



SAP® MaxAttention™ Innovation Workshop

Enhance Cybersecurity and Compliance in Your SAP Environment

Virtual, June 17, 2021

PUBLIC

Agenda **Thursday June 17, 2021**

- Welcome & Introduction - Colin Hughes
- [Cyber Risks: Recent Cyberattacks on SAP Customers](#) - Brian Gonsales
- [Risk Scenario: Monitoring & Threat Detection](#) - Brian Gonsales
- [Securing Your SAP Environment with SAP Premium Engagements](#) - Brian Gonsales
- [Risk Scenario: Access Risk and Segregation of Duties](#) - Brian Gonsales
- [Risk Scenario: Data Protection and Privacy](#) - Brian Gonsales



SAP® MaxAttention™ Innovation Workshop

Enhance Cybersecurity and Compliance in Your SAP Environment

Brian Gonsales
June 2021

PUBLIC

Welcome!

In this session, we will discuss:

- **Common scenarios** in focus topic Cybersecurity & Compliance;
- How products in the **SAP Security Portfolio** can help increase Security of your landscapes (On-premise, Cloud and Hybrid);
- Demonstrate how SAP **Premium Engagement** services can help customers innovate with confidence.



Agenda

Time	Duration	Topic	Speaker
09:00 a.m. GMT 10:00 a.m. CET	0:15	Welcome & Introduction	Colin Hughes Head of Premium Engagements EMEA North, Customer Success, SAP
09:15 a.m. GMT 10:15 a.m. CET	0:15	Cyber Risks: Recent cyberattacks on SAP customers - Real world examples of threats	
09:30 a.m. GMT 10:30 a.m. CET	0:30	Risk Scenario: Monitoring & Threat Detection - Introduction to SAP Secure Operations Map - Cyber Intrusion - System Outages	
10:00 a.m. GMT 11:00 a.m. CET	0:15	Break	Brian Gonsales Technical Lead, CoE Cybersecurity & Compliance, Customer Success, SAP
10:15 a.m. GMT 11:15 a.m. CET	0:30	Securing Your SAP Environment with SAP Premium Engagements - Methodology and Service Flow	
10:45 a.m. GMT 11:45 a.m. CET	0:30	Risk Scenario: Access Risk and Segregation of Duties - Segregation of Duties - Operational Access Downtime	
11:15 a.m. GMT 12:15 p.m. CET	0:30	Risk Scenario: Data Protection and Privacy - Data Leak Events - Regulatory Compliance	Colin Hughes Head of Premium Engagements EMEA North, Customer Success, SAP
11:45 p.m. GMT 12:45 p.m. CET		Q&A and Closing	

Poll #1

Provide feedback using the “Polls” functionality on Zoom



Where to find help?

Frequently asked questions in Cybersecurity & Compliance



"I have a question about..."

... a specific product feature.

Example:

"Does the SuccessFactors platform provide Audit Log information?"



SAP Help Guides

help.sap.com

1. Search for the Product in question (e.g. SuccessFactors platform)
2. Look for guides under *Security* or *Administration* sections

... Compliance certifications for SAP Cloud solutions.

Example:

"Is Concur ISO 27001-certified?"



SAP Trust Center

sap.com/about/trust-center/

Use the **Compliance Finder** to display the desired certification for your SAP solution.

Where to find help?

Frequently asked questions in Cybersecurity & Compliance



"I have a question about..."

... A Security-related issue that needs troubleshooting.

Example:

*"The Single Sign-On flow for one of my Cloud solutions just broke.
Can SAP help me troubleshoot and fix it?"*



SAP ONE Support Launchpad

launchpad.support.sap.com

Raise a customer incident.

... a cybersecurity vulnerability I have just discovered.

Example:

*"I have discovered an exploit in a standard ABAP program.
How can I report this to SAP?"*



SAP Product Security Response Team

[SAP Trust Center](#)

Customers can report issues via regular Support incident.
Cybersecurity researchers must submit a **security vulnerability form**.

... security best practices for AS ABAP, Java or HANA.

Example:

"What's the recommended password policy for Productive ABAP systems?"

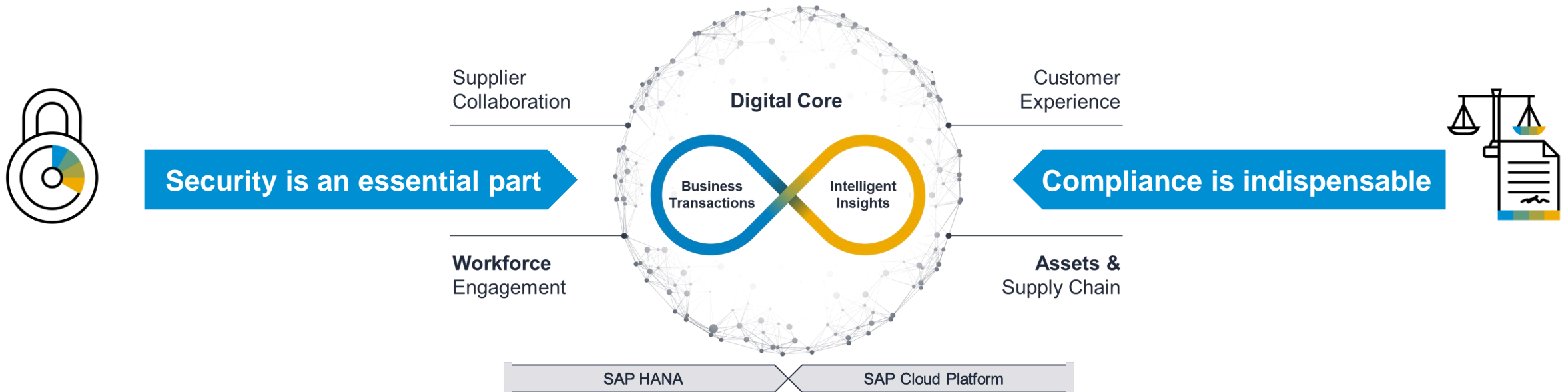


SAP Security Baseline Template

support.sap.com/sos or [SAP Note 2253549](#)

Why do we need Cybersecurity & Compliance?

The SAP Digital Transformation Framework



SAP invests significantly to provide secure software compliant with regulatory demands

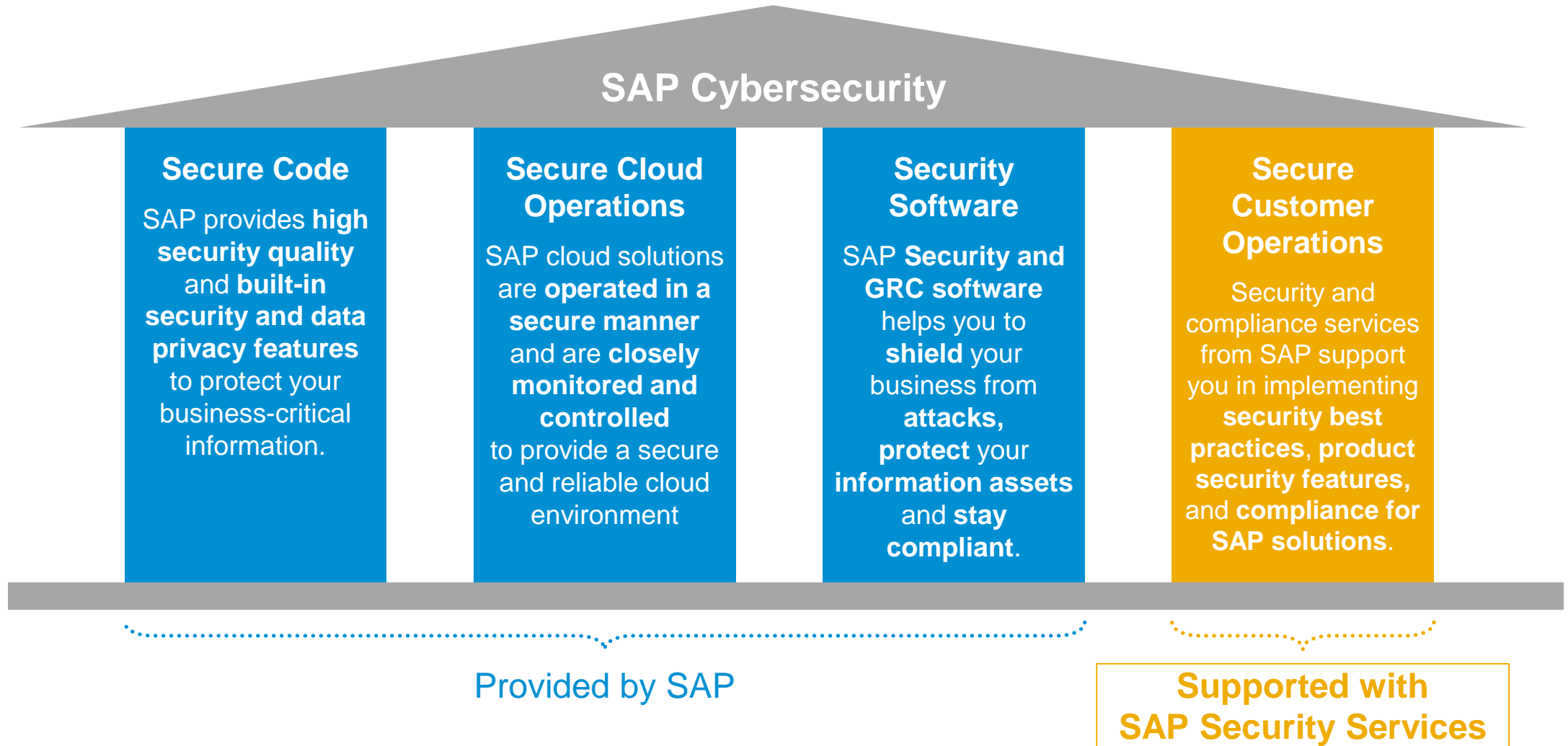
SAP business software provides **high security quality** and **built-in security and data privacy & protection features** to protect your business-critical information.

SAP **security and GRC software** can help you **shield** your business from **attacks**, **protect** your **information assets** with secure solutions and **stay compliant**.

If not designed, built, and run securely and compliant by the customer, the resulting landscapes will remain insecure and non-compliant

Security and compliance engagement services from SAP Digital Business Services offer support to implement **security best practices**, **product security features**, and **compliance for SAP solutions**.

Pillars of SAP Cybersecurity & Compliance



Our Basic Offering: SAP “Best Practice” Security Services

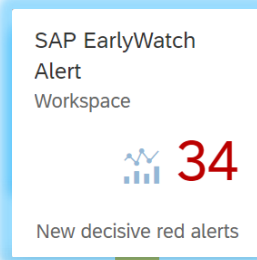
Available to all customers, free of charge

More details on SOS Landing Page: support.sap.com/sos

Comparison against SAP recommendations

Security in EarlyWatch Alert (EWA)

Overview



Security Optimization Service
System Recommendations

Detail

A

System	IT Admin Role	System Priority	Security Notes	Hot News	Performance Notes	Legal Change Notes	License Audit Notes
SABRY-SP-ATC	Quality Assurance System	Undefined	12	98	278	522	20
S84-WAS-ATC	Undefined	Undefined	32	112	303	546	15
S81-WAS-ATC	Undefined	Undefined	36	113	326	562	21
A28-ABAP	Undefined	Undefined	15	101	406	604	5
A75-JAVA	Undefined	Undefined	76	104	272	526	19
A82-JAVA	Undefined	Undefined	83	108	274	527	17

Company's
Security
Policy

Company's
SAP Security
Baseline

Target
System

Comparison against company's security policy

Management Dashboard



Configuration Validation

C

System	IT Admin Role	System Priority	Security Notes	Hot News	Performance Notes	Legal Change Notes	License Audit Notes
SABRY-SP-ATC	Quality Assurance System	Undefined	12	98	278	522	20
S84-WAS-ATC	Undefined	Undefined	32	112	303	546	15
S81-WAS-ATC	Undefined	Undefined	36	113	326	562	21
A28-ABAP	Undefined	Undefined	15	101	406	604	5
A75-JAVA	Undefined	Undefined	76	104	272	526	19
A82-JAVA	Undefined	Undefined	83	108	274	527	17

Service delivery example:

A Automated services indicate security gaps

Recommendation: Detailed look into gaps through experts

Service – Part 1:

- B**
- Root cause analysis for security gaps
 - SAP Security Baseline maintenance

Service – Part 2:

