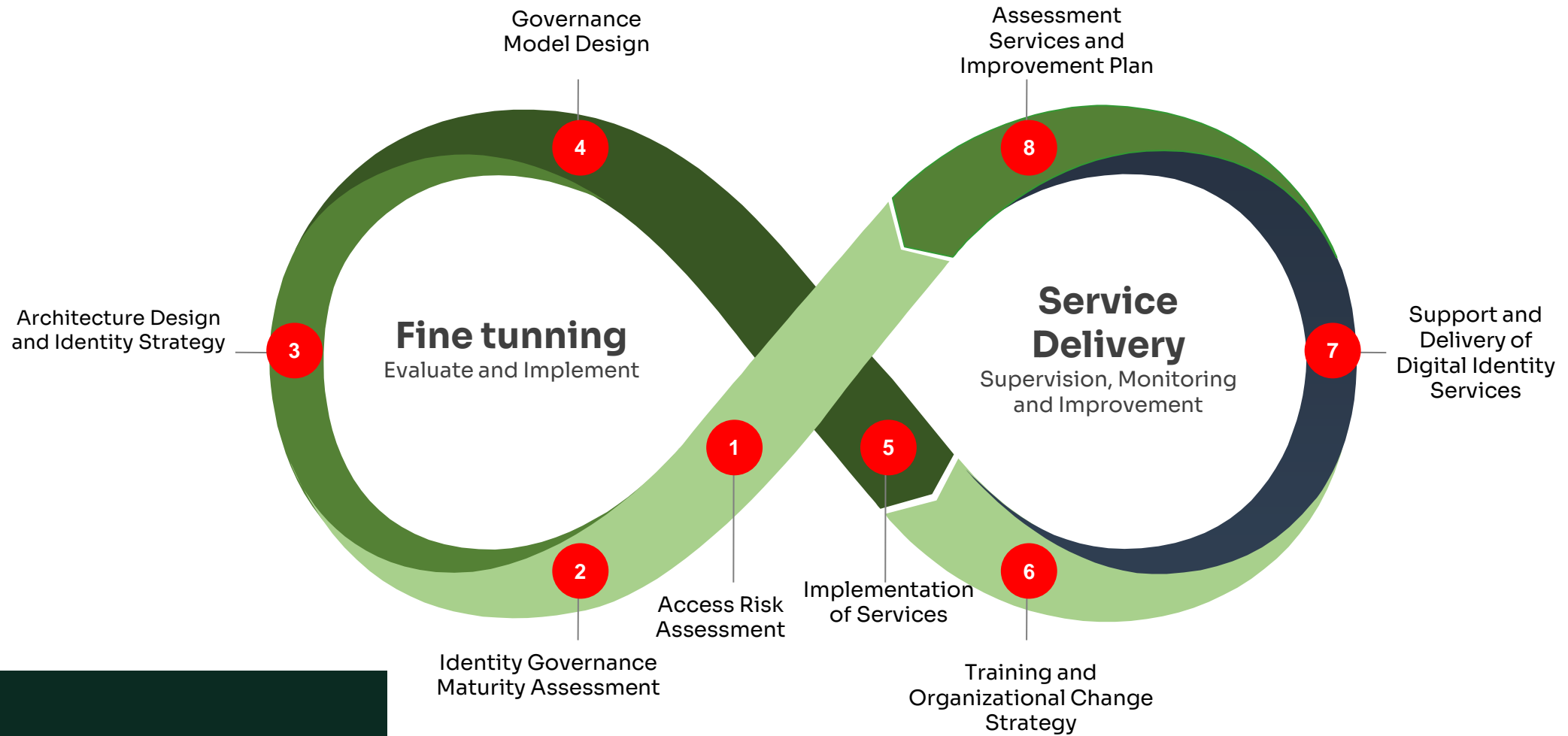
Microsoft Sign in

Solution process

