WELCOME TO

Workshop Building the Roadmap for Your Future IAM

Martin Kuppinger
Principal Analyst & Founder
KuppingerCole Analysts AG

Christopher Schütze
CISO & Director Practice Cybersecurity
KuppingerCole Analysts AG

Dr. Phillip Messerschmidt
Lead Advisor & Analyst
KuppingerCole Analysts AG

Agenda

08:30 – 09:00	Welcome, Introduction and Methodology
09:00 – 10:15	Your IAM Capabilities Part I
10:15 – 10:30	Break
10:30 – 12:00	Your IAM Capabilities Part II
12:00 – 12:30	How to prioritize and create a roadmap

You need the app, and we need your attention

A workshop: collaborate, discuss, work and share

Technical prerequisites

On-Site and Remote:

- You need the KuppingerCole App
- You can download the handout in the App
- All polls will be done in the app

On-Site:

- Asking questions via App or just raising your hand

Remote:

- Asking questions only possible via app

Internet Access via WLAN

Name: EIC2023

Key: EIC2023!

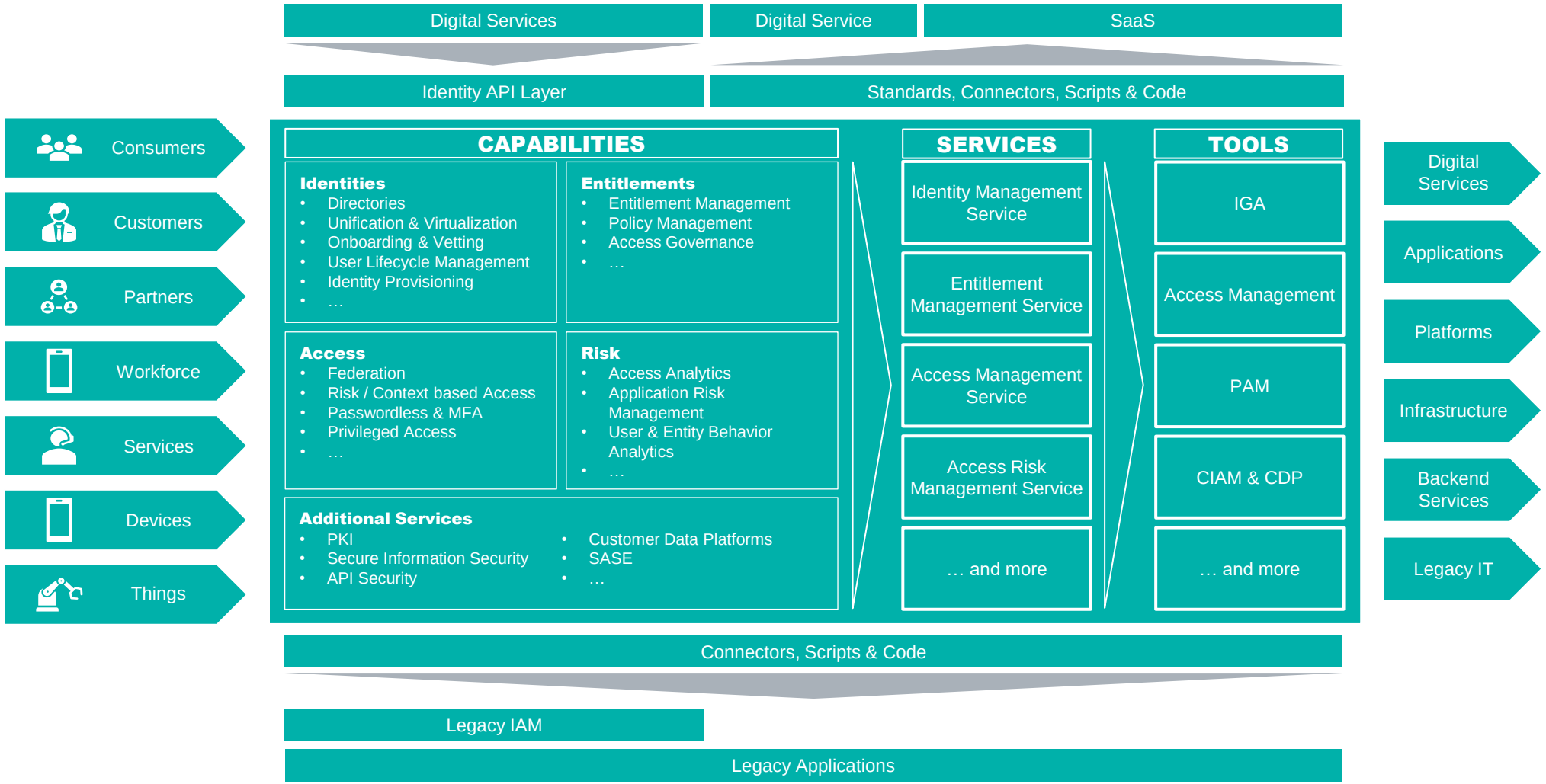
How we are going to run the workshop

Workshop methodology

1. **We explain the KuppingerCole Frameworks**
   - Identity Fabric
   - Reference Architecture
2. **We explain an individual building block**
   - You think about your organization and whether this is relevant for your or not
   - You enter your priority and maturity in the poll in the KuppingerCole App
   - GoTo: 2
3. **At the end: joint evaluation and building the target picture across all attendees**
   - No individual values will be shown
4. **We presents how to prioritize and create a roadmap**

Control through management of functions & services

Identity Fabric: A standard framework for architecting a modern IAM



Identity and Access Management is more than IGA

KuppingerCole IAM Reference Architecture: Key building blocks for IAM

Here are the average results leading to a IAM readiness

IAM Readiness Assessment based on the average value from all polls

Administration	Capability Level	Priority	Coverage
Directory Services	Core IAM	medium	0%
Identity Information Quality Mgmt	Core IAM	high	0%
Onboarding & Identity Vetting	Core IAM	high	0%
Decentralized Identity Issuance	Core IAM	high	0%
User Lifecycle Management	Core IAM	medium	0%
CIEM / DREAM	Core IAM	medium	0%
Entitlement Management	Core IAM	low	0%
Identity Provisioning	Core IAM	low	0%
User Self Service	Core IAM	medium	0%