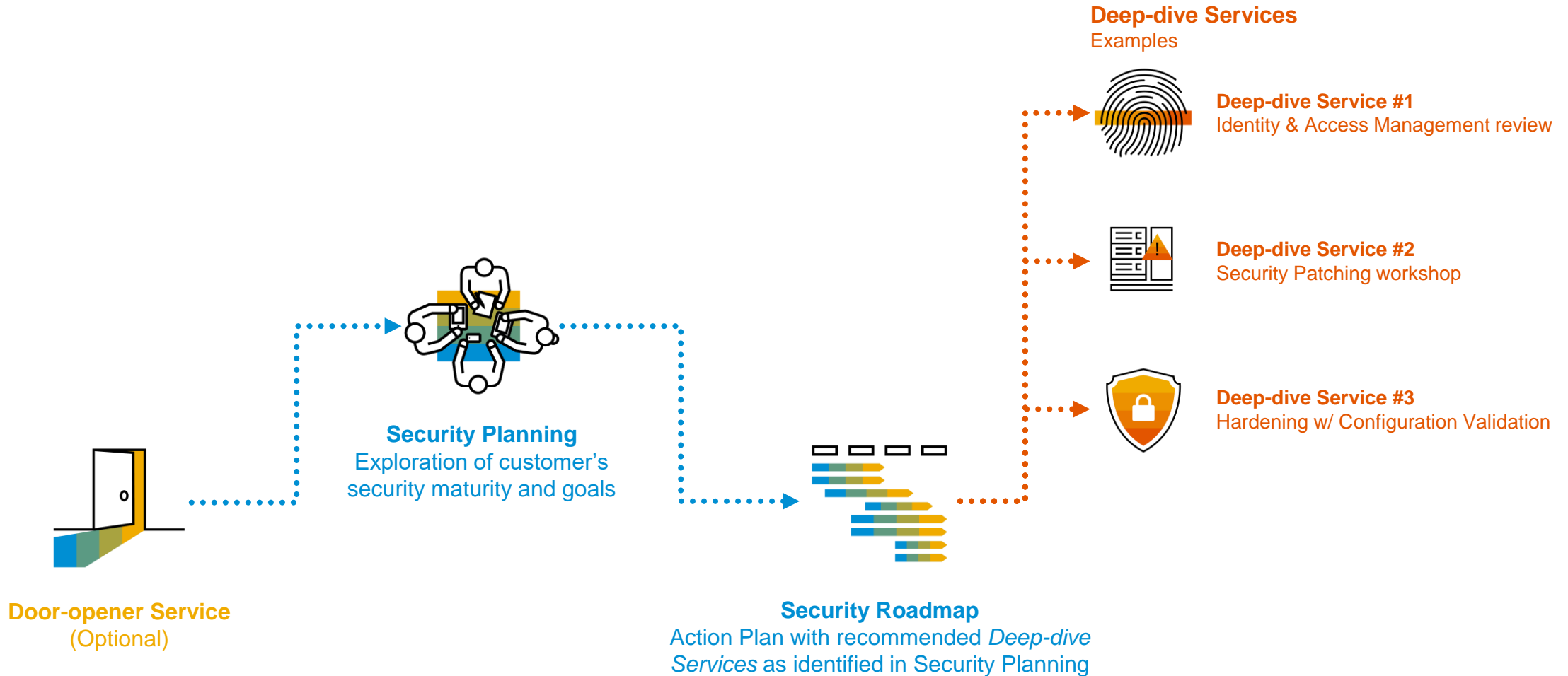
- C**
- Security patch deployment cycle
 - Configuration setup
 - Proactive threat identification

Service – Part 3:

- D**
- Security control via dashboard

Cybersecurity & Compliance: Service Flow

(Simplified view)



SAP Security Software: The GRC Solution Portfolio



Enterprise Risk and Compliance

- ✓ SAP Risk Management
- ✓ SAP Process Control
- ✓ SAP Audit Management
- ✓ SAP Business Integrity Screening
- ✓ SAP Regulation Management by Greenlight



Identity and Access Governance

- ✓ SAP Access Control
- ✓ SAP Cloud Identity Access Governance
- ✓ SAP Single Sign-On
- ✓ Identity Authentication (SAP Cloud Identity Services)
- ✓ SAP Identity Management
- ✓ Identity Provisioning (SAP Cloud Identity Services)
- ✓ SAP Access Violation Management by Greenlight
- ✓ SAP Dynamic Authorization Management by NextLabs

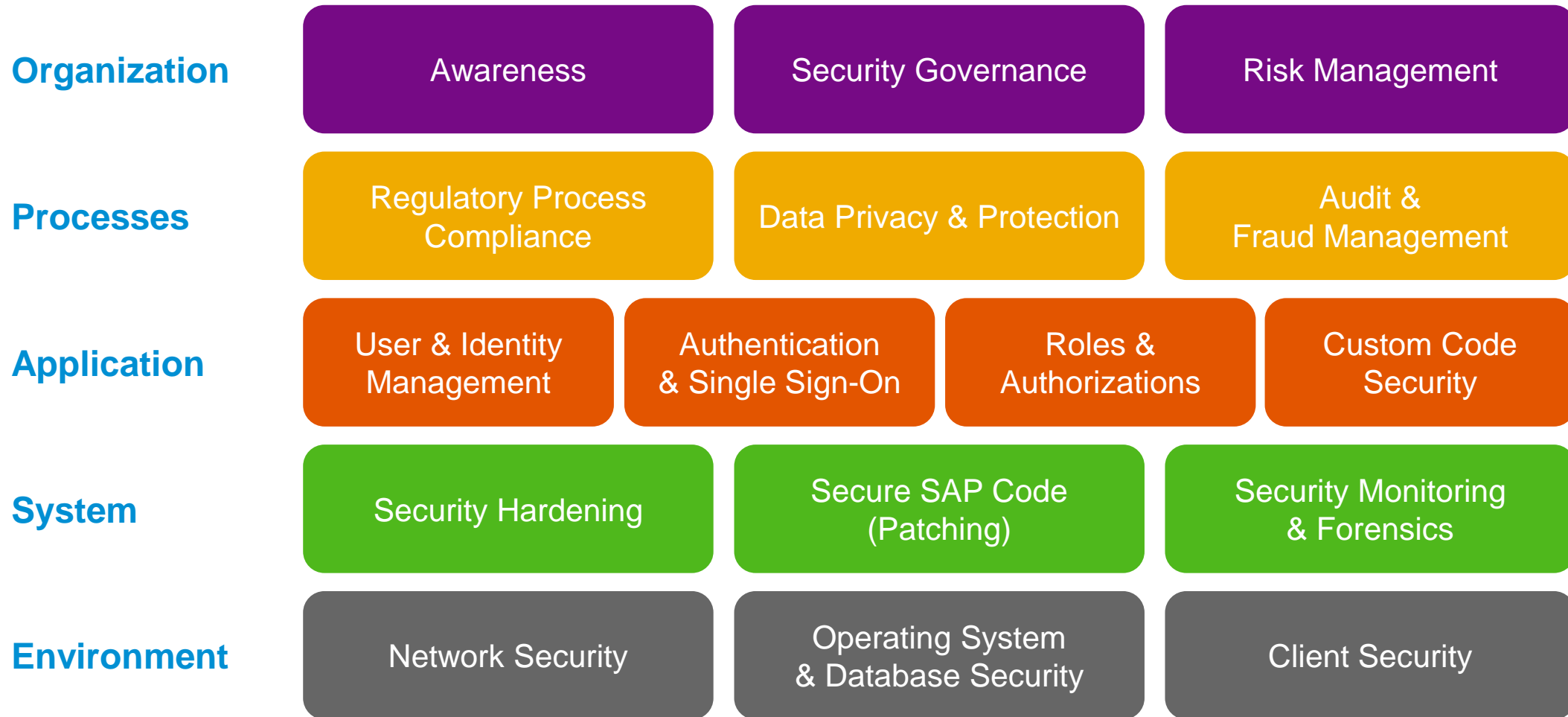


Cybersecurity, Data Protection and Privacy

- ✓ SAP Enterprise Threat Detection
- ✓ SAP Code Vulnerability Analyzer
- ✓ SAP Fortify by Micro Focus
- ✓ SAP Focused Run
- ✓ SAP Privacy Governance
- ✓ SAP Privacy Management by BigID
- ✓ UI data protection masking
- ✓ UI data protection logging
- ✓ SAP Data Custodian
- ✓ The Onapsis Platform for Cybersecurity

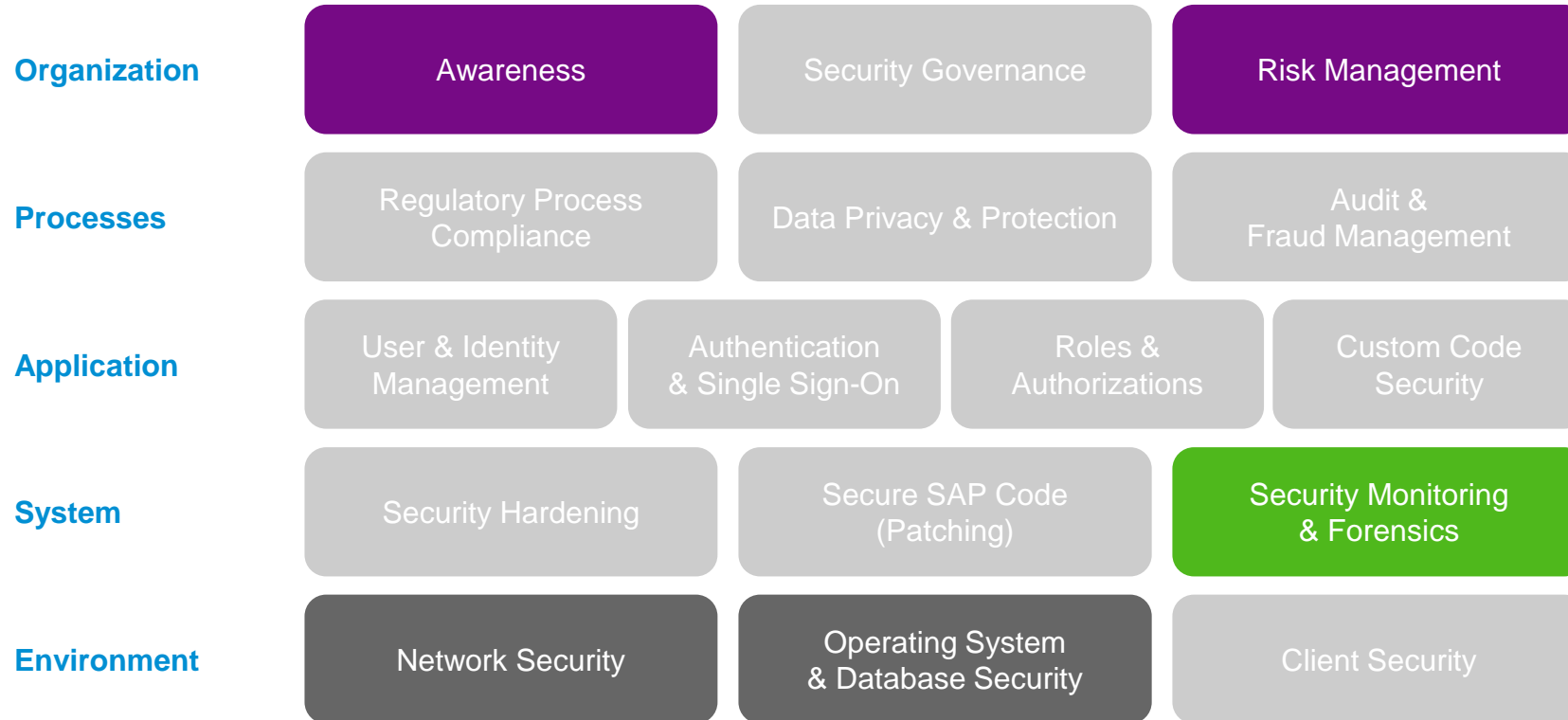
Secure Customer Operations: The Secure Operations Map

Full version available as a public [Customer Presentation](#)



Using the Secure Operations Map: Scenario Projections

Example A: Security Monitoring, Forensics & Threat Detection



Common Customer Questions



- How to **respond to security breaches** and mitigate any potential damage?
- How to minimize the performance and storage impact of **SAP Security Logs** and still have the information when needed?
- How to bridge the worlds of **traditional SIEM** (Security Information & Event Management) and enrich my threat intelligence with **SAP application-level logs**?

Using the Secure Operations Map: Scenario Projections

Example B: Access Risks & Segregation of Duties

Organization

Awareness

Security Governance

Risk Management

Processes

Regulatory Process
Compliance

Data Privacy & Protection

Audit &
Fraud Management

Application

User & Identity
Management

Authentication
& Single Sign-On

Roles &
Authorizations

Custom Code
Security

System

Security Hardening

Secure SAP Code
(Patching)

Security Monitoring
& Forensics

Environment

Network Security

Operating System
& Database Security

Client Security

Common Customer Questions



- How to reliably automate time-consuming **user management** tasks across multiple solutions and platforms (on-Premise, SaaS, PaaS)?
- How to enforce Segregation of Duties and **minimize risks** introduced by elevated privileges?
- What SAP features or solutions can be leveraged to achieve compliance with **Data Privacy** regulations?