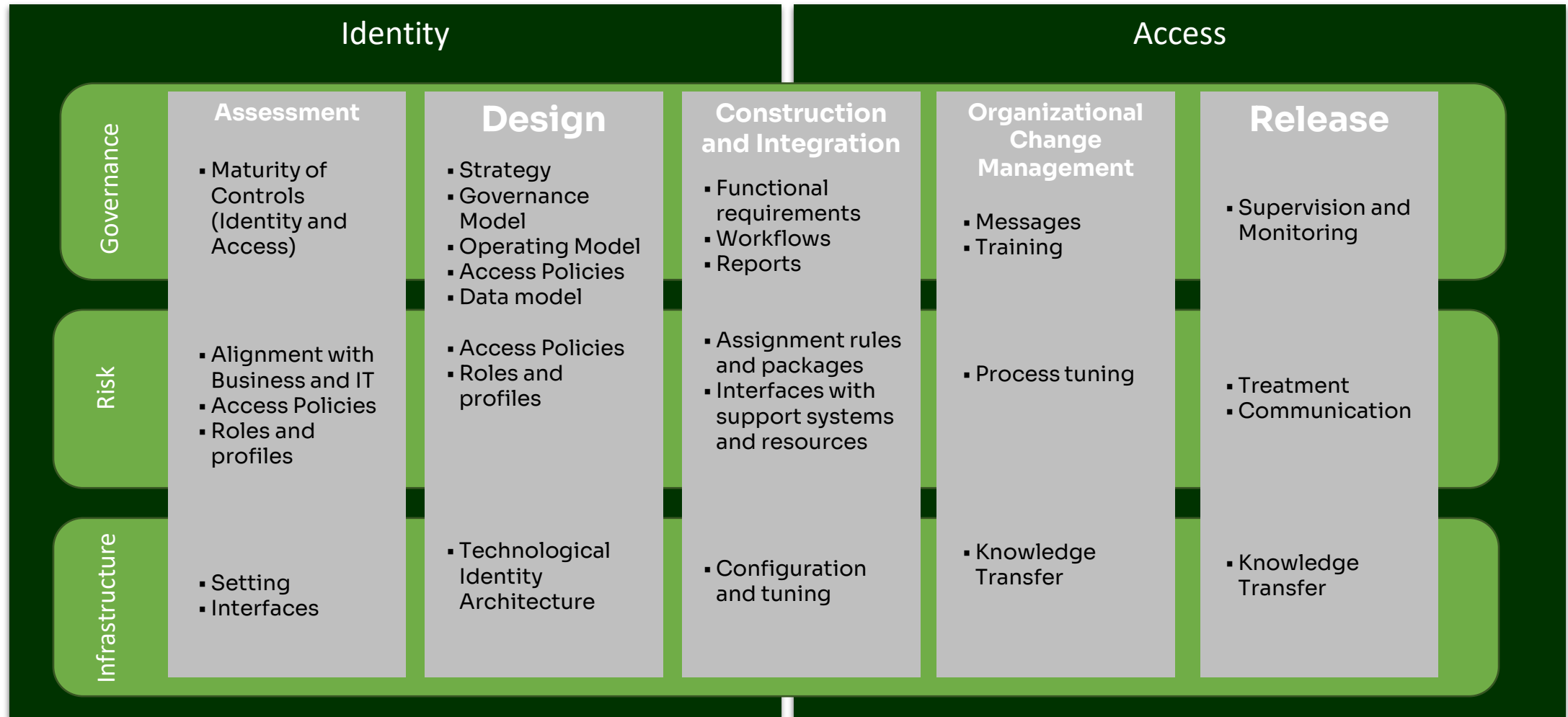
ALWAYS SECURE, NEVER AT RISK.