Analytics & Risk	Capability Level	Priority	Coverage
Access Governance	Core IAM	high	0%
Access Analytics	Core IAM	high	0%
User & Entity Behavior Analytics	Core IAM	high	0%
Application Risk Management	Core IAM	high	0%
Privileged User Behavior Analytics	Core IAM	high	0%
Privileged Session Management	Core IAM	medium	0%

Authentication	Capability Level	Priority	Coverage
Adaptive Authentication	Core IAM	high	0%
Decentralized Identity Acceptance	Core IAM	low	0%
Credentials Management	Core IAM	high	0%
Web Access Management	Core IAM	high	0%
Decentralized Identity Federation	Core IAM	high	0%
Enterprise SSO	Core IAM	high	0%
Shared Account Password Mgmt	Core IAM	high	0%

Authorization	Capability Level	Priority	Coverage
Privilege Elevation	Core IAM	medium	0%
Policy-based Access Management	Core IAM	medium	0%
Just-in-Time Access (JIT)	Core IAM	medium	0%

IAM Readiness Assessment

Number of capabilities	Core IAM	Extended IAM	Integrations
high	14	0	0
medium	8	0	0
low	3	0	0
total	25	0	0

Priority Coverage	Core IAM	Extended IAM	Integrations
high	0%	0%	0%
medium	0%	0%	0%
low	0%	0%	0%
total	0%	0%	0%

Topic Coverage	Core IAM	Extended IAM	Integrations
Administration	0%	0%	0%
Analytics & Risk	0%	0%	0%
Authentication	0%	0%	0%
Authorization	0%	0%	0%
total	0%	0%	0%

There are several ways to use this IAM Assessment

Transition from the IAM Readiness Assessment into follow-up activities

IAM Readiness Assessment

Target state/architecture (functional & technical)

Status Quo (functional & technical)

Target Operating Model (TOM)