Using the Secure Operations Map: Scenario Projections

Example C: Data Protection & Privacy

Organization

Awareness

Security Governance

Risk Management

Processes

Regulatory Process
Compliance

Data Privacy & Protection

Audit &
Fraud Management

Application

User & Identity
Management

Authentication
& Single Sign-On

Roles &
Authorizations

Custom Code
Security

System

Security Hardening

Secure SAP Code
(Patching)

Security Monitoring
& Forensics

Environment

Network Security

Operating System
& Database Security

Client Security

Common Customer Questions



- How to **reduce overhead** normally associated to multiple, often overlapping regulations?
- How to achieve advanced **data privacy capabilities** such as anonymization or read access logging?
- How to **harden** SAP systems and ensuring logging **retention timelines** meet the regulatory requirements?

Poll #2

Provide feedback using the “Polls” functionality on Zoom



Cyber Risks

Real-world examples and threat scenarios



Trends: Ransomware on the Rise

*“Serious cyberattacks in Europe **doubled in the past year**, new figures reveal, as criminals exploited the pandemic.”*

– Nick Paton Walsh, CNN

Article: <https://edition.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html>



Aluminium Manufacturing company, EMEA North

When: March 2019

Summary: Ransomware compromised OS and SAP applications running on them



Two Electric Utilities companies, EMEA North

When: April 2020

Summary: Ransomware (RagnarLocker) compromised OS and SAP applications running on them, likely spread from an unpatched VPN server

Cyberattacks During the COVID-19 Pandemic

Driving Factors



Remote Workforce

- Increased surface area due to unprotected Wi-Fi access points
- Lack of secure communication channels (VPN, DirectAccess)
- Unwarranted use of personal devices for business activities
- Increase public network traffic makes intrusion detection difficult



Stretched Resources

- IT/Security resources often faced with the decision to expose critical applications to the internet to ensure business continuity
- As resources are diverted to ensure business continuity, proactive/defensive security activities (e.g. patching, monitoring) are pushed to the side-lines
- Remote access channels experience high traffic and are particularly vulnerable to Denial of Service (DoS) attacks



Increased Attacker Motivation

- Opportunistic phishing and social engineering
- Public sector in the crosshairs: hospitals and electric utilities companies have been experiencing acute pressure from Cyberattackers. Attacks could sometimes have catastrophic results – such as shutting down essential services and forcing patients to be relocated at major healthcare facilities¹

¹ Cyberattack on Czech Hospital Forces Tech Shutdown During Coronavirus Outbreak

<https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak>

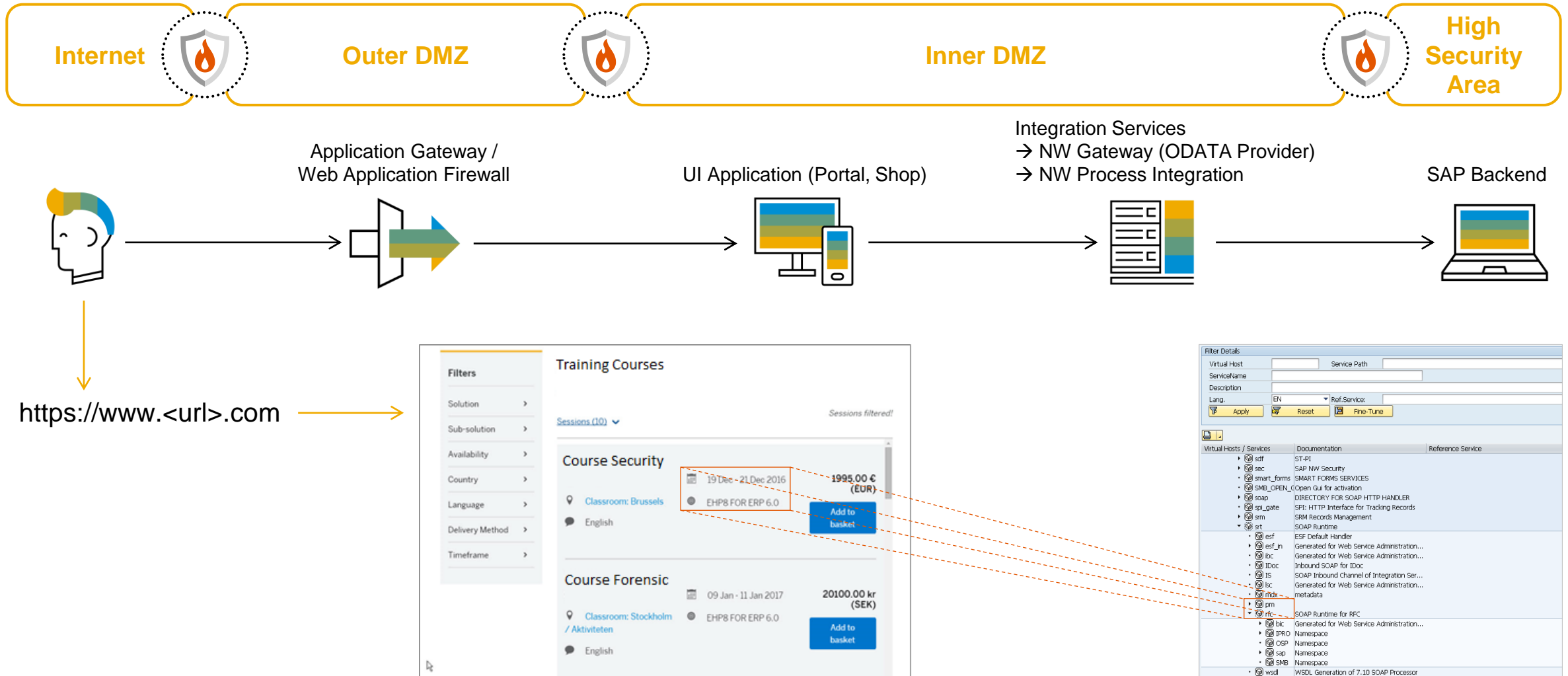
One story from real-life

- Customer identified that hackers have compromised the customer internal network to a large extent
- Customer identified that SAP NetWeaver system was used by attackers as one entry point
- SAP was contacted to support a forensic investigation
 - Gather details how SAP NetWeaver system has been compromised
 - Gather details about attack timeline
 - Derive Indicators of Compromise (IoC)
 - Analyze if other parts of the SAP customer landscapes have been compromised, too



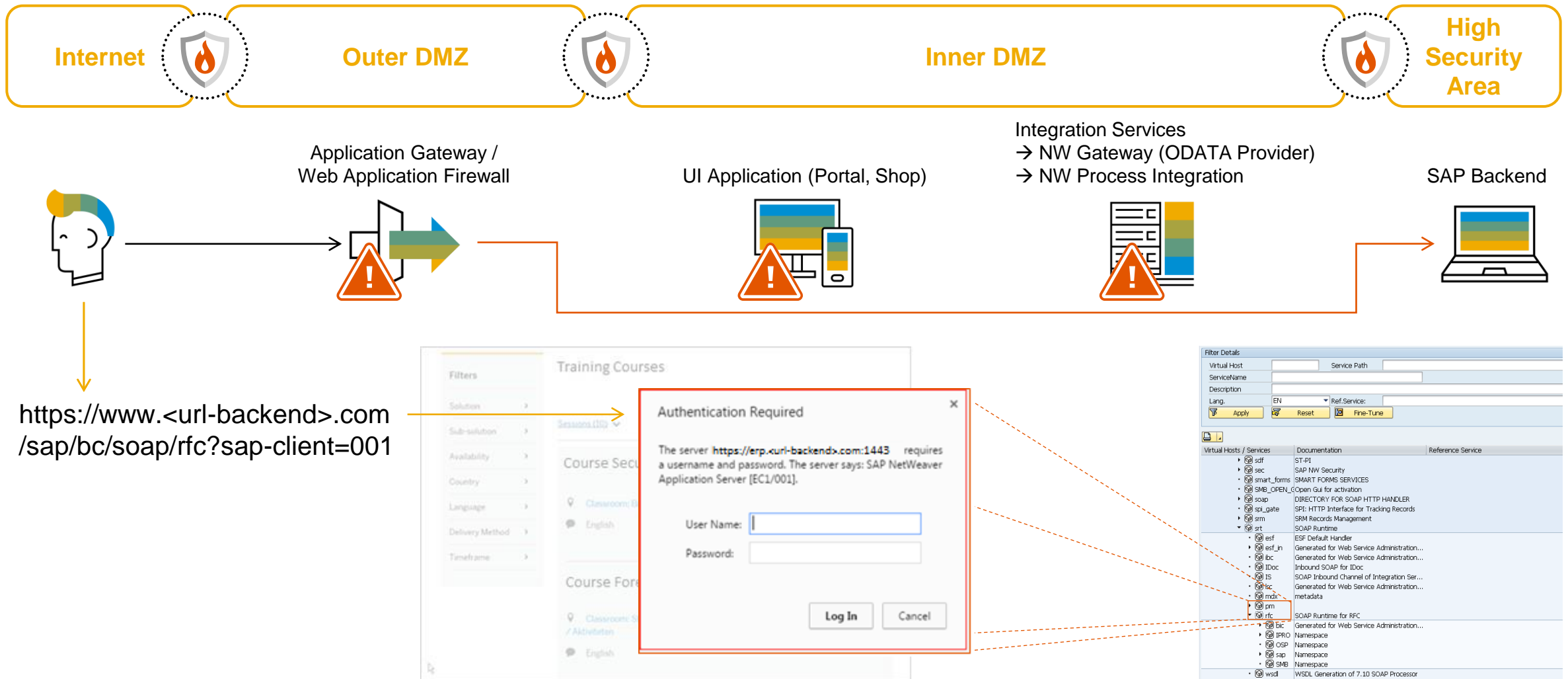
One story from real-life

Landscape Architecture



One story from real-life

What went wrong?



One story from real-life

What went wrong?

In most companies,

- frontend application designers / portal operations
- backend (SAP) operators
- and network security

are in entirely **different teams**.



Communication failures happen frequently such as:

- portal operations assumes that direct URLs will be rewritten / blocked by WAF (network security)
- network security does not know which access type to block (e.g. watch for “sap-client=000”)
- SAP operations are not aware that their system is exposed at all.



If SAP operations then (assuming they are not exposed) think it is not really dangerous to have

- **critical ICF services** active
- SAP standard users still up and running, even with **default passwords**,

(Even with passwords reset, anyone could easily halt the transport system by locking TMSADM)

One story from real-life

Results of the forensic investigation that can be shared

Details on the attacked SAP system

- Attacks on Internet-facing SAP NetWeaver system were running at least for 1 year
- Information / fixes for exploited SAP vulnerabilities were published 5 years ago. Details how to exploit vulnerabilities are available publicly for several years.
- Tools for remote code execution were installed and hidden as SAP components. Attackers had full access to the vulnerable SAP NetWeaver system
- Attackers had substantial knowledge on SAP NetWeaver technology

Lateral Movement to other SAP systems

- It was not possible to proof that other SAP systems of the customer landscapes were attacked due to
 - **weak SAP security configuration** of the whole SAP landscape
 - **inactive** SAP logs



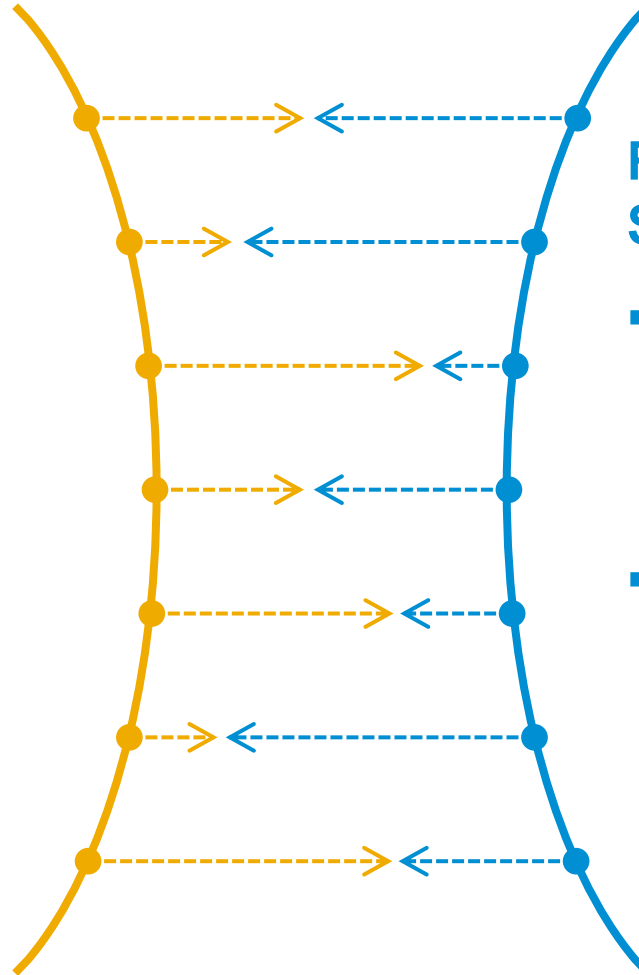
One story from real-life

Business impact vs forensic analysis



Business Impact of the attacked SAP system

- SAP system was removed from the Internet immediately after attacks were identified
- Backups were not available to restore SAP system before first successful attacks
- SAP system was not available for **several weeks**