ONESEC Identity Consulting Services Delivery Process

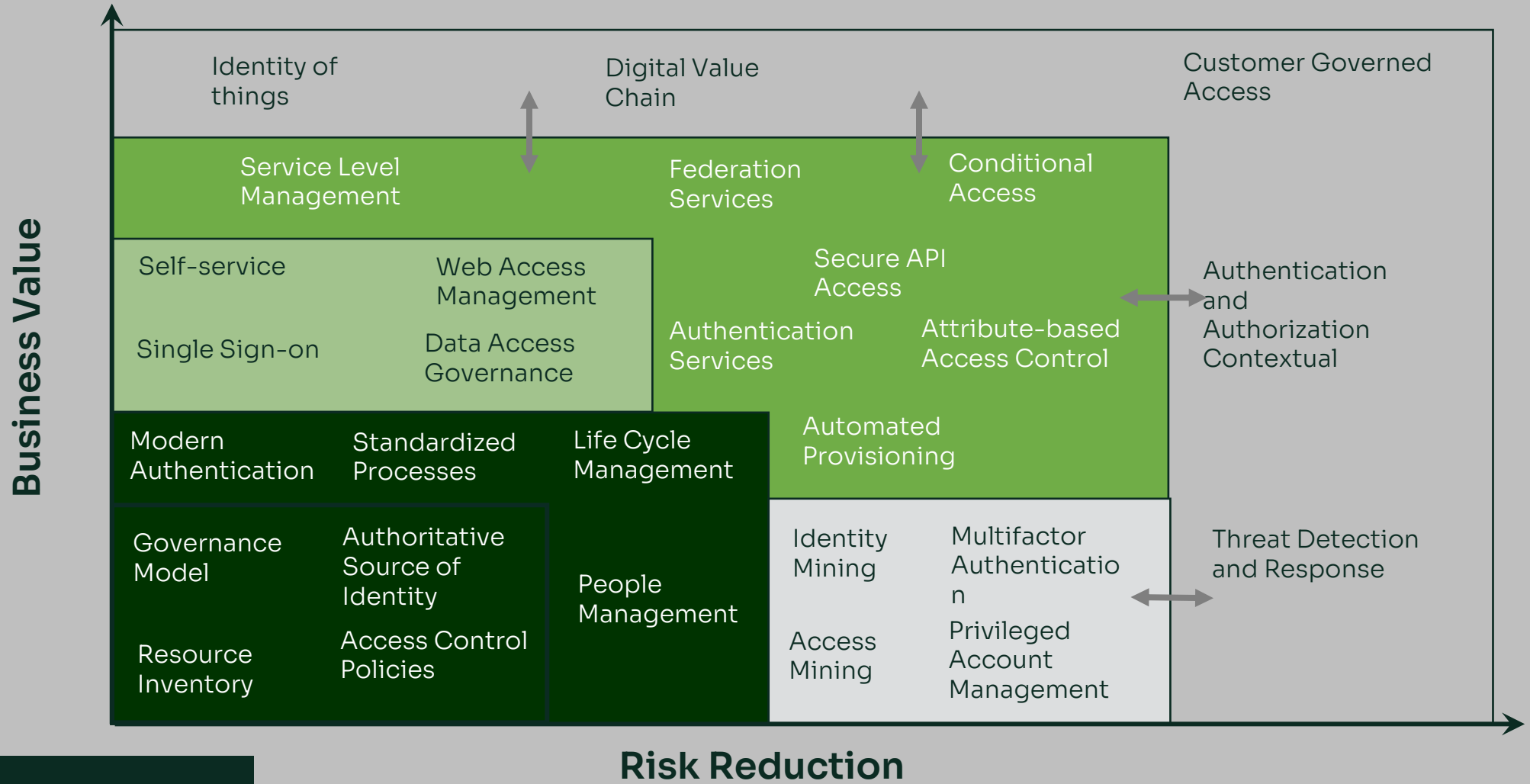


Implementation Roadmap

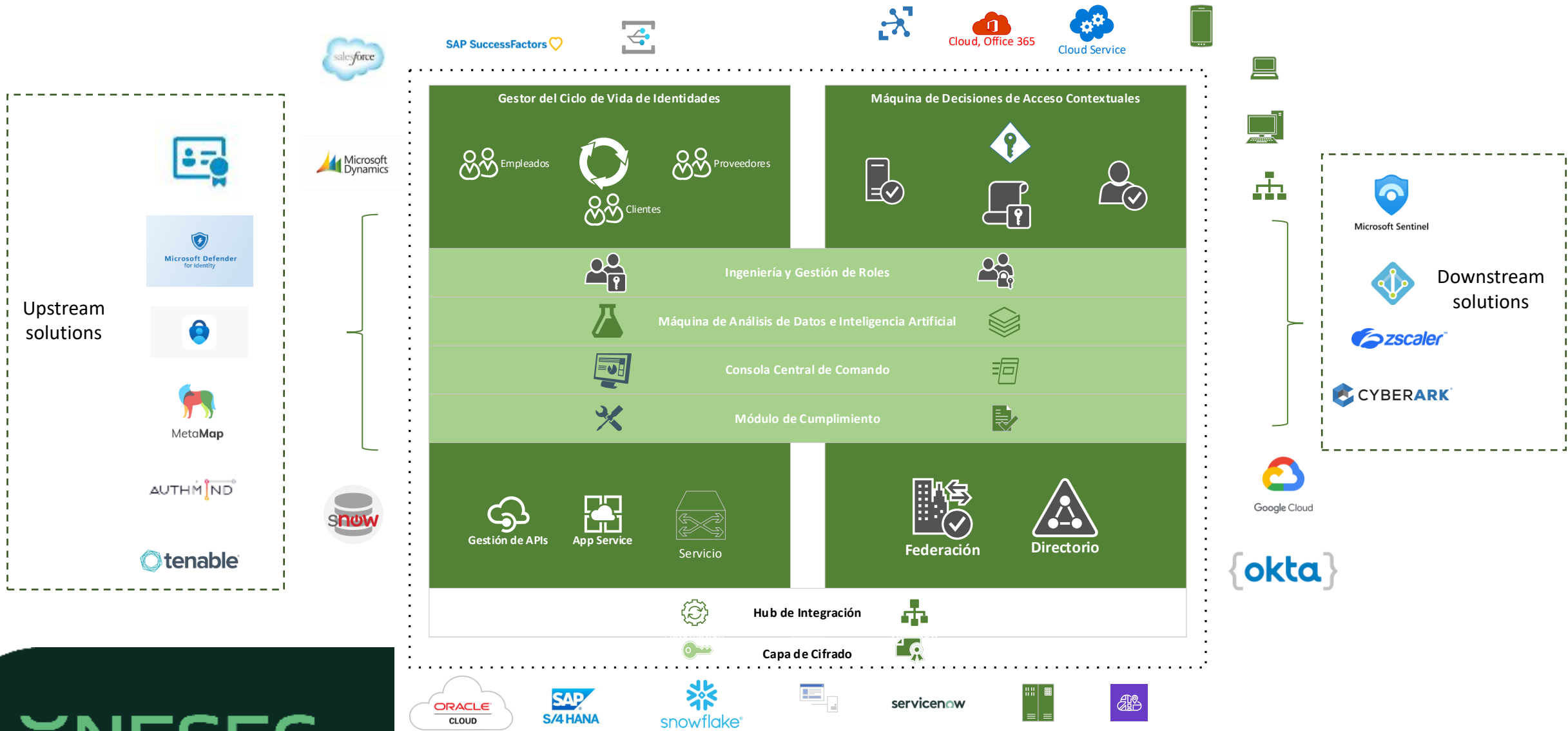


