TOREON

TOREON

Solution Portfolio – IAM architecture

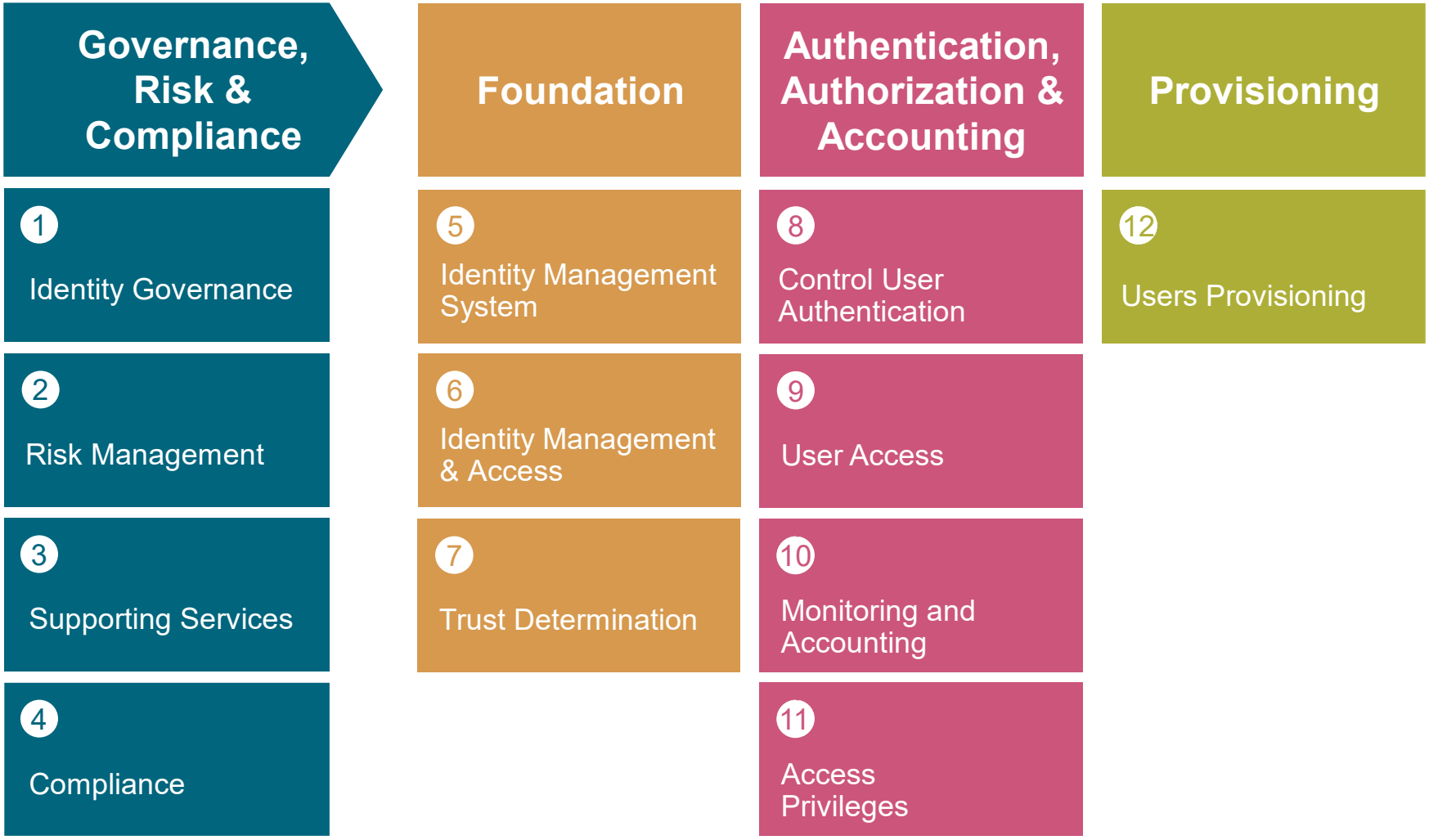
◆ CREATING TRUST FOR A SAFER DIGITAL SOCIETY ◆

Identity management basic principals

- Access to resources
- Identity management system
- User authentication
- User provisioning
- Least privilege
- Secure administration
- Strong authentication
- Adaptive access control
- Identity and access management
- Trust determination
- Credentials and authentication
- Security related training

IAM Zero trust architecture

Zero Trust (ZT) is a security architecture model which institutes a deny all until verified approach for access to resources from both inside and outside of the network. This approach addresses the challenges associated with a shifting security perimeter in a cloud-centric and mobile workforce era. This approach can be extended into the Identity and Access Management domain, and hence Toreon has developed and finetuned an approach to ZT identity architecture based upon Microsoft and industry standards best practices.