IAM Roadmap

Selection/Exchange of tools

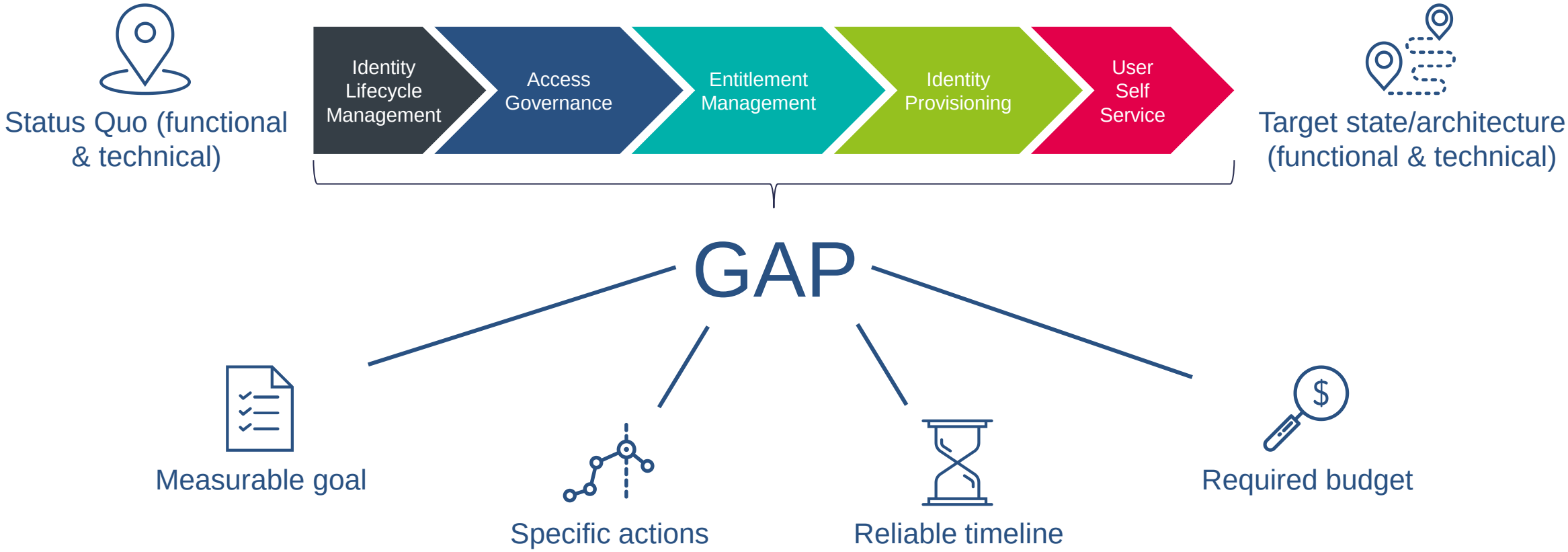
Improvements & activities as projects

Benchmarking

Support M&A

Deriving your IAM Roadmap is all about the gap

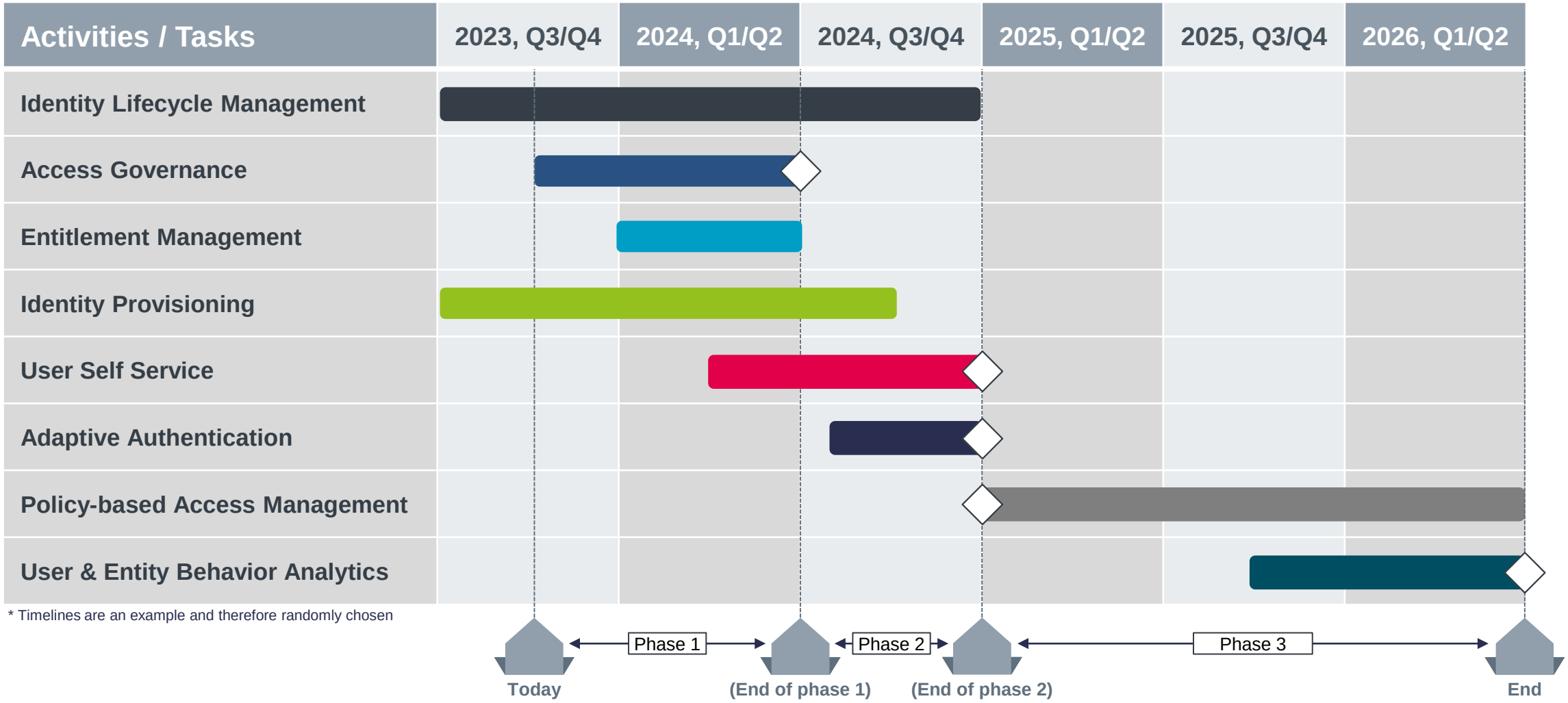
Building the Roadmap for Your Future IAM (1/2)



Operationalize your IAM Roadmap with a timetable

Building the Roadmap for Your Future IAM (2/2)

Exemplary illustration



THANKS!

Any questions?

If you have questions please reach out to:

- Martin Kuppinger (mk@kuppingercole.com)
- Christopher Schütze (chs@kuppingercole.com)
- Dr. Phillip Messerschmidt (phm@kuppingercole.com)

KuppingerCole Analysts AG
Wilhelmstr. 20 - 22
65185 Wiesbaden | GERMANY

P: +49 | 211 - 23 70 77 - 0
F: +49 | 211 - 23 70 77 – 11

E: info@kuppingercole.com
www.kuppingercole.com

Back-Up

Directory Services

Definition and Examples – Directory Services

Capability

Directory Services

Area

- Core IAM
- Administration

Definition

Directory Services as identity repositories are a core component of an IGA deployment and provide a mechanism to manage and store identities, identity attributes, access entitlements, and other identity related information strategically located and operated within the IT environment.

Examples

- Databases
- LDAP servers
- IoT Hubs
- Cloud directories

Related Acronyms

- UAP
- IGA
- ADFS

Identity Information Quality Management

Definition and Examples – Identity Information Quality Management

Capability

Identity Information Quality Management

Area

- Core IAM
- Administration

Definition

Mechanisms to consolidate data from source systems and to maintain constantly the required level of data quality. Functions provided include correlation of identities and data, cleanup and rewriting of attributes, lookup, and enrichment of identity data

Examples

- ETL solutions (Extract, transform, load)
- IGA-built-in data quality features
- Data Quality solutions

Related Acronyms

- IGA
- MDM
- DQM

Onboarding & Identity Vetting

Definition and Examples – Onboarding & Identity Vetting

Capability

Onboarding and Identity Vetting

Area

- Core IAM
- Administration

Definition

A verified digital identity is an important foundation for trusted IAM.
Enterprise applications such as new employee onboarding, access to sensitive applications, and account recovery are processes where proof of authenticity of a real-life identity is essential.
Consumer facing applications often require verification of identities e.g., for enabling trusted business relationships or ensuring compliance to embargo regulations.
This capability provides functions for the unique identification of a trusted digital identity for different identity types (internal and external persons, devices, etc.).
Verifiable Credentials for identification documents, diplomas, and more can be accepted by enterprises for new employee onboarding, making remote onboarding possible.

Examples

- Providers of verifiable credentials
- Remote identity proofing

Related Acronyms

- Dids
- UAP
- SCIM

DII is a future trend with a growing market

Definition and Examples – Decentralized Identity Issuance

Capability

Decentralized Identity Issuance

Area

- Core IAM
- Administration

Definition

Increasingly organizations also act as issuers of decentralized identities, that are a set of attributes, identifiers, and credentials that have been captured in a specific electronic format. A decentralized identity is cryptographically secure, so that even though your ID is stored in a digital format, it cannot be tampered with, duplicated, or stolen. The issuer organization is the entity that is responsible for that credential. The enterprise can then issue Verifiable Credentials to the new hire for use within the company: an employee ID, as belonging to a particular department, etc. These can be used as a form of authentication and as credential-based access control.
Integrations with systems like SAML and LDAP enable decentralized identity to become part of the traditional IAM structure.