Road Map for Value Generation

IGA/IAM capabilities



Digital Identity Services Blueprint



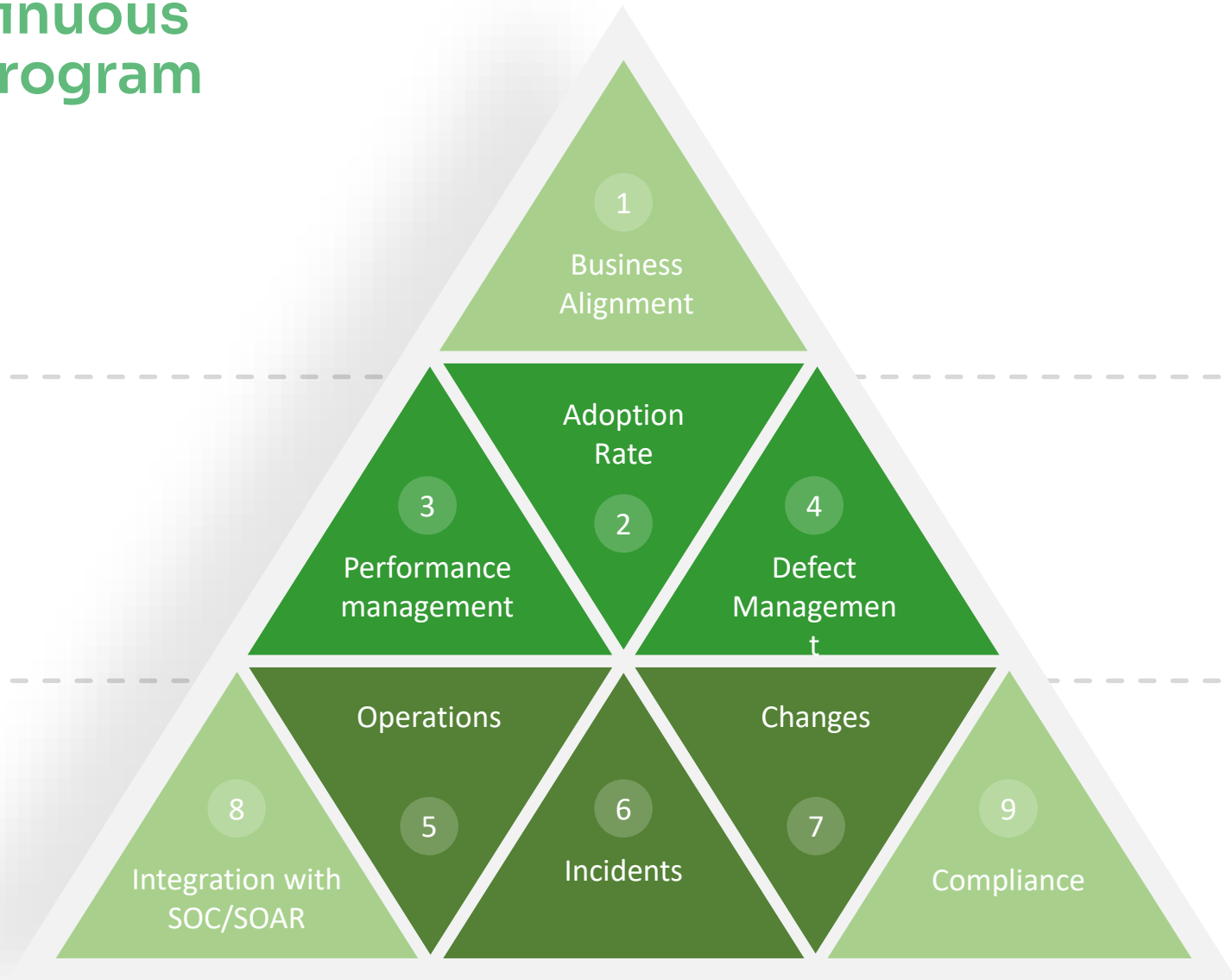
NESEC