Re-attach SAP system to Internet



- SAP recommended to re-build system from scratch as hints were found that attackers were able to modify additional parts of the system
- **Customer business decision:**
 - SAP system was re-attached to the Internet with manual removal of infected parts
 - Unknown if attacker manipulated other parts of the SAP system

Poll #3

Provide feedback using the “Polls” functionality on Zoom

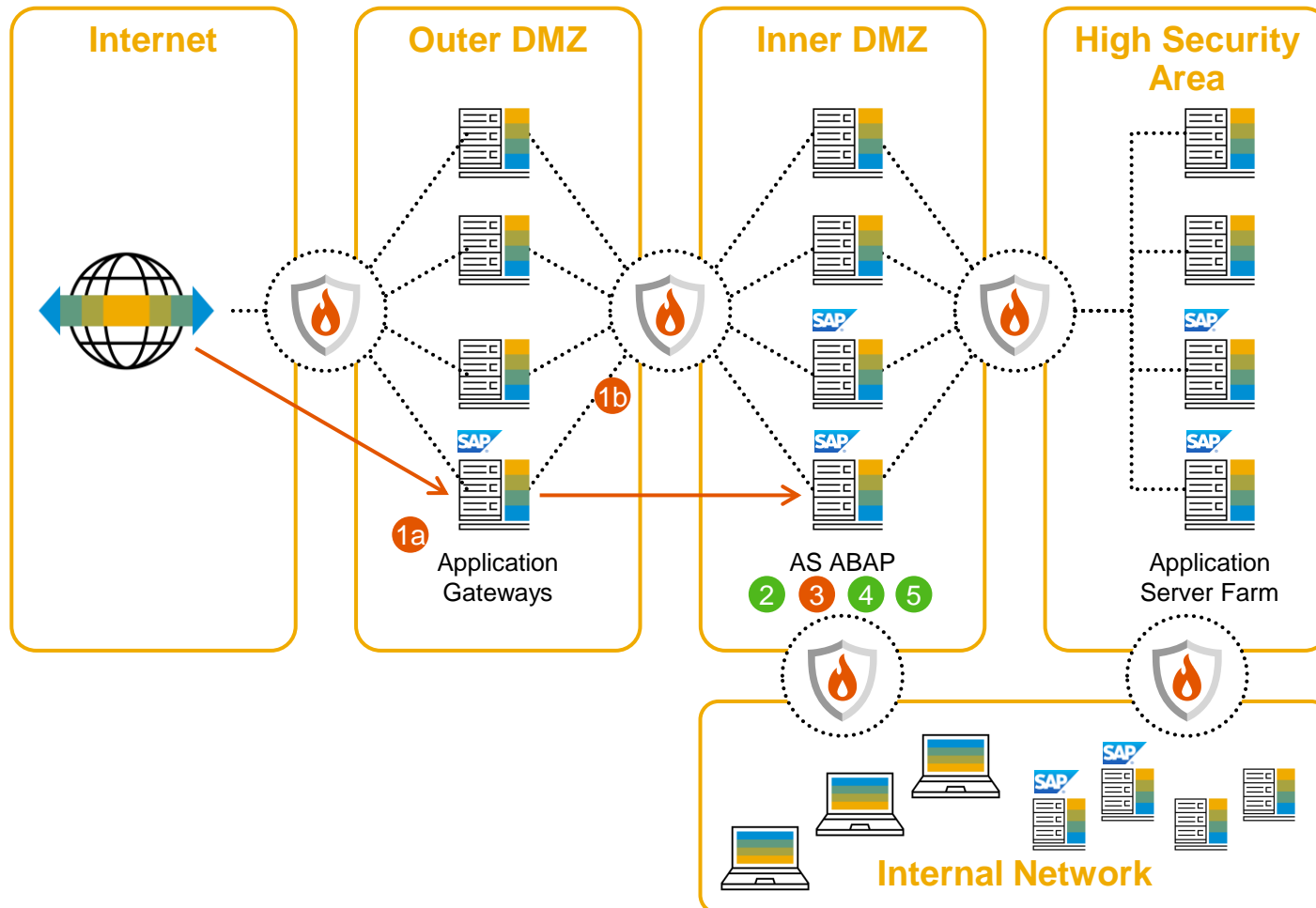


Risk Scenario:

Security Monitoring & Threat Detection



Internet Scenarios with SAP NetWeaver



- 1a SAP Web Dispatcher HTTP Log
- 1b SAP ICM HTTP Log
- 2 System Log
- 3 Security Audit Log
- 4 Business Transaction Log / Workload Analysis
- 5 User Change Log

Security Logging Main Log Providers

On-Premise and Cloud

	SAP Cloud						
SCP	S/4 HANA Cloud Edition	S/4 HANA Private Cloud Edition	Sales Cloud	SF	Ariba		
Audit Log			Audit Log	Change Audit Reports	BuyerNodeLog		
Application Log					Configuration Log		
					J2EE Setup Log		
Security Audit Log							
Database Change Log							
HTTP Server/Client Log							
Business Transaction Log	SOAP Web Service Log						
Gateway Log	UI Logging	Security Audit Log		Debug Log			
User Change Log	Read Access Log	Security Log		Change Log			
Change Documents	System Log	HTTP Access Log	Audit Trail	Audit Log Inbound Traffic	ICM Logs	Audit Log	Connectivity Log
S/4 HANA & ABAP Based Systems		JAVA Systems	HANA	Cloud Connector	Web Dispatcher	Host Agent	SAPRouter
	SAP OnPrem Systems						

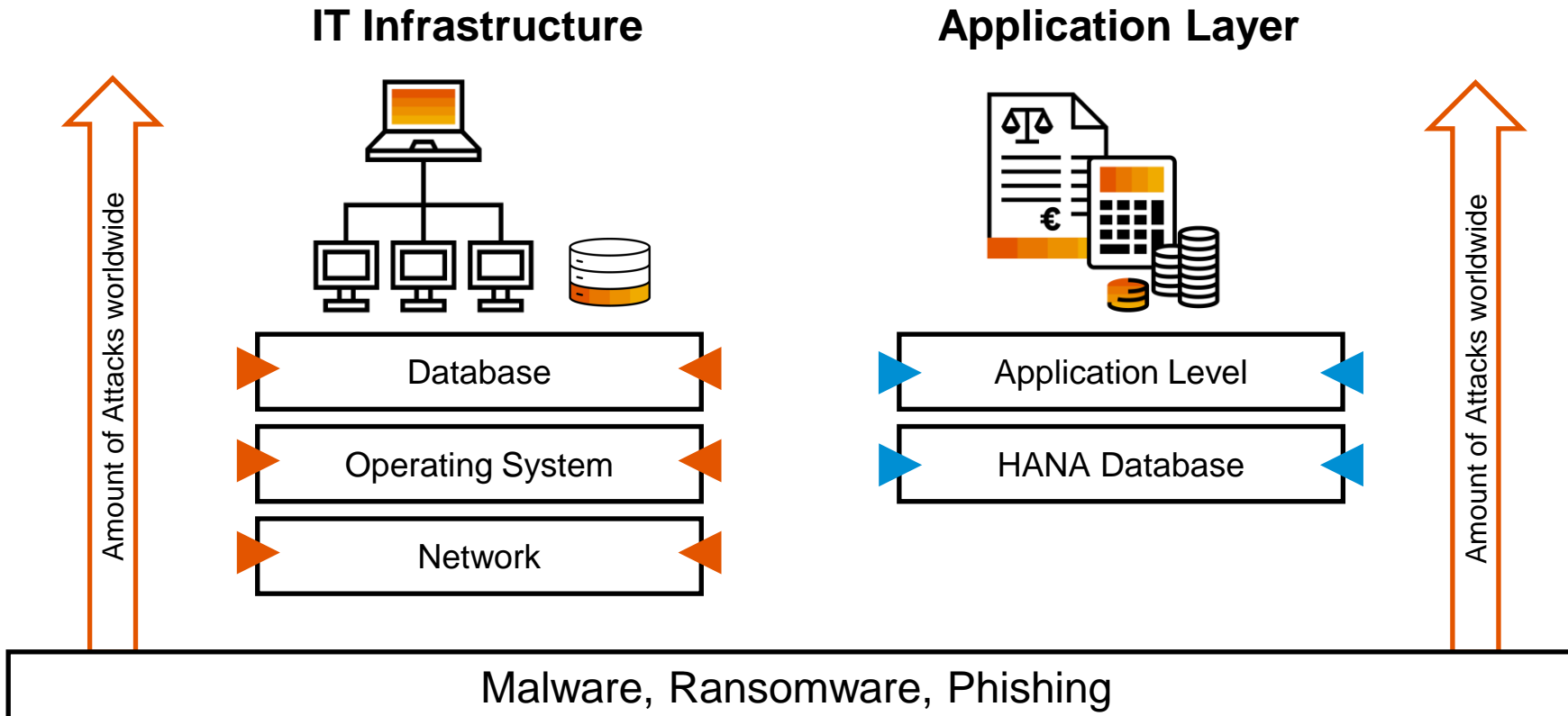
Input required to provide good, reliable facts

Important steps to make sure you have what you need when you need it

A. Accuracy ————— B. Existence ————— C. Centralization

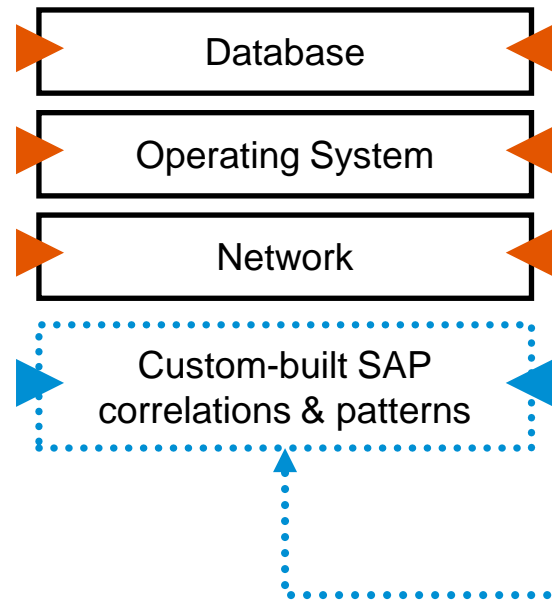
- Make sure all **TIMESTAMPS** match, throughout your entire IT infrastructure, including switches, routers...
 - Set everything to UTC if possible. Sync properly – a mismatch by several seconds may lead to inconsistent views.
- **REASONABLE** switch on logging of security events for critical parts of your IT infrastructure. Don't stop at switches, routers, operating systems, databases etc.
- **CENTRALIZE LOGS** to a safe place if possible – as fast as possible.
 - Get alerted if local logs are deleted or switched off.
 - Enable integrity protection mechanisms wherever available.