Examples

- Providers of decentralized identities

Related Acronyms

- Dids
- AuthN
- AuthZ

Identity Lifecycle Management

Definition and Examples – Identity Lifecycle Management

Capability

Identity Lifecycle Management

Area

- Core IAM
- Administration

Definition

Identity lifecycle management provides the mechanisms for creation, modification, and deletion of identity and associated account information across the target systems and applications. Often referred to as Joiners, Movers, and Leavers (JML) processes, identity lifecycle management offers inclusive support for all identity related events either through available connectors for automated provisioning/ de-provisioning or use of workflows for manual intervention. Apart from the often-used term JML, identity lifecycle management goes far beyond these processes and often reflect detailed knowledge of organizational polices and processes.
Different types of identities can have different life cycles, which must then be reflected appropriately in each case. The goal is to understand an identity fully always over the course of its lifecycle and to represent it appropriately in terms of its attributes and entitlements.

Examples

- Usually part of IGA (Identity Governance and Administration) solutions
- Dedicated Workflow engines
- IT Service Management (ITSM)
- Discouraged: Homegrown scripts and tools

Related Acronyms

- JML
- ULM
- DREAM

CIEM / DREAM

Definition and Examples – CIEM / DREAM

Capability

CIEM / DREAM

Area

- Core IAM
- Administration

Definition

The multi-hybrid, multi-cloud infrastructure is becoming increasingly common, but this change in IT infrastructure and increasing use of agile development and DevOps tools means that the management of infrastructure must keep pace with the proliferation of entitlements across these complex and dynamic infrastructures.
Cloud Infrastructure Entitlement Management (CIEM) are aimed at helping organizations to manage identities and access across multiple clouds.
The DREAM (Dynamic Resource Entitlement & Access Management) model envisages common service development, delivery, and operations; infrastructure management and operations; and security and identity across on-prem, Edge, and private and public cloud, including managed service providers.

Examples

- Specific CIEM/DREAM products
- Some IGA solutions

Related Acronyms

- CIEM
- IGA
- PAM

Entitlement Management

Definition and Examples – Entitlement Management

Capability

Entitlement Management

Area

- Core IAM
- Administration

Definition

Entitlement management comprises both role/group management and policy management capabilities, but also covers further approaches to assign access to identities. This includes direct administrative assignment of entitlements within systems and applications.
Role Management is a strategic, but traditional approach for understanding an organizational structure and for describing and defining enterprise processes. As such it lays the foundation for assigning access by means of predefined roles to individuals. It is defined as the systematic and strategic approach for defining and administering both business and IT-level roles and their associated entitlements. While still widely used, especially in regulated industries, RBAC shows a variety of weaknesses, making alternative, more dynamic approaches to handling entitlements increasingly important.
To relieve complexity and increase efficiency, policy-based access control (PBAC) is used to assign access rights based on functional decisions, which are based on attributes of identities, in an automated way. Policy-based access, often also referred to as attribute-based access control (ABAC) demands for the proper definition of a policy framework.
Entitlement management provides the capabilities to manage roles concepts and their lifecycles, as well as policy frameworks and their lifecycles. These lifecycles include appropriate workflows and specifications for both roles and policies, such as request and approval processes, versioning, and historization.

Examples

- IGA tools
- Specialized role management solutions
- Policy-based Access Management solutions

Related Acronyms

- PBAC
- ABAC
- AuthZ

Identity Provisioning

Definition and Examples – Identity Provisioning

Capability

Identity Provisioning

Area

- Core IAM
- Administration

Definition

Identity Provisioning is about provisioning identities and access entitlements to target systems. This includes creating and managing accounts in connected target systems and associating the accounts with groups, roles, and other types of administrative entities to enable entitlements and authorizations in the target systems. Identity Provisioning aims at automating these tasks, based on defined processes for creating, updating, and deleting identity-related information in the target systems.

Core components in provisioning are connectors (also: adapters) that enable technical communication with the respective target systems. The challenge in provisioning is to maintain and prove successful communication for the provision of accounts and their attributes. To ensure that provisioning has taken place successfully and that no changes have subsequently been made to accounts and entitlements in the target system, reconciliation processes and techniques are used to enable the comparison of target and actual data.

Examples

- IGA solutions
- Enterprise Service Bus (ESBs)
- IT Service Management for manual and semi-automated provisioning

Related Acronyms

- ULM
- DREAM
- AD

User Self-Service

Definition and Examples – User Self-Service

Capability

User Self-Service

Area

- Core IAM
- Administration

Definition

Self-service user interface for users to maintain defined sets of attributes or to request access to IT assets such as applications, databases, and other resources. This includes the approval of such requests and further delegated operations.
User self-service covers the areas of password reset and account unlock.

Examples

- IGA solutions
- Workflow engines
- IT Service Management (ITSM)
- Password management services

Related Acronyms

- ITSM
- IDaaS

Access Governance

Definition and Examples – Access Governance

Capability

Access Governance

Area

- Core IAM
- Analytics & Risk

Definition

Access governance is one of the key IAM technology for any organization due to the massive impact of potential security risks arising from the lack of proper access governance controls. Access Governance is an IAM focused risk management discipline, focuses on providing answers to three key questions: Who has access to what? Who has accessed what and why? Who has granted that access? Access governance solutions focus on implementing and governing the controls for access management. This includes controls for attestation and recertification processes as well as auditing, reporting, and monitoring capabilities, which, in turn, invoke active management of preventive controls to identify and mitigate the access risks. Other risks managed include intellectual property theft, occupational fraud in ERP systems including SoD (Segregation of Duties) conflicts and other policy violations, reputational damage due to the loss of customer information and privacy-related data, and many more.

Key capabilities include:

Access Request Management: Access requests are a key capability requiring users to be able to identify the assets (applications, services…) they need access to and the specific entitlements. Access Request Management includes flexible approval workflows.