Supervision and Continuous Improvement of the Program

Governance

Optimization Strategies

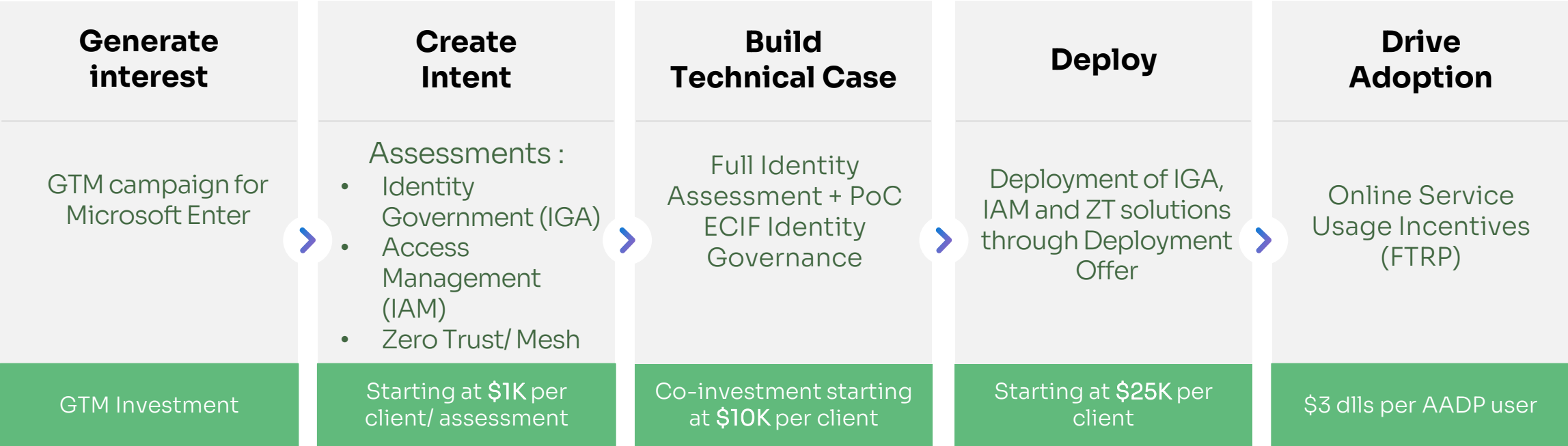
Continuous Monitoring and Program Management