Governance, Risk & Compliance
Foundation
Authentication, Authorization & Accounting
Provisioning
1
Identity Governance
2
Risk Management
3
Supporting Services
4
Compliance
5
Identity Management System
6
Identity Management & Access
7
Trust Determination
8
Control User Authentication
9
User Access
10
Monitoring and Accounting
11
Access Privileges
12
Users Provisioning

1. Identity Governance

(External) user Lifecycle

- Onboard (external) users through an approval process
- Create access reviews of all guests in teams and groups
- Review and remove guests with unnecessary access

Manage Group memberships

- Group based licenses and lifecycles
- Delegate group management
- Reduce stale access and creep to groups
- Eligible and timebound assignments for privileged access groups

Role assignments

- Azure AD and Azure resource role assignments eligible and time-bound (PIM)
- Configure MFA and approvals for role activation
- Access reviews for Azure AD role assignments

Audits and reports

- Audit history of all privileged access to Azure AD or resource roles
- Alerts for suspicious or usage activities related to Azure AD roles
- Reports for what reviews being conducted for the organization

2. Risk Management

1. Identity risk factor management

- Orphaned accounts
- Shared and service accounts
- Unauthorized changes
- Movement of identities
- Unreviewed access
- Toxic (noncompliant) combinations (no segregations of duties)
- Access outliers (out-of-role access)
- Overprovisioned access
- Mobile access

2. Identity Threat model

3. Supporting services

1. Acquisitions and merger services
2. User/admin (security) trainings
3. Advanced Threat Protection – Continuous evaluation and SOC integrations

4. Compliance

1. Laws
2. Regulations
3. Company policies & Procedures
4. Security methodologies
5. Security Frameworks
6. Industry standards
7. Partner & supplier management

Governance, Risk and Compliance

- Governance definition is a critical precursor to any Zero Trust initiative. Governance is the glue which combines and holds all pieces of the identity framework together.
- Approaching situations from a risk perspective lets the actual solution bee a good fit for any organization who is aware of their risks and is willing to address them.
- Compliance helps organizations meet industry standards, regulations and laws.

5. Identity Management System

Create identity management system foundation

- Designating Global administrators
- Designating fallback account (Break glass)
- Designating non-global admin roles
- Privileged identity management
- Self-service password reset
- Combined registration SSPR and MFA
- Identity Policies design

Password guidance

- Custom banned password list
- On-premise integration with Azure AD Password protection
- Microsoft password guidance
- Disable periodic password resets

Authentication

- Smart lockouts
- Block legacy authentication
- Deploy Multi-factor authentication

Protection mechanisms

- Azure AD Identity Protection
- User risk detections

6. Identity management and access

1. Integrate Domains
2. Integrate on-premise AD with Azure
3. Identity management plane (Microsoft or 3rd party)
4. Identity architecture (attributes, buildup, authentication flows)
5. IDP architecture and setup

7. Trust determinations

- Hybrid identity
- Azure AD Connect
- Password Hash Synchronization
- Pass-through Authentication
- Federation
- Single-Sign On
- Azure AD B2B
- Azure AD B2C
- 3rd party identity provider integrations/IDP’s

Foundation level

- On the foundational level all the groundwork is put in place to further build the IAM solution upon.
- At the foundational level core access to the management plane is handled and the architectural frameworks are setup and decisions are made by which the organization will abide by.