Access Reviews: Beyond regular review campaigns, risk-based and other types of reviews improve efficiency, reduce the workload for reviewers and focus on high-risk items. Additionally, Access Analytics identifies e.g., high-risk users and entitlements.

SoD management: Having more than one person required to complete a task is an administrative control used by organizations to prevent fraud, sabotage, theft, misuse of information, and other security compromises.

Examples

- IGA
- Workflow engines
- GRC tools

Related Acronyms

- UBA
- SoD
- PKI

Access Analytics

Definition and Examples – Access Analytics

Capability

Access Analytics

Area

- **Core IAM**
- **Analytics & Risk**

Definition

Analytical capabilities to facilitate business-friendly understanding of the current status of access controls to IT assets. This includes insight into the current state, but also support in continuous improvement of defined and assigned access. By covering the aspects of least privilege, and segregations of duties (SoD) access analytics supports in achieving compliance.

Access analytics is increasingly becoming a field where AI/ML is used to identify critical entitlements, for example, and assist administrators in making suggestions for optimization.

Examples

- **IGA tools**
- **Business intelligence solutions**
- **Dedicated Access Analytics tools**

Related Acronyms

- **IAG**
- **SoD**
- **UAM**

User & Entity Behavior Analytics

Definition and Examples – User & Entity Behavior Analytics

Capability

User & Entity Behavior Analytics

Area

- Core IAM
- Analytics &

Definition

UEBA tools consume the user's access activity such as authentication and authorization information across IT applications and systems to establish and continuously update user access patterns based on their role and peers' group. These analytics can also feed user access information from authentication and authorization events to AI/ML tools for prototyping user access behavior patterns and detecting anomalous access.

Examples

- IGA tools
- Specific UBA / UEBA tools

Related Acronyms

- IAG
- SIEM
- SOCs

Application Risk Management

Definition and Examples – Application Risk Management

Capability

Application Risk Management

Area

- Core IAM
- Analytics & Risk

Definition

Application risk management solution look at access risks within line-of-business (LoB) applications, to ARM (Application Risk Management), to deliver a comprehensive, unified insight into the state of access risks and regulatory compliance.
They aim at providing comprehensive insights across all types of LoB applications and beyond. They look at insufficient SoD (Separation of Duties) rules, but also the fact that overentitlements and access risks are continuously used by both internal and external attackers.

Examples

- IGA tools
- Dedicated ARM tools
- IT Risk Management

Related Acronyms

- IRM
- GRC

Privileged User Behavior Analytics (PUBA)

Definition and Examples – Privileged User Behavior Analytics (PUBA)

Capability

Privileged User Behavior Analytics (PUBA)

Area

- Core IAM
- Analytics & Risk

Definition

PUBA extends user and entity behavior analytics towards privileged use cases. PUBA uses data analytic techniques, some assisted by machine learning tools, to detect threats based on anomalous behavior against established and quantified baseline profiles of administrative groups and users. Any attempted deviation from least privilege would be red flagged.

Examples

- Privileged Access Management Solutions

Related Acronyms

- PAM
- EPM
- PADLM

Privileged Session Management

Definition and Examples – Privileged Session Management

Capability

Privileged Session Management

Area

- Core IAM
- Analytics & Risk

Definition

A privileged session is any session (interactive or automated) that is executed by an account with elevated access rights.
Privileged Session Management offers basic auditing and monitoring of privileged activities. Privileged Session Management is a central component of PAM as a far-reaching IT security process. As such, it can be used to control, monitor, and record administrative access to servers, databases, and network devices. Properly implemented access controls monitor allowed access based on request and approval. Approval can be given by a colleague or supervisor, for example. Less critical access can also be automated and without loss of time based on well-defined policies. Privileged Session Management offers the technology to establish a privileged session to target systems including basic auditing and monitoring of privileged activities. Session Management tools can also offer authentication and Single Sign-On (SSO) to target systems.
Privileged Session Management is often augmented with basic Session Recording Management capabilities. These offer advanced auditing, monitoring, and review of privileged activities during a privileged session. This includes:

- **key-stroke logging**
- **video session recording**
- **screen scraping**
- **OCR translation and further session monitoring techniques**

Examples

- **Privileged Access Management Solutions**
- **Limited support in CIEM / DREAM**

Related Acronyms

- **PAM**
- **AAPM**
- **SSO**

Adaptive Authentication

Definition and Examples – Adaptive Authentication

Capability

Adaptive Authentication

Area

- Core IAM
- Authentication

Definition

Adaptive Authentication (AA) is the process of gathering additional attributes (including strong, e.g. biometric features) about users and their environments and evaluating the attributes in the context of risk-based policies. The goal of AA is to provide the appropriate risk-mitigating assurance levels for access to sensitive resources by requiring users to further demonstrate that they are who they say they are. This is usually implemented by "step-up" authentication.

A wide variety of adaptive authentication mechanisms and methods exist in the market today. Examples include:

- **Knowledge-based authentication (KBA)**
- **Strong/Two-Factor or Multi-Factor Authentication (Smart Cards, USB authenticators, biometrics)**
- **One-time password (OTP), delivered via phone, email, or SMS**
- **Mobile push notifications / Out-of-band (OOB) application confirmation**
- **Identity context analytics, including**
  - **IP address**
  - **Geo-location**
  - **Geo-velocity**
  - **Device ID and device health assessment**
  - **User Behavioral Analysis**

Examples

- **Access Management Solutions**
- **Enterprise Authentication Solutions**
- **Customer/Consumer Authentication Solutions**

Related Acronyms

- **KBA**
- **MFA**
- **OOB**

Decentralized Identity Acceptance

Definition and Examples – Decentralized Identity Acceptance

Capability

Decentralized Identity Acceptance

Area

- Core IAM
- Authentication

Definition

The ability to accept, trust and use decentralized identities in access management.
Decentralized identities can add strong verified biometric, or real-world identity factors to an authentication.
Acceptance of decentralized identities as an authentication method supports both workforce and consumer IAM, as does decentralized identity federation.

