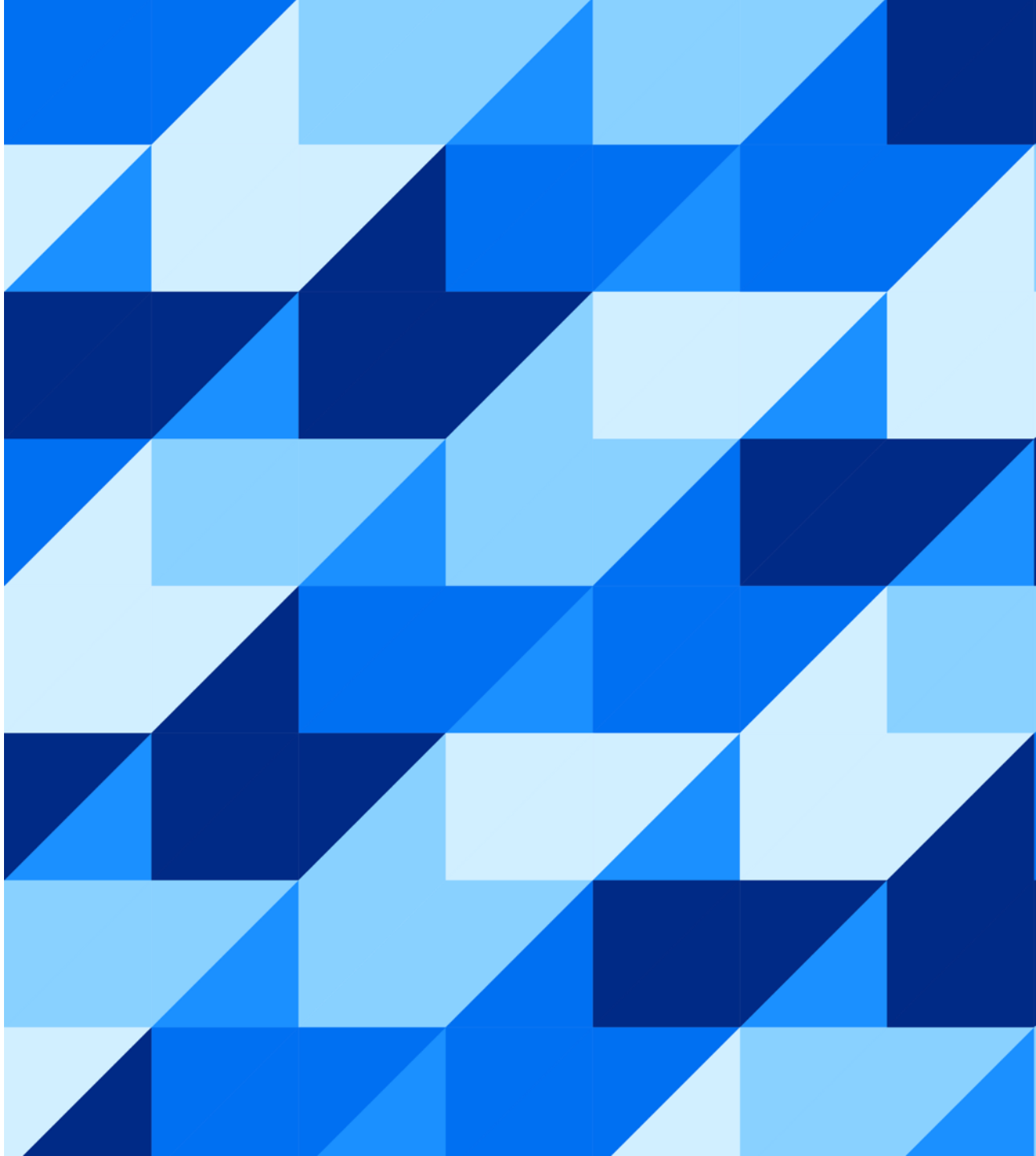


Shared Responsibility in SAP S/4HANA Cloud

Patrick Boch, SAP

Public

Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

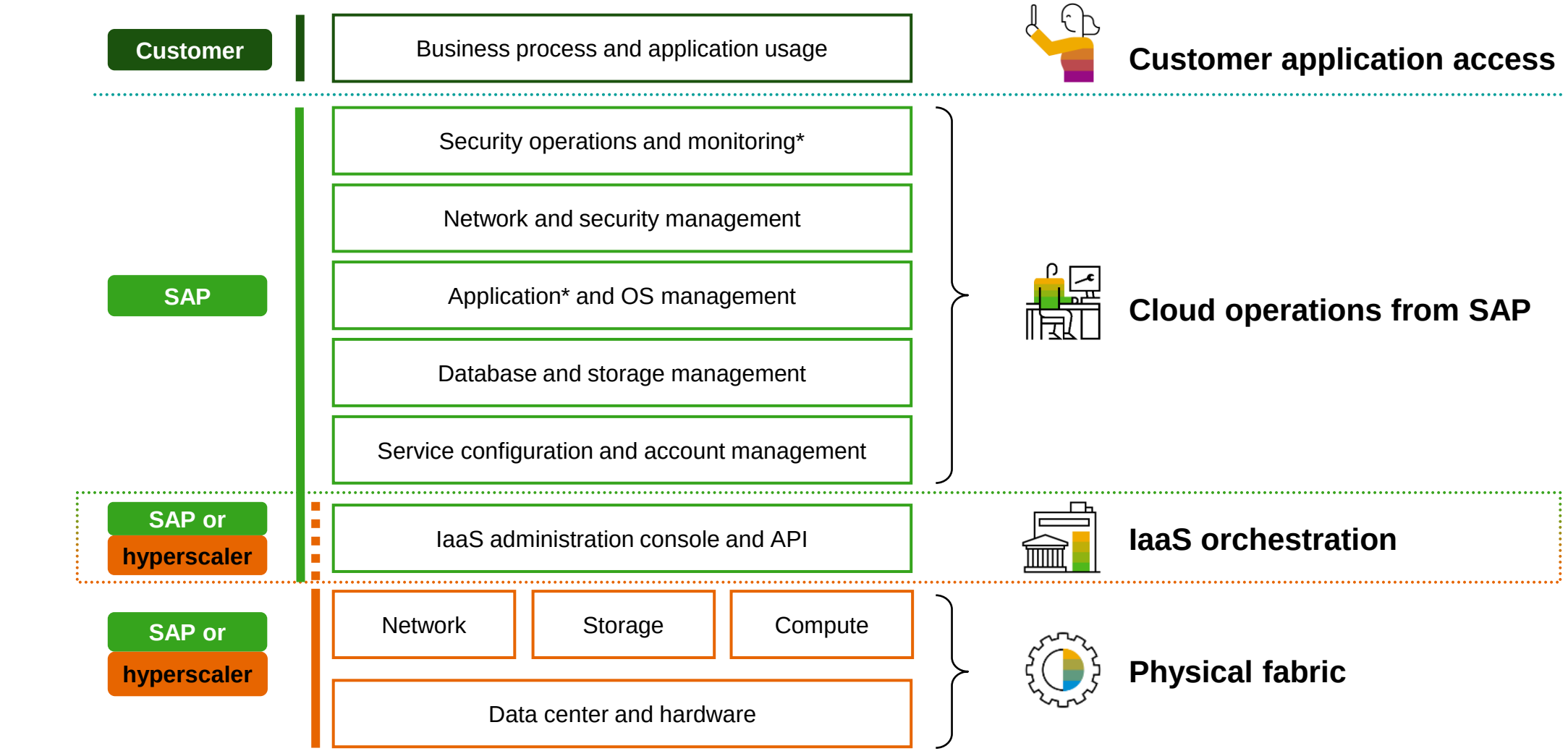
This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

SAP S/4HANA Cloud shared responsibility