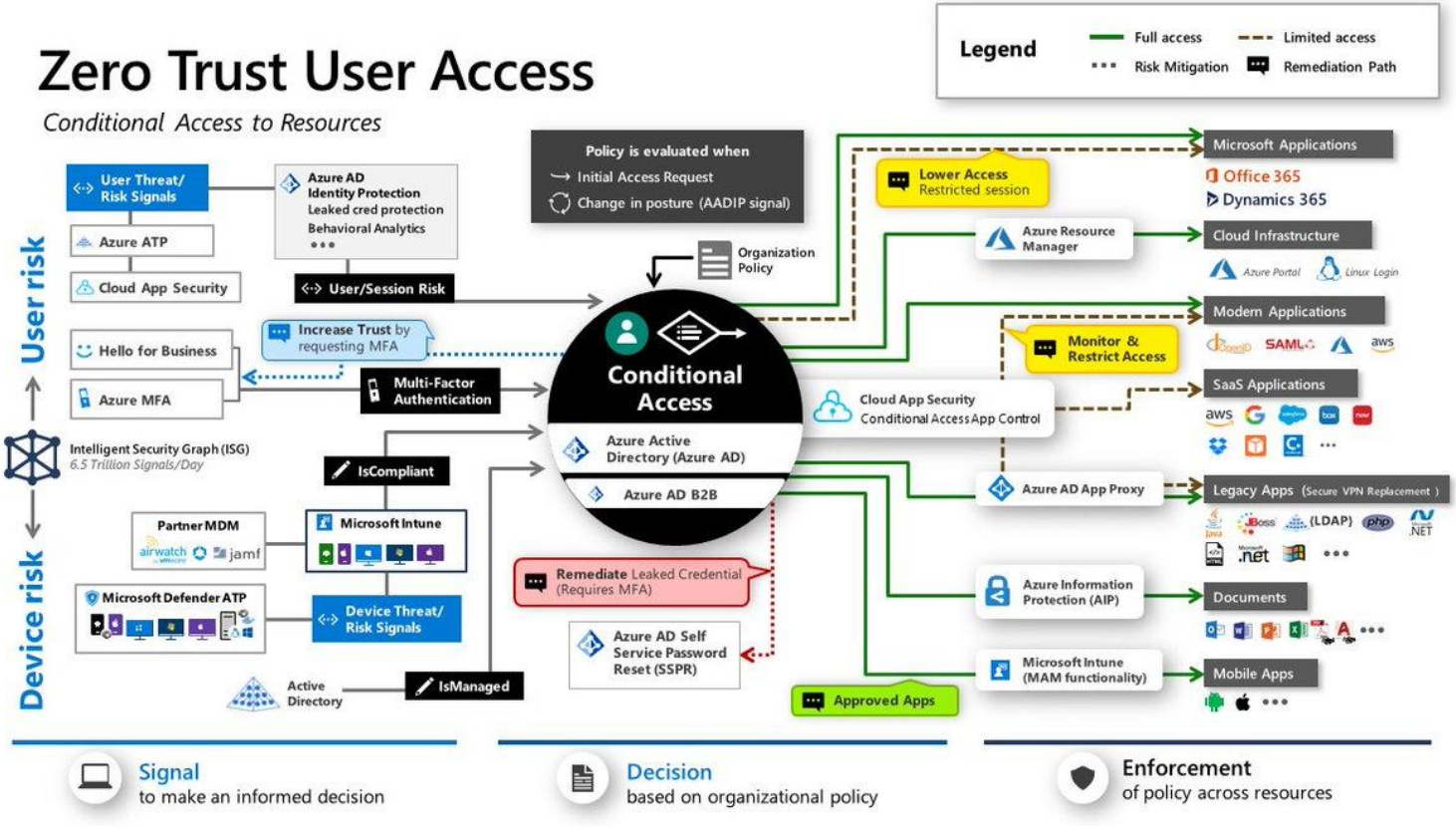
8. Control user authentication

Determine authentication methods;

- Passwords
- SMS
- Authenticator apps
- Password-less
- FIDO2
- App passwords
- Hardware tokens
- OAUTH

Implement secure authentication (MFA)

9. User Access



10. Monitoring and accounting

- Monitor user activity
- Monitor Login attempts
- Monitor breaches
- Alerting
- Proof of disposition

11. Access privileges

- Least privilege user access
- Role based access control
- Policy based access control
- Attribute based access control
- Need-to-know basis

Authentication

Authentication is the process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying credentials.

Authentication can come in many forms and formats. The type of authentication and which factors are used should be based upon risk.

Not all access requirements for resources are the same throughout and organizations infra- and applistructure.

12. User Provisioning

1. Manual/automatic provisioning
2. User (object) lifecycle management & policies

Provisioning

- On a provisioning level all the objects are being created according to the designs in the foundational level.
- Objects can be anything from devices up until actual end users.
- Objects are the actual identities which will allow an entity to authenticate, authorize and gain access towards resources.

Connections

On a connection level all the connections (trusts) are being made and managed towards and from the main IDP for the organization.

Setting up these trusts can be very complex and requires careful planning as this opens up the IAM environment for collaboration.

Access

- There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data. In this case we are talking about the latter one.
- Access can be granted in several ways. Again, the input for decision making should be risk based.
- Common best practice dictates that you should only have access to networks, system files and date on a need-to-know basis or if it is required to fulfill the current role of an end-user.

Sources:

1. SP 800-207, Zero Trust Architecture | CSRC (nist.gov)
2. Continuous Diagnostics and Mitigation (CDM) Program | CISA
3. https://www.enisa.europa.eu/
4. Cybersecurity Certification| CISSP - Certified Information Systems Security Professional | (ISC)² (isc2.org)
5. Certificate of Cloud Security Knowledge (CCSK) | CSA (cloudsecurityalliance.org)