Examples

- Access Management Solutions
- Federation services

Related Acronyms

- Dids
- AA

Credentials Management

Definition and Examples – Credentials Management

Capability

Credentials Management

Area

- Core IAM
- Authentication

Definition

This block comprises functionalities around the administration of authentication factors and further credentials. This includes both the management of passwords, i.e. changing passwords, resetting passwords, etc., and the management of other factors, i.e. on-boarding and lifecycle management of hardware and software tokens for strong authentication factors. It also includes the management of other factors, i.e. on-boarding and lifecycle management of hardware and software tokens for strong authentication.

Examples

- Access Management Solutions

Related Acronyms

- authN
- SCIM

Web Access Management

Definition and Examples – Web Access Management

Capability

Web Access Management

Area

- Core IAM
- Authentication
- Authorization

Definition

(Web) Access Management is a rather traditional approach that puts a layer in front of web applications that takes over authentication and – usually coarse-grained – authorization management. Legacy access management wraps existing legacy application into a management layer to integrate them into an overall access management.

Examples

- Web Access Management Solutions
- Broader Access Management Solutions

Related Acronyms

- Oauth2
- SAML
- OIDC

Identity Federation

Definition and Examples – Identity Federation

Capability

Identity Federation

Area

- Core IAM
- Authentication
- Authorization

Definition

Identity federation is a system of trust between two parties for the purpose of authenticating users and conveying information needed to authorize their access to resources. Thus, federation is a capability that allows splitting authentication and authorization between an IdP (Identity Provider) and a Service Provider (SP) or Relying Party (RP). Identity Federation can be used in various configurations, including federating from internal directories and authentication services to Cloud Service Providers or between different organizations.

Examples

- Access Management Solutions
- Enterprise Authentication Solutions
- Customer/Consumer Authentication Solutions

Related Acronyms

- IdP
- SP
- SSO

Enterprise SSO

Definition and Examples – Enterprise SSO

Capability

Enterprise SSO

Area

- Core IAM
- Authentication

Definition

Enterprise SSO (E-SSO) provides centrally managed solutions that grant access to various applications, both traditional “fat client” and web applications, while being fully transparent to the applications and thus non-intrusive, in contrast to other approaches such as Identity Federation.

Examples

- Enterprise SSO Solution
- Access Management Solutions
- Integrated in IAM/IGA suites

Related Acronyms

- TGT
- JWT
- SAML

Shared Account Password Management

Definition and Examples – Shared Account Password Management

Capability

Shared Account Password Management

Area

- Core IAM
- Authentication

Definition

Shared accounts are resources that have a single pair of credentials but are used to authenticate multiple users. Shared resources are not target system-specific, but can be tied to any platform, system, infrastructure, or service.
Shared Account Password Management offers technology to securely manage privileged credentials including system accounts, service accounts, or application accounts that are generally shared in nature. At the core of SAPM products is an encrypted and hardened password vault for storing passwords, keys, and other privileged credentials for a controlled, audited, and policy-driven release and update. Frequently, Password Vaults also manage SSL/TLS keys, encryption keys, SSH keys, access to cloud services, and other confidential data in their vaults.
This includes the management and rotation of passwords and access to them. Access scenarios can vary. In the simplest case, an administrative user requests the password that is provided to him for one-time use (Password Checkout). A better solution is to transparently inject the password into an initiated session after extraction from the vault, so that the administrator never has direct knowledge of the password.

Examples

- Privileged Access Management Solutions

Related Acronyms

- PAM
- PSM
- PUBA

Privilege Elevation

Definition and Examples – Privilege Elevation

Capability

Privilege Elevation

Area

- **Core IAM**
- **Authorization**

Definition

Privilege Elevation allows users to gain elevation of access rights, traditionally for administrative purposes and for short periods with least privilege rights.

Examples

- **Privileged Access Management Solutions**

Related Acronyms

- **CEPDM**
- **PAM**

Policy-based Access Management

Definition and Examples – Policy-based Access Management

Capability

Policy-based Access Management

Area

- Core IAM
- Authorization

Definition

Policy-based Access Management (Attribute Based Access Control / Dynamic Authorization Management) is an authorization capability in which organizations leverage their identity and access management environment to control access to restricted resources. Access control to file shares, network subnets, document repositories, and applications are made in real-time by a centrally managed decision point, using attributes in a user's directory entry. Increasingly context information is additionally taken into consideration (see: Adaptive authentication)

Examples

- Policy Based Access Management Solutions

Related Acronyms

- Authz
- DAM
- AD

Just-in-Time Access (JIT)

Definition and Examples – Just-in-Time Access (JIT)

Capability

Just-in-Time Access (JIT)

Area

- Core IAM
- Authorization

Definition

JIT solutions ensure that identities have only the appropriate privileges: when necessary, as quickly as possible, and for the least time necessary. This process can be entirely automated so that it is frictionless and invisible to the end user.

Based on already granted access to a system (in general, but not active), there is a request for actual access, which can be subsequently approved (Auto-approval or policy-based approval or manual approval) and verified (e.g., potential SoD checks). Activation of access and actual access are allowed during the approved period and deactivation of access takes place after a defined grace period.

Examples

- Privileged Access Management Solutions
- Modern Access Management Solutions, especially Policy Based Access Management

Related Acronyms

- Authz
- PAM
- PBAC

PKI

Definition and Examples – PKI

Capability

PKI

Area

- **Extended IAM**
- **Administration**

Definition

Public Key Infrastructures (PKI) facilitate the issuance and management of digital certificates to protect sensitive data. They are therefore essential systems in many companies for providing unique digital identities for users, devices, and applications, establishing confidentiality and enabling secure end-to-end communication.

Examples

- **Dedicated PKI solutions, e.g. Certificate authorities (CAs)**
- **Provided as part of server infrastructure, e.g. Microsoft AD**

Related Acronyms

- **IAG**
- **CMK**
- **DEK**

Secrets Management

Definition and Examples – Secrets Management

Capability

Secrets Management

Area

- **Extended IAM**
- **Administration**

Definition

Secrets Management manages the secrets that applications and other non-human identities need to gain access to infrastructure, data, and other resources. Based on policy- or role-based access control with native attributes of the accessing identity, the required secrets can be provided (especially sensitive secrets such as passwords, SSH keys, and web service or API keys).

Examples

- **Dedicated Secrets Management tools**
- **Privileged Access Management Solutions**
- **CIEM / DREAM**

Related Acronyms

Fraud Reduction & Intelligence

Definition and Examples – Fraud Reduction & Intelligence

Capability

Fraud Reduction & Intelligence

Area

- Extended IAM
- Analytics & Risk

Definition

Fraud Reduction Intelligence comprises a set of capabilities to reduce fraud at runtime based on various aspects. Typical capabilities include:

- **ID Proofing – verification that the proper user subject is issued digital credentials, often validated against government-issued ID credentials.**
- **Credential Intelligence - information about prior usage of digital credentials, to answer questions such as "has this credential known to have been recently compromised?" or "has this credential been used for fraud at other sites?"**
- **User Behavioral Analysis (UBA) – examination of past user activities to determine if the current transaction request is within normal parameters.**
- **Device Intelligence - includes device hygiene (OS patch versions, anti-malware client presence, and RAT detection), device history and reputation, location history, IP reputation, etc.**
- **Behavioral/Passive Biometrics – the ability to analyze metrics of users' physical interaction with devices for comparison against registered samples.**
- **Bot Detection – evaluation of pertinent cyber threat intelligence on botnet activities.**

Examples

- **Dedicated Fraud Reduction and Intelligence Platforms**
- **Sometimes delivered through Access Management Solutions**

Related Acronyms

Data Access Governance

Definition and Examples – Data Access Governance

Capability

Data Access Governance

Area

- Extended IAM
- Analytics

Definition

Data Governance is about taming layers of unstructured data and aligning data to the business strategy or the organization. Unstructured data has little value if it cannot be organized and shared across the organization and aligned with the business. The primary goal for Data Governance platforms is to classify and protect files and other data sources in line with organizations policies and goals.
These tools manage access requests, approvals, certification, and analysis of the entitlements at a more granular level. Compliance and security are key drivers for Data Governance platforms, but there is also an added benefit in deriving business value from organized data by offering capabilities that allow analysis of data to provide unique business insights. This is where governance meets business innovation and competitive instincts.

Examples

- Dedicated Data Access Governance Tools
- Data Governance solutions (in combination with Data Catalogs and Metadata Management)
- Less frequently in IGA solutions

Related Acronyms

- IAG
- SoD

Cloud Access Security Broker

Definition and Examples – Cloud Access Security Broker

Capability

Cloud Access Security Broker

Area

- Extended IAM
- Authentication

Definition

CASBs address the challenges of security and compliance around the use of cloud services. They provide security controls that are not available through existing security devices and a point of control over access to cloud services by any user and from any device. The market for CASBs has evolved from the first products that focused on the discovery of cloud usage, through network access control points to become integrated cloud security solutions.

The fundamental functionalities that these solutions provide are:

- **Discovery of the cloud services being used, by whom and for what data.**
- **Control over who can use which services and what data can be transferred or accessed.**
- **Protection of data in the cloud against unauthorized access and leakage.**
- **The capabilities to enforce and demonstrate compliance with regulations.**

Examples

- **Dedicated CASB solutions**
- **Components within integrated cloud security solutions**

Related Acronyms

- **SaaS**
- **DLP**
- **UEBA**

API Security & Management

Definition and Examples – API Security & Management

Capability

API Security & Management

Area

- Extended IAM
- Authentication
- Authorization

Definition

As there is a rapidly growing demand for exposing and consuming APIs, which enables organizations to create new business models and connect with partners and customers, many organizations are adopting e.g., lightweight RESTful APIs.
Core API management capabilities include basic API gateway functionality, native identity management, monitoring, and analytics capabilities.
A proper, well-planned strategy for protecting various internal and external, own, and 3rd-party APIs must address every step along the API lifecycle, which, at least for APIs developed in-house, starts with secure design, long before the operational phase. At later phases, several different technologies must be applied, including but not limited to network security (encryption, firewalling, DLP, etc.), protection against numerous API-specific threats and exploits, strong authentication and fine-grained access control, maintaining sensitive data integrity, as well as monitoring and analytics.

Examples

- API Management Solution
- API Security Solutions
- Cloud platforms with built-in API gateways

Related Acronyms

- DSG
- OIDC
- TLS

Web Application Firewalls

Definition and Examples – Web Application Firewalls

Capability

Web Application Firewalls

Area

- Extended IAM
- Authentication

Definition

Web Application Firewalls (WAF) provide the capability to protect web-based applications as well as its data, which are commonly found in small to large organizations. They are used to protect web applications through inspection of HTTP traffic. WAFs often act as a reverse proxy to inspect the traffic flows or requests before they arrive at the origin web application. A similar approach can also be used to examine requests going from the web application server to the end-user. More advanced WAF capabilities protect against the more complex and changing types of web attacks. These more advanced capabilities often protect against malicious web bots.
Typical capabilities include DDoS Protection, Rule-based Detection, OWASP top 10, Logging, Reporting, Centralized Management, Hybrid Deployment Models, Bot Management, API Protection, Threat Intelligence and Compliance Reporting.