Roadmap Microsoft - Onesec

Presale

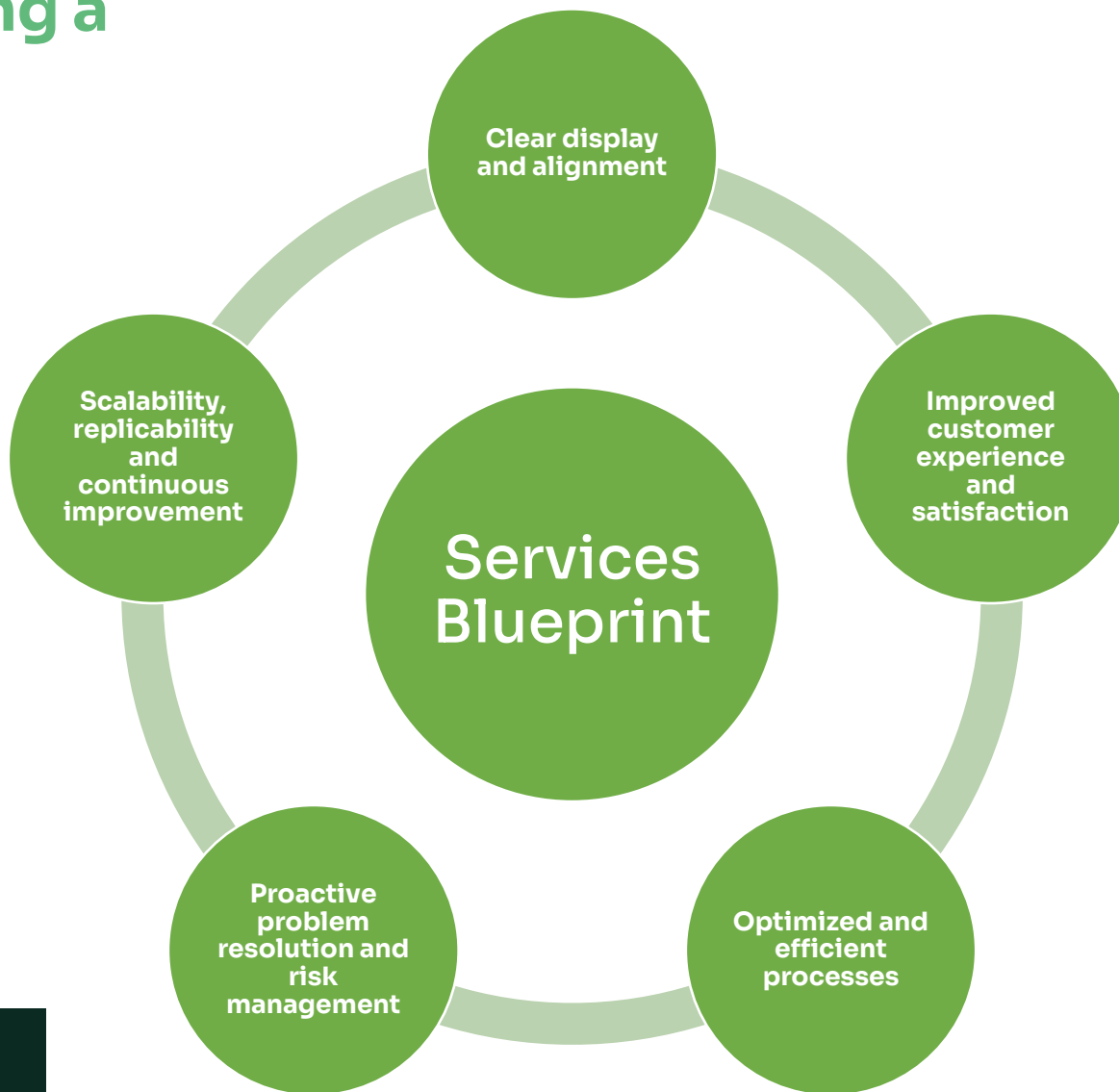
After-sales



Benefits of having a Digital Identity Blueprint

Justification: Provides a foundation to scale services, replicate them in new markets and iterate based on lessons learned while customers can expect increasing service quality
Benefit: Ensures sustainable growth and consistent, evolving services for the organization

Rationale: Bottlenecks, redundancies and potential risks become evident
Benefit: Anticipating and addressing potential issues ensures smooth service delivery and building user and stakeholder trust .



Justification: A visual representation facilitates understanding and communication due to the unified approach of the Identity Strategy.
Benefit: Ensures that stakeholders have a shared understanding leading to a unified and coherent approach to service.

Justification: It allows you to identify possible points of friction during the implementation of the solution.
Benefit: Focus on the journey and experience of the customer user, greater satisfaction and commitment.

Rationale: A Digital Identity blueprint provides an avenue for optimization
Benefit: Optimized components lead to execution resource savings for the client and better user experiences.

What is the ONESEC Digital Identity Blueprint based on?

Standards and best practices:

NIST Special Publication 800-207 (Zero Trust Architecture) : This document provides an abstract definition of Zero Trust Architecture (ZTA) and its principles. Provides detailed guidance on creating a zero trust environment.