SIEM Operations Today

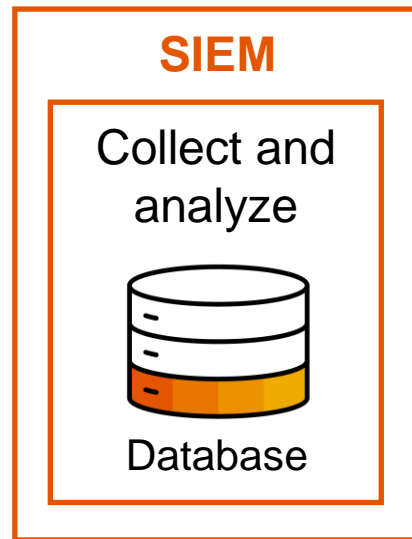


Challenges of Single SIEM

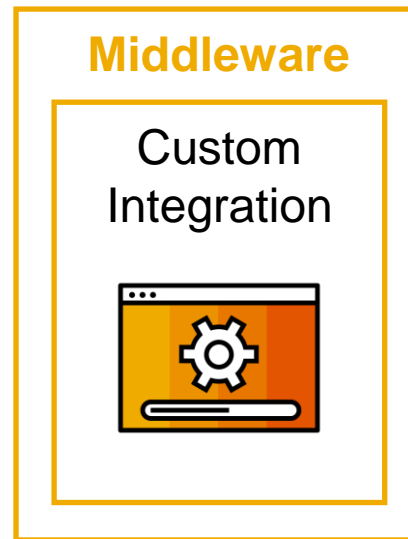
SIEM solutions focus on



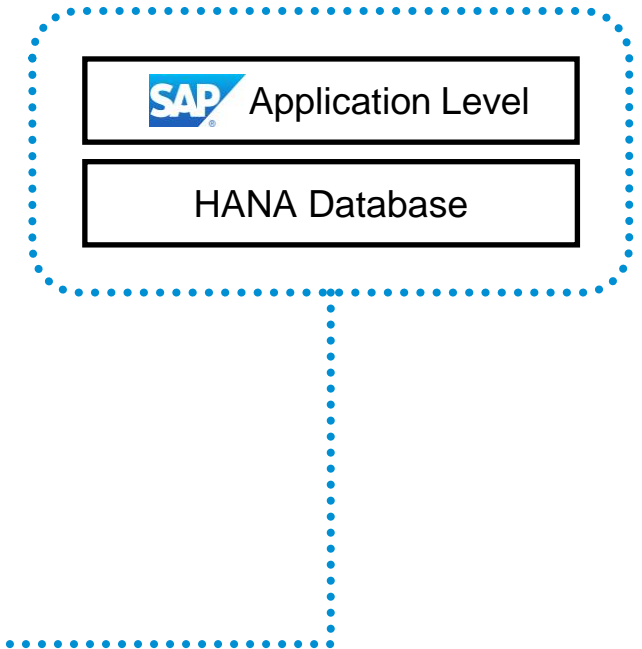
IT Infrastructure



Integration Layer

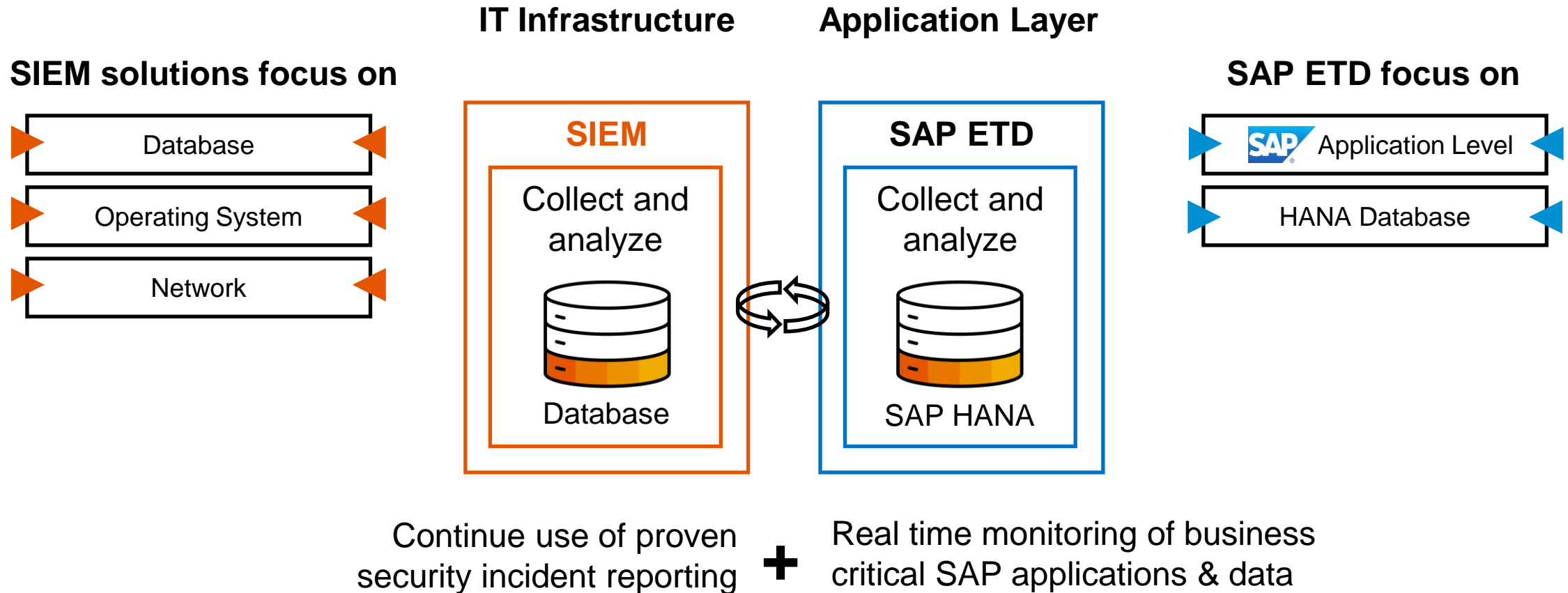


Application Layer



Not only **integration** must be built to parse SAP logs, but **content** must also be developed from scratch

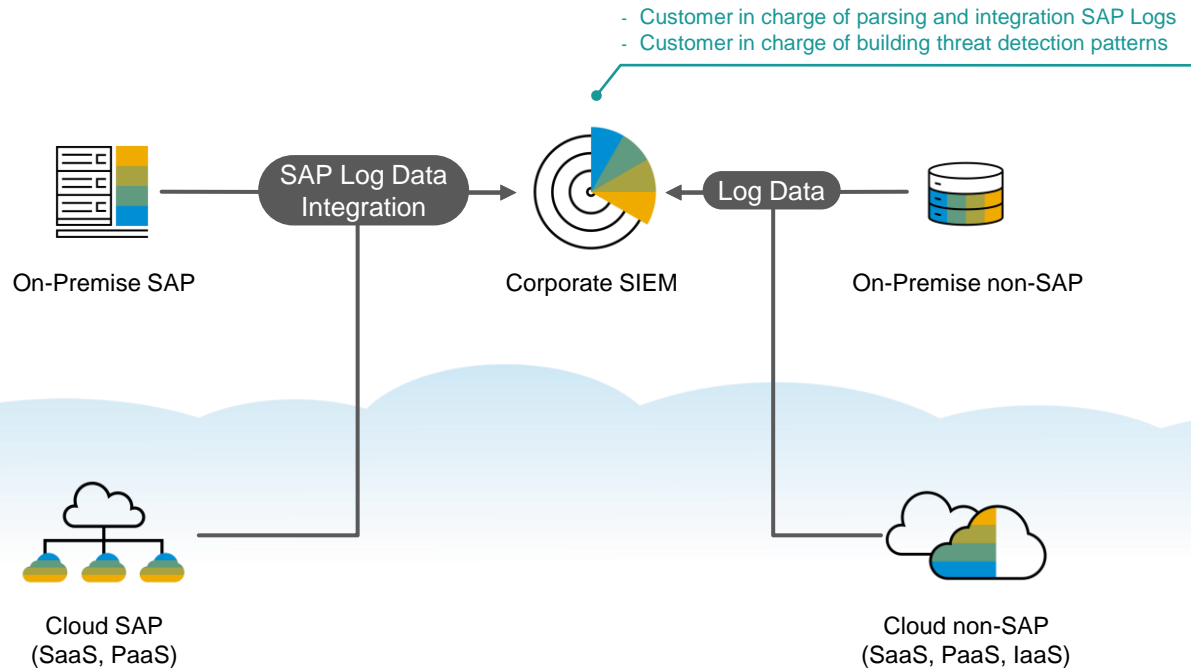
SAP Enterprise Threat Detection (ETD) and generic SIEM systems



Integration of SAP ETD with all leading SIEM solutions (HP Arcsight, IBM QRadar, Splunk) available

SIEM Architecture A

Single SIEM



Pros:

- + Reduced licensing and maintenance costs
- + Direct integration scenario and simplified architecture

Cons:

- Customer is in charge of integrating, parsing and normalizing SAP Logs
- Content (i.e. threat detection patterns) must be created from scratch – which could be challenging, even if attempting to reverse-engineer ETD content.

SIEM Architecture B

Integrated ETD (On-premise)

- Alert publishing to SIEM in JSON or LEEF format
- Latest SAP detection patterns delivered as out-of-the-box content
- Normalization and compression of SAP logs
- High-availability

- Centralized SIEM solution
- Increased reach: full visibility into SAP events and alerts



Pros:

- + Native integration and ready-to-use content provide an accelerated start
- + Content can be kept up-to-date with latest SAP-native threats, vulnerabilities and trends
- + JSON/LEEF integration ensures corporate SIEM is the single source of truth, enriched by SAP-specific alerts

Cons:

- Increased licensing and maintenance costs
- Complexified technical architecture

Possible Operating Models for ETD:



SIEM Architecture C

Cloud ETD (SIEM-as-a-Service)



- Cloud Deployment
- Latest SAP detection patterns delivered as out-of-the-box content

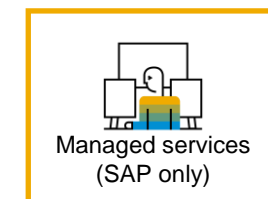
Pros:

- + Cloud deployment only requires technical integration to be made at managed system level
- + SAP-operated Managed Services allow true “SIEM-as-a-Service” experience with fixed price offerings

Cons:

- No alert integration to SIEM possible at present
- No customer-operated or partner-operated managed services possible – only SAP operators can provide SIEM operations “as a service” for the moment

Possible Operating Models for ETD:



SIEM Architecture C

Cloud ETD

- Extended service
- Committed response times
 - Individual adapted security analysis
 - Customized service level agreements

- Base service
- ✓ 24x7 monitoring of your SAP software environment
 - ✓ Checking for ~60 standard attack path patterns
 - ✓ Risk-based and prioritized alerting
 - ✓ Monthly reporting of all incidents and all log data

German data center*

Service provision within the European Union

Language: English

* Other data centers are in discussion.



Enterprise Threat
Detection, Cloud Edition

Top Tips: Monitoring & Threat Detection

Key factors for intelligent cybersecurity operations

Logging

- Ensure all recommended logs are turned on, set to a unified time zone and always available for consumption
- Establish log retention policies. Free up storage by archiving or erasing logfiles as needed.

SIEM

- Expand coverage of your SIEM to detect attack patterns in SAP applications. This can be achieved through integration or SAP's own Enterprise Threat Detection solution

Organizational

- SAP Security expertise and solid understanding and adoption of Cybersecurity frameworks and standards (e.g. NIST Cybersecurity Framework, ISO/IEC, OWASP).





Getting there with Premium Engagements

Services for Logging & Forensics

- Understand the basics of Logging and SIEM Architecture options with an **Empowering Session**;
- Plan your architecture transformation via a **Planning Session for Logging & Forensics**;
- Request a **Proof of Concept Implementation** of Enterprise Threat Detection;
- Have SAP safeguard your Productive implementation via the **Security Architect** engagement model.

Poll #4

Provide feedback using the “Polls” functionality on Zoom

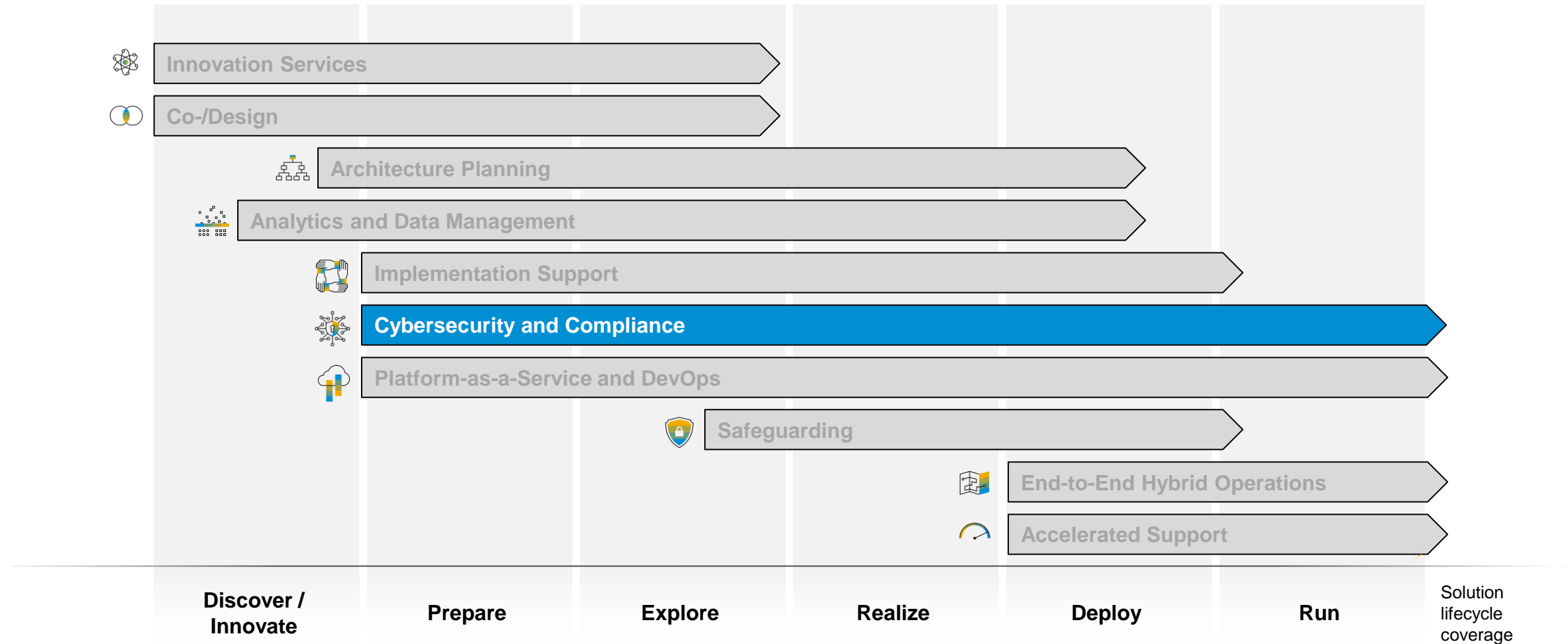


Securing Your **SAP Environment**

SAP Premium Engagements Offerings

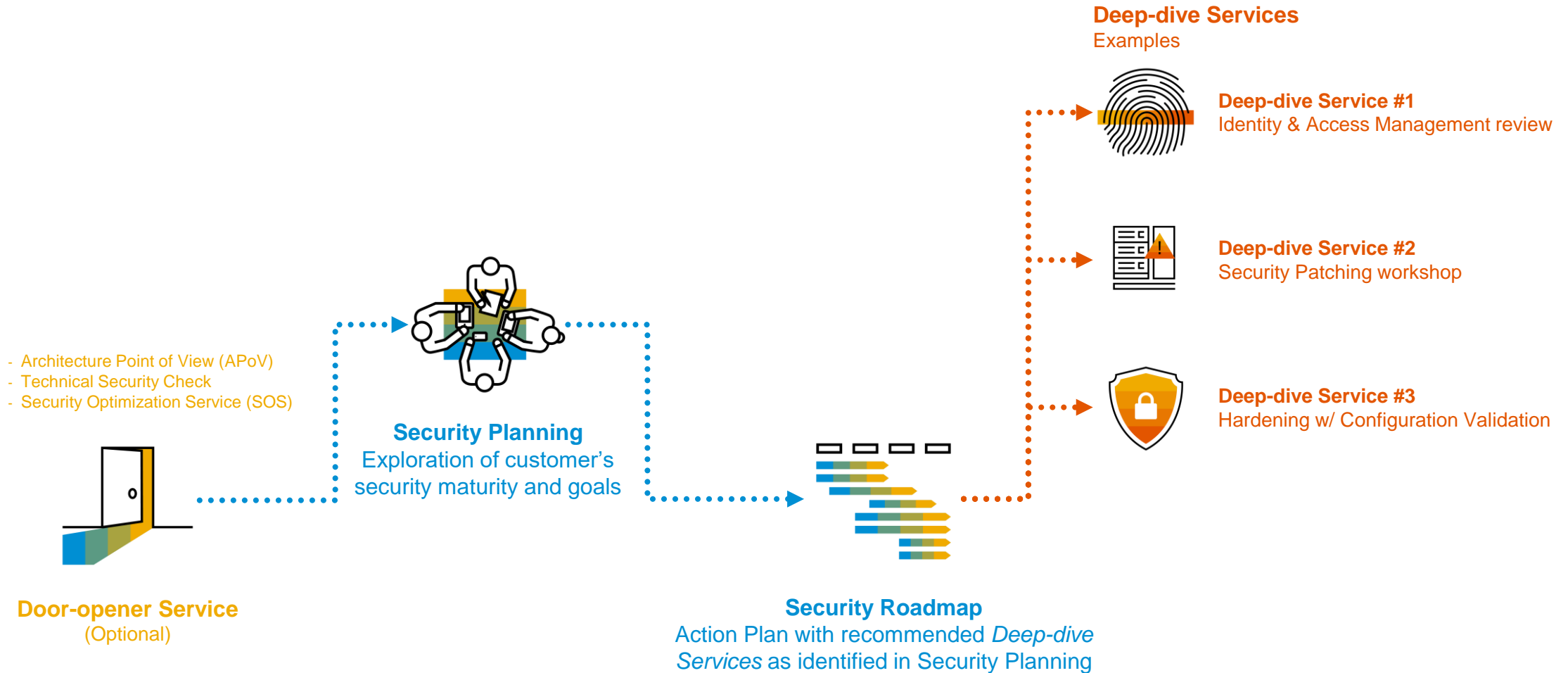


Cybersecurity and Compliance

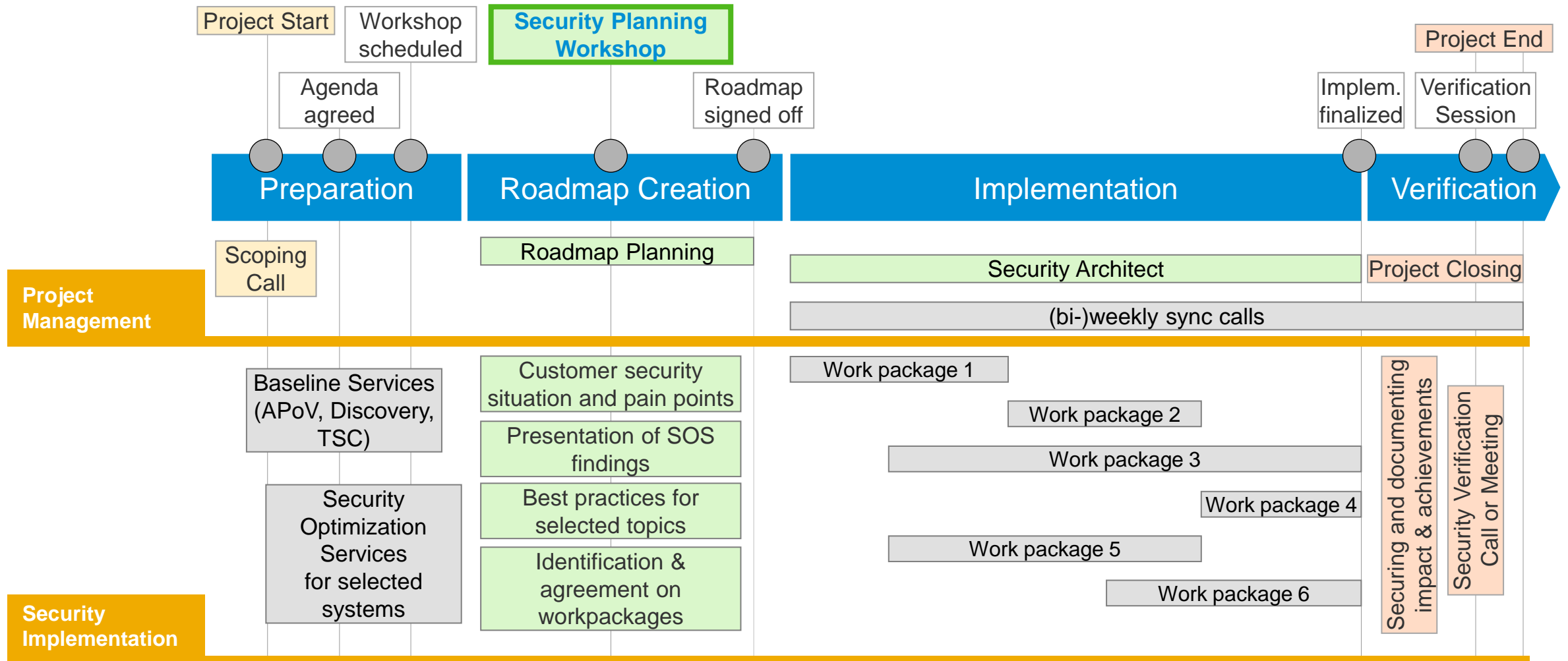


Cybersecurity & Compliance: Service Flow

(Simplified view)



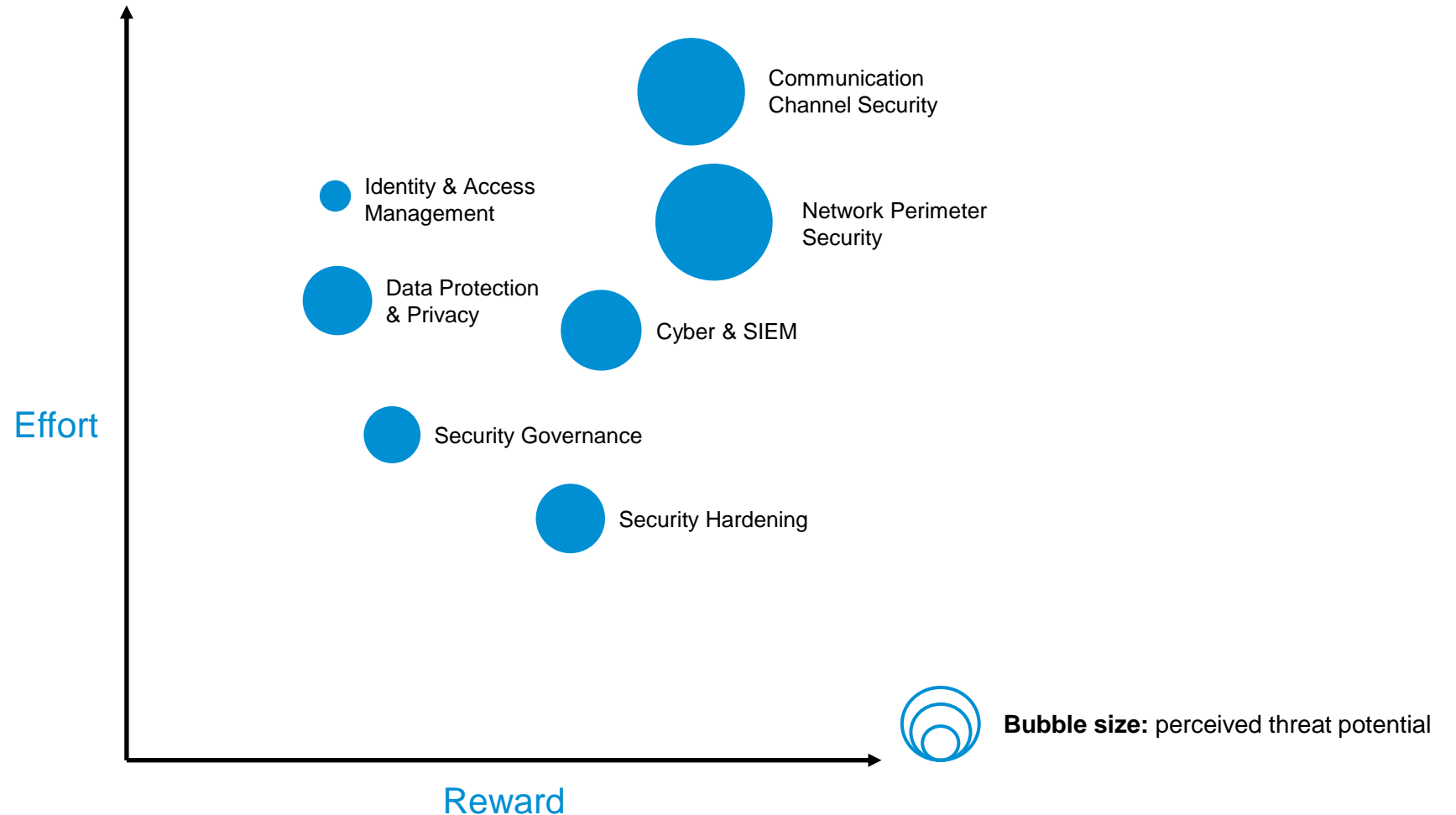
Sample Roadmap: Security & Compliance Workshop



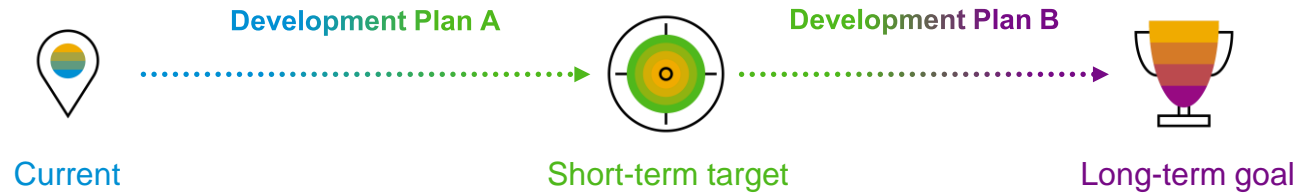
Planning: Prioritization of Work Packages

Contextual factors

- Due to nature of the industry, sensitive data is constantly flowing through;
- Some of the teams are newly acquainted to SAP security;
- Multiple SAP applications exposed to the internet.

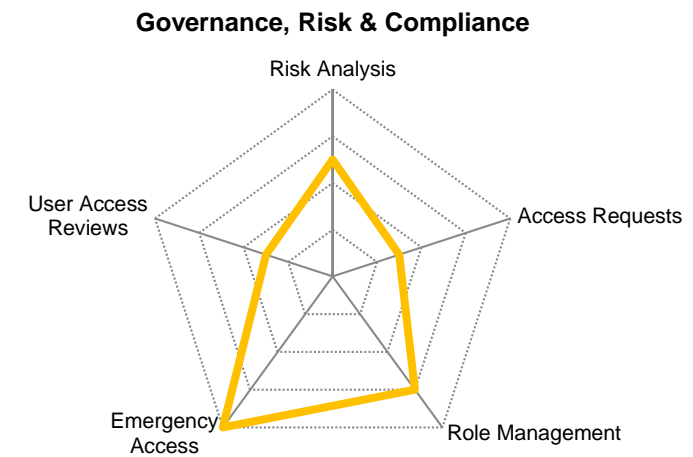
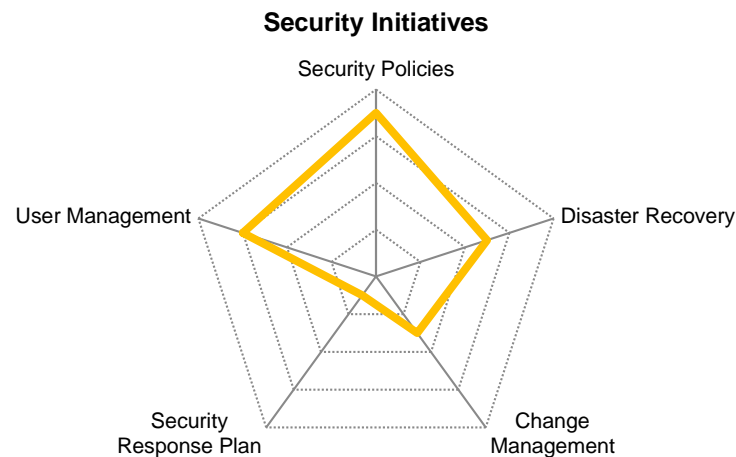


Establishing Success Criteria: Security Maturity Spectrum



	1: Initial	2: Realized	3: Controlled	4: Optimized
Processes	<ul style="list-style-type: none"> No security processes defined No user and authorization setup process No impact and risk analysis of business processes 	<ul style="list-style-type: none"> Main security processes defined First business critical processes identified Process for setting up users and authorizations available 	<ul style="list-style-type: none"> Security processes fully implemented Business critical processes analyzed and risk mitigation defined 	<ul style="list-style-type: none"> ISO 2700x conform ISMS Uniform, corporation-wide security processes on all levels Complete continuity mgmt for all business critical processes

Example outputs:



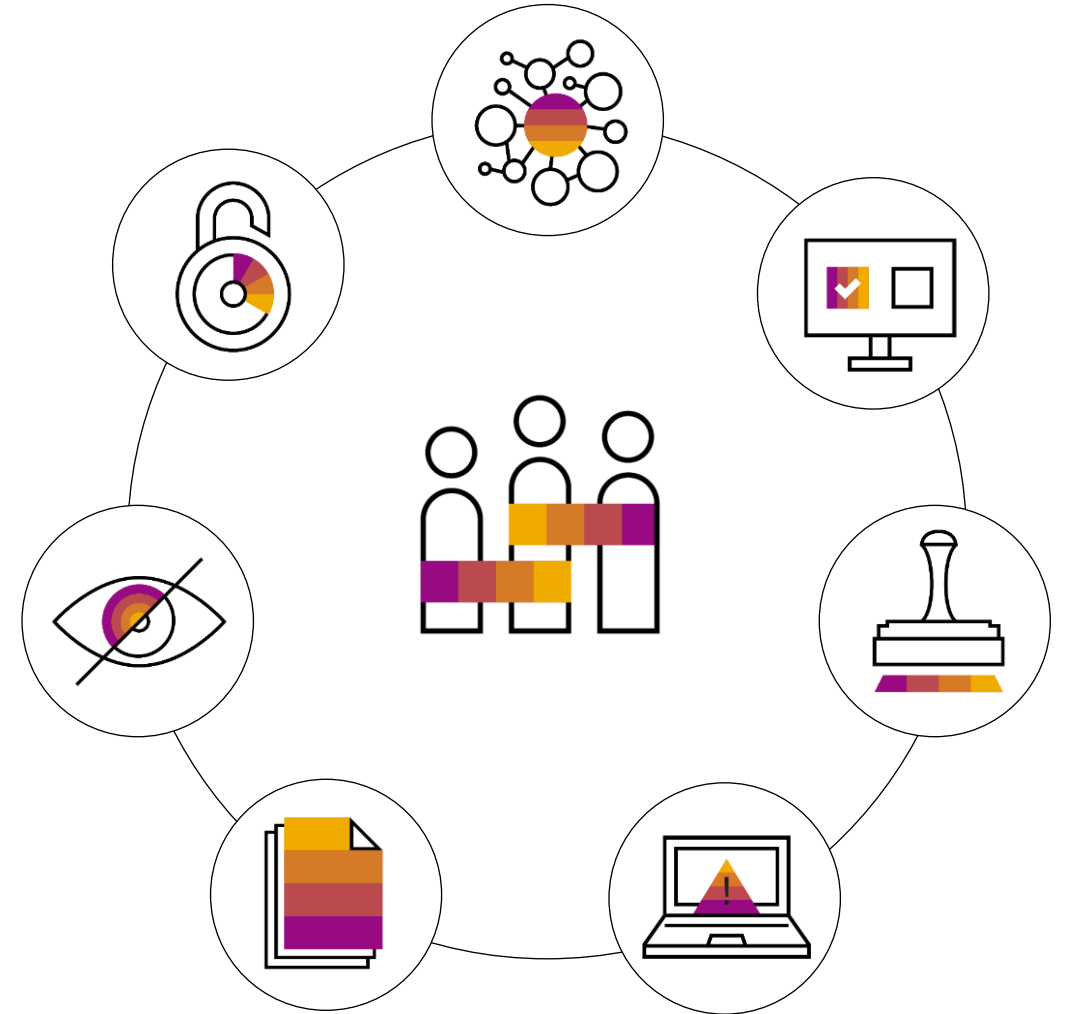
Risk Scenario:

Access Risks & Segregation of Duties



Why is managing access so hard?

- Increasing number and complexity of enterprise applications
- Different types of authorization models (Cloud, On-premise)
- Key requirement for many regulations
- Fragmented approach to managing access risk
- Manual administrative processes
- Lack of visibility into user access and access risk
- Inability to prevent access risk violations



Access management – critical elements

Ensure right access at right time to right person

- Enable business users to perform needed functions

Meet regulatory needs

- Analyze access and establish required control
- Simplify the process of getting the right access

Optimize roles to ensure security, privacy, business functionality, and ease of maintenance

Manage privileged access

Provide transparent auditability of who got what, when, and why



SAP Security Software: The GRC Solution Portfolio

Identity & Access Governance



Enterprise Risk and Compliance

- ✓ SAP Risk Management
- ✓ SAP Process Control
- ✓ SAP Audit Management
- ✓ SAP Business Integrity Screening
- ✓ SAP Regulation Management by Greenlight



Identity and Access Governance

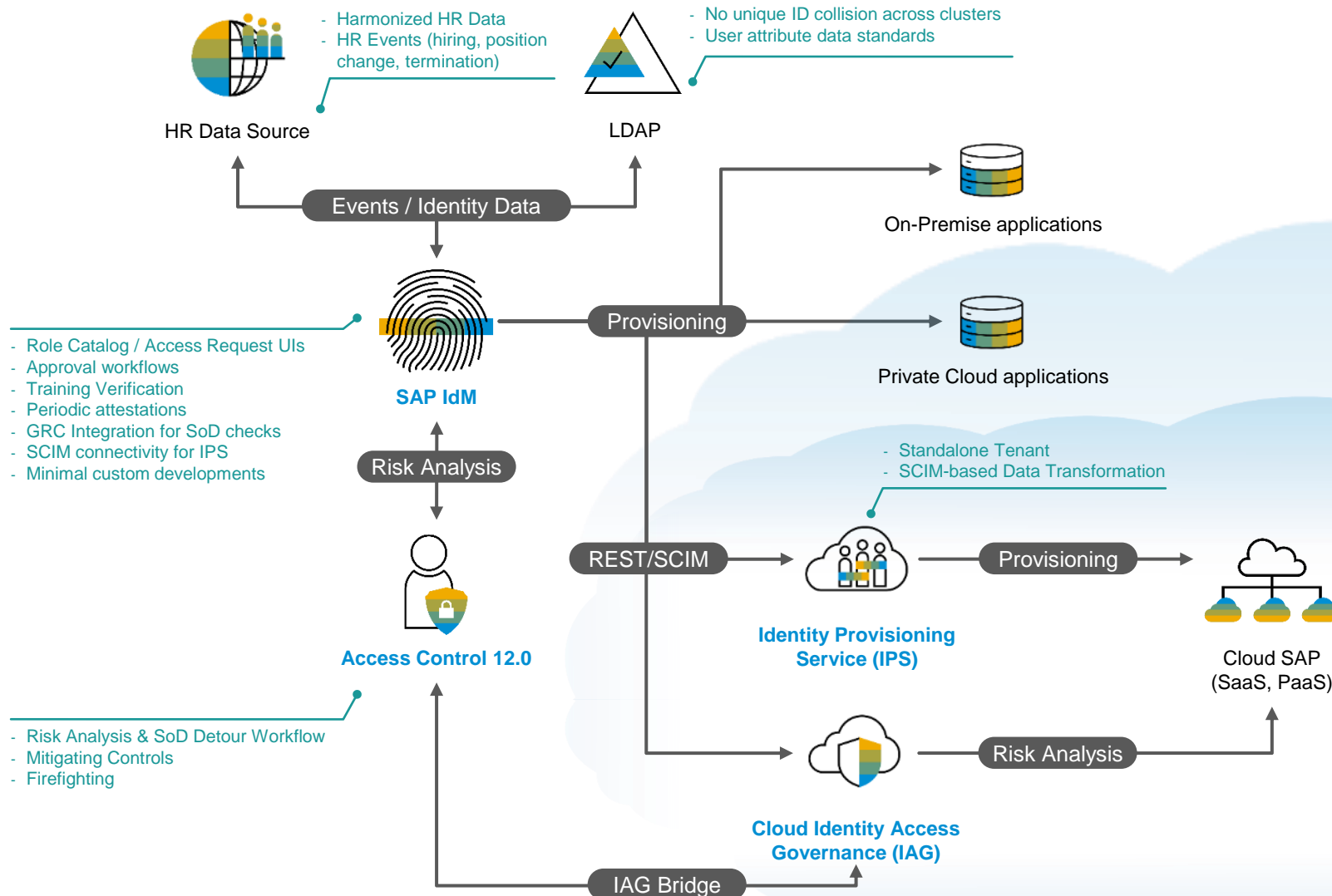
- ✓ SAP Access Control
- ✓ SAP Cloud Identity Access Governance
- ✓ SAP Single Sign-On
- ✓ Identity Authentication (SAP Cloud Identity Services)
- ✓ SAP Identity Management
- ✓ Identity Provisioning (SAP Cloud Identity Services)
- ✓ SAP Access Violation Management by Greenlight
- ✓ SAP Dynamic Authorization Management by NextLabs



Cybersecurity, Data Protection and Privacy

- ✓ SAP Enterprise Threat Detection
- ✓ SAP Code Vulnerability Analyzer
- ✓ SAP Fortify by Micro Focus
- ✓ SAP Focused Run
- ✓ SAP Privacy Governance
- ✓ SAP Privacy Management by BigID
- ✓ UI data protection masking
- ✓ UI data protection logging
- ✓ SAP Data Custodian
- ✓ The Onapsis Platform for Cybersecurity

IAM Architecture A: Hybrid & Compliant IAM



Top Tips: Identity & Access Management

Key factors for successful IAM implementations / transformations

Identity Management

- High-quality, harmonized data sources (e.g. LDAP, HR systems)
- Well-documented, intuitive Access Request procedures

Access Risk Analysis

- Uncompromising design of Access Risk Ruleset, tailored to specific industries, products and Board risk appetite
- Real-time access risk reporting and comprehensive audit trails

Organizational

- Clear-cut, universally adopted IAM policies
- Strong buy-in from stakeholders and senior leadership





Getting there with Premium Engagements

Services for Identity & Access Management

- Discover value-added reference architectures via an **Architecture Point of View** service;
- Dive deeper and plan your idealized, end-to-end, Hybrid Identity Lifecycle via **IAM Planning Workshop**;
- Discover the complete feature set of your IAM Products via **Proof of Concept** implementation services;
- Have SAP safeguard the Productive implementation of your IAM landscape via the **Security Architect** engagement model.

Poll #5

Provide feedback using the “Polls” functionality on Zoom



Risk Scenario:

Data Protection & Privacy



The impact of risk management and regulatory demands

Example: Compliance laws all over the world

Risk & fraud management

Spot opportunities, track hazards, unveil cheaters

Tax & trade compliance

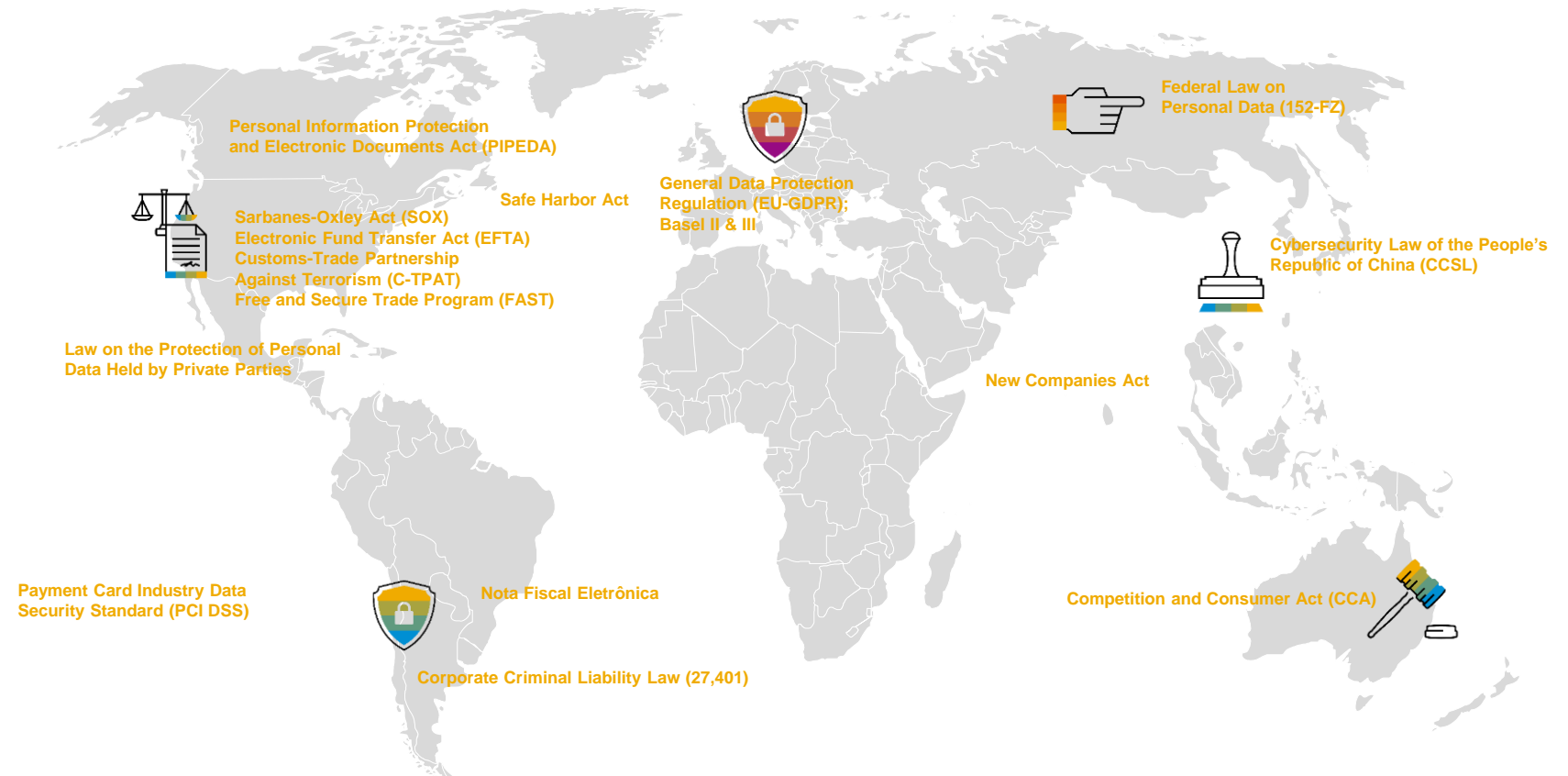
Different laws in each country

Audit management

Address requests quickly and continuously

Internal control system

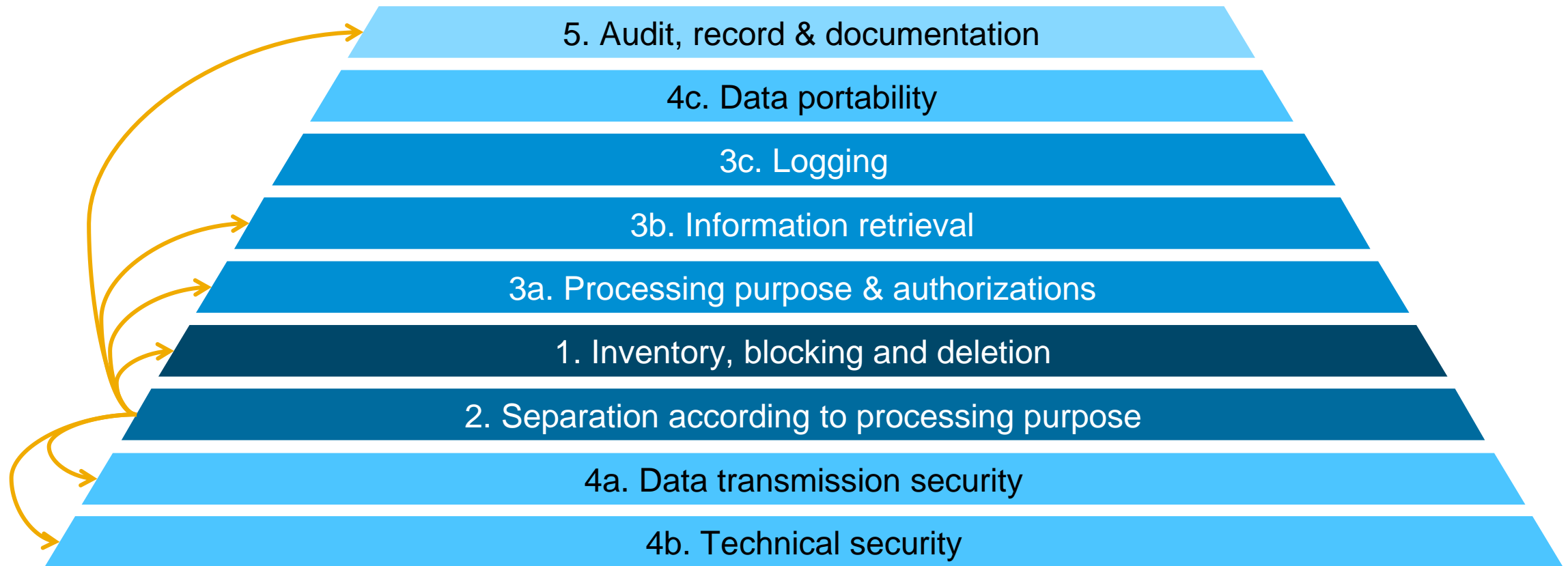
Mandatory in a variety of jurisdictions



“Results would indicate that companies are overly focusing on current risks instead of taking a proactive approach to new risks coming to the fore” (Accenture 2018)

Data Privacy within SAP Business Suite & S/4 HANA

Procedure model for the inductive approach



Source: Rheinwerk Verlag: Lehnert, V. et.al.; *Datenschutz in SAP Business Suite und S/4HANA*; publication date 12 2017.

Data Privacy within SAP Business Suite & S/4 HANA

Technical & Organizational Measures (TOMs)



Physical Access Control

Prevent unauthorized access to premises in which personal data is processed or used.



Authentication

Secure procedures to enable system access based on personal authentication.



Authorization

Procedures allowing the differentiation of which data can be accessed and in which mode.



Disclosure Control

Ability to document all access to personal data.



Change Control

Ability to document all changes to personal data.



Transmission Control

Procedures and safeguards for the transmission of personal data, such as encryption during transmission.



Job Control

Data Controller must ensure that the data processor is following instructions and guidelines.



Availability Control

Business continuity mechanisms such as backup, database replication and disaster recovery.

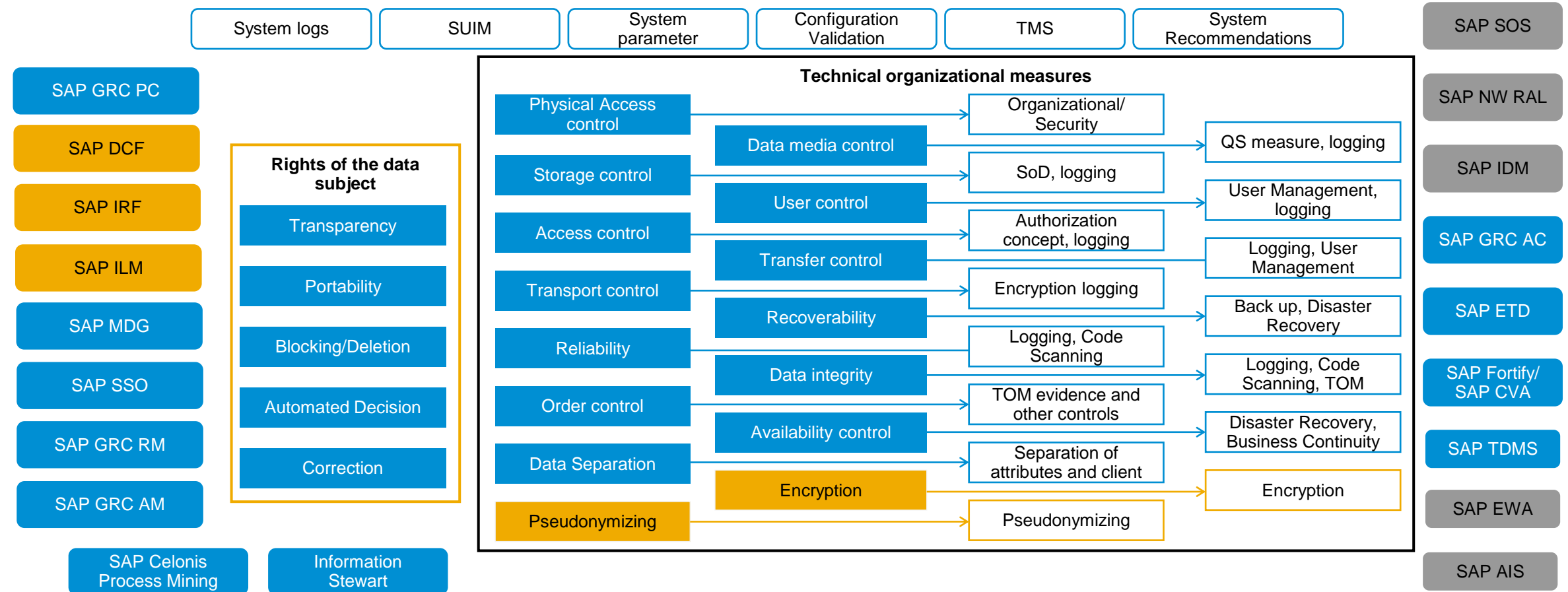


Data Separation

Personal data collected for a specified purpose must be separated from the same data gathered for other purposes.

3. Data Privacy within SAP Business Suite & S/4 HANA

Technical implementation of the procedure model



Source: Rheinwerk Verlag: Lehnert, V. et.al.; *Datenschutz in SAP Business Suite und S/4HANA*; publication date 12 2017.

Top Tips: Data Protection & Privacy

Achieving DP&P maturity and regulatory compliance

Organizational

- Legal, DP&P and business teams are vital for defining scope, legality and requirements to be fulfilled
- Data Privacy assessments and data inventory are essential for defining toolset, practices and governance
- Building new information systems with DP&P in mind is much easier than introducing DP&P capabilities in a system that's already live

Toolset

- Means to an end: not every customer will need every DP&P product in the line-up – these should be picked based on a solid business case and be indispensable for meeting DP&P requirements.





Getting there with Premium Engagements

Services for Data Protection & Privacy

- Discover the full range of SAP's Data Privacy solutions via **Architecture Point of View** service;
- Cover the basics on your ERP systems with a **GDPR Technical Basic Check**;
- Discover our **extended Data Privacy portfolio** with SAP Professional Services.

Poll #6

Provide feedback using the “Polls” functionality on Zoom



Wrapping Up:

Key Messages





Wrapping Up

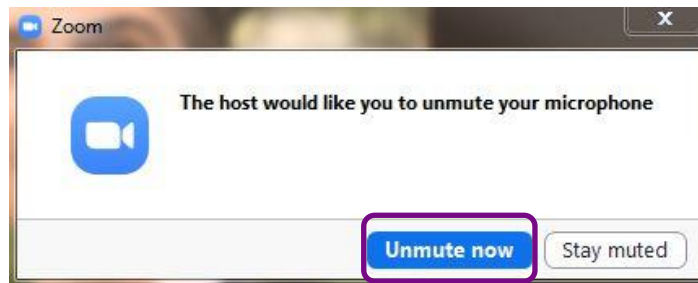
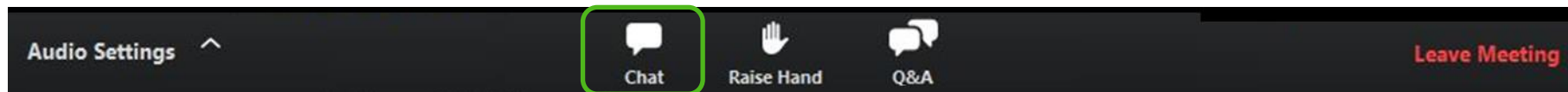
Key Messages

- SAP provides **products and solutions** for robust Cybersecurity on Cloud, On-premise and Hybrid environments;
- SAP also offers **Premium Services** for customers who wish to innovate with confidence on the topic of Cybersecurity & Compliance;
- You can **learn more** about product and service offerings available by contacting your SAP Technical Quality Manager (TQM).



Questions & Answers

Use the Zoom **Chat functionality** or **unmute**



Thank you.

Contact information:

CoE Cybersecurity & Compliance – Dublin, Ireland
securitydeliverycoedublin@sap.com