Examples

- Dedicated Web Application Firewalls
- Web Access Management Solutions

Related Acronyms

- DDoS
- SIEM
- OWASP

Secure Information Sharing

Definition and Examples – Secure Information Sharing

Capability

Secure Information Sharing

Area

- **Extended IAM**
- **Authorization**

Definition

To support business processes, it is important to be able to provide access to sensitive data, but it is also important that cyber security and governance requirements are adequately observed. Solutions to the management of access to shared data are diverse. The products fall into two broad approaches:

- **Secure repository with strong access control on file access. These solutions typically use encryption to protect documents and provide a key management solution. In some cases, a single repository is supported; this might be an on-premises storage facility, or it might be a cloud-based managed service. In other cases, a captured environment is used whereby documents are encrypted so that they can be stored anywhere, but they can only be accessed by a client that can decrypt them.**
- **Rights management approach whereby solutions validate user permissions to access/modify a document at the time access is requested. Several solutions in this space support Microsoft Azure Information Protection, some adopt their own information rights management solution, and some solutions use client software to manage external storage or emailing. The provision of classification capabilities is important to customers since documents need to be appropriately codified for a rights management system to be effective.**

Examples

- **Secure repositories**
- **Secure Collaboration & Sharing Platforms (Rights Management)**
- **Industry Collaboration Platforms**

Related Acronyms

- **IRM**
- **RMS**

IT Service Management

Definition and Examples – IT Service Management

Capability

IT Service Management

Area

- **Integrations**
- **Administration**

Definition

IT service management (ITSM) solutions aim at delivering IT management capabilities to help organizations to continually optimize the design, delivery, support, use, and governance of IT services to cut costs, increase productivity and efficiency, and improve employee and customer satisfaction.

ITSM is based on the concept of IT delivered as a service to meet business needs. In this context, an IT service is any piece of IT that enables users to find, access, view, update, report, and exchange data to achieve the outcome of meeting business needs and potentially improving the satisfaction of service users through improved ease of use, efficiency, and productivity. IT services include laptops, applications, managed services, and shared IT resources.

Typical ITSM capabilities include: Incident Management, Problem Management, Configuration Management, Change Management, Release Management, Service Desk, Self-Service Portal, SLA Management, Asset Lifecycle Management, IT Knowledge Management

Examples

- **Dedicated IT Service Management solutions**

Related Acronyms

- **IGA**
- **ESM**

SIEM & SOAR

Definition and Examples – SIEM & SOAR

Capability

SIEM & SOAR

Area

- Integrations
- Analytics & Risk

Definition

Traditional SIEMs are unified platforms for gathering, analyzing, and correlating security events from multiple sources to provide a centralized overview of all security-related events across the whole enterprise, alert the team of security experts, and provide tools for forensic analysis. SIEMs serve as a focal point (if not the only component) of their Security Operations Centers (SOC).

New intelligent automation capabilities, whether integrated directly into newer SIEM solutions or augmenting the existing ones with new functions, ensure that security monitoring, forensic analysis, and incident response remain a core component of any modern cybersecurity architecture.

Security Orchestration, Automation, and Response (SOAR) platforms are designed to provide a centralized analyst and management interface for security teams. They consolidate security event information and allow for faster and more efficient investigations and responses. SOAR solutions can help organizations reduce the Mean Time to Detect (MTTD) and Mean Time to Resolve (MTTR) security incidents.

The orchestration aspect of SOAR involves not only the collection of telemetry from different sources (including SIEM), but also initiating a workflow, opening cases and tickets where appropriate, and correlation and enrichment of event information. Enrichment of event data can be facilitated by SOAR systems by the automatic collection of additional forensic evidence on-site, such as outputs of EPP scans, obtaining non-standard log files, memory dumps, etc. Some solutions can kick off automated threat hunts (looking for IOCs across multiple nodes in an environment) and add the results to a preliminary investigation.

Examples

- SIEM & “Next-Gen SIEM”
- SOAR
- XDR

Related Acronyms

- IAG
- SOCs
- UEBA

IT Risk Management / IT GRC

Definition and Examples – IT Risk Management / IT GRC

Capability

IT Risk Management / IT GRC

Area

- Integrations
- Analytics & Risk

Definition

IT Risk Management encompasses the policies, procedures, and technologies that a company employs to mitigate negative impacts on IT and thus on the business processes mapped in it. The aim is, on the one hand, to mitigate threats from malicious actors and, on the other, to reduce vulnerabilities in information technology that have a negative impact on the confidentiality, integrity, and availability of data.
IT GRC as the bigger picture enables organizations and businesses to create and organize GRC policies and controls, and assists organizations keep on top of an increasingly complex and changing regulatory environment.

- Governance: sets objectives and rules for an organization
- Risk: the threat to those objectives and rules
- Compliance: the range of laws and regulations that an organization must meet

As a baseline, an IT-GRC solution supports the most common forms of compliance controls and standards such as ISO 27x series, COBIT, ITIL etc., dashboard controls, log management and reporting functions.
Increasingly, varying levels of automation that allow departments to perform significant GRC checks without consultants and senior IT involvement are added, including AI/ML capabilities.

Examples

- IT GRC platforms
- Part of broader Integrated Risk Management Platforms

Related Acronyms

- IRM
- VM
- GDPR

Privacy & Consent Management

Definition and Examples – Privacy & Consent Management

Capability

Privacy & Consent Management

Area

- Integrations
- Authorization

Definition

Privacy and Consent Management stands for the administrative and governance capabilities over data privacy within the organization. They are designed to enable compliant data collection, build compliant consumer profiles, and monetization while enabling the privacy choices of end users and the intersection of global regulations.

Key capabilities include

- **Compliance support for global privacy regulations including GDPR and CCPA**
- **Compliant collection of user consent**
- **Enforcement of user consent**
- **Prevent non-compliant tracking and profiling on customer channels**
- **Provide insight into movement and protection of personal data within the organization and in transit to partners**
- **Data mapping and inventory of personal data in the enterprise**
- **Provide data risk management support, for example de-identifying data via anonymization, pseudonymization, aggregation, redaction, or differential privacy**
- **Support in the design, implementation, and enforcement of privacy policies**
- **Enable self-service privacy choices for users**

Examples

- **Privacy and Consent Management**

Related Acronyms

- **CMP**
- **IAM TCF**
- **DPIA**