NIST Special Publication 800-63 (Digital Identity Guidelines) – Provides detailed technical guidelines on identity verification, authentication, and lifecycle management.

ISO/IEC 27001 and 27002 : International standards for information security management. They provide a systematic approach to managing sensitive company information and ensuring data privacy.

CIS (Center for Internet Security) Controls: A set of actionable controls that focus on fundamental and organizational cybersecurity best practices.

OWASP (Open Web Application Security Project): Provides guidance on securing web applications, including authentication and session management best practices.

What is the ONESEC Digital Identity Blueprint based on? (' cont)

Regulations:

GDPR (General Data Protection Regulation): European regulation focused on the data protection and privacy of individuals within the European Union.

FISMA (Federal Information Security Management Act) – US legislation that defines a comprehensive framework to protect government information, operations, and assets.

SOX (Sarbanes-Oxley Act): American regulation that requires the protection of shareholders and the general public against accounting errors and fraudulent practices .

Industry specific guidelines:

PCI DSS (Payment Card Industry Data Security Standard): Applicable to organizations that handle branded credit cards, this standard focuses on improving the security of payment cards.

SWIFT Customer Security Programme: Specific to the banking sector, it focuses on transaction security banking and the protection of the integrity of the SWIFT messaging platform.



XNESEC

ALWAYS SECURE, NEVER AT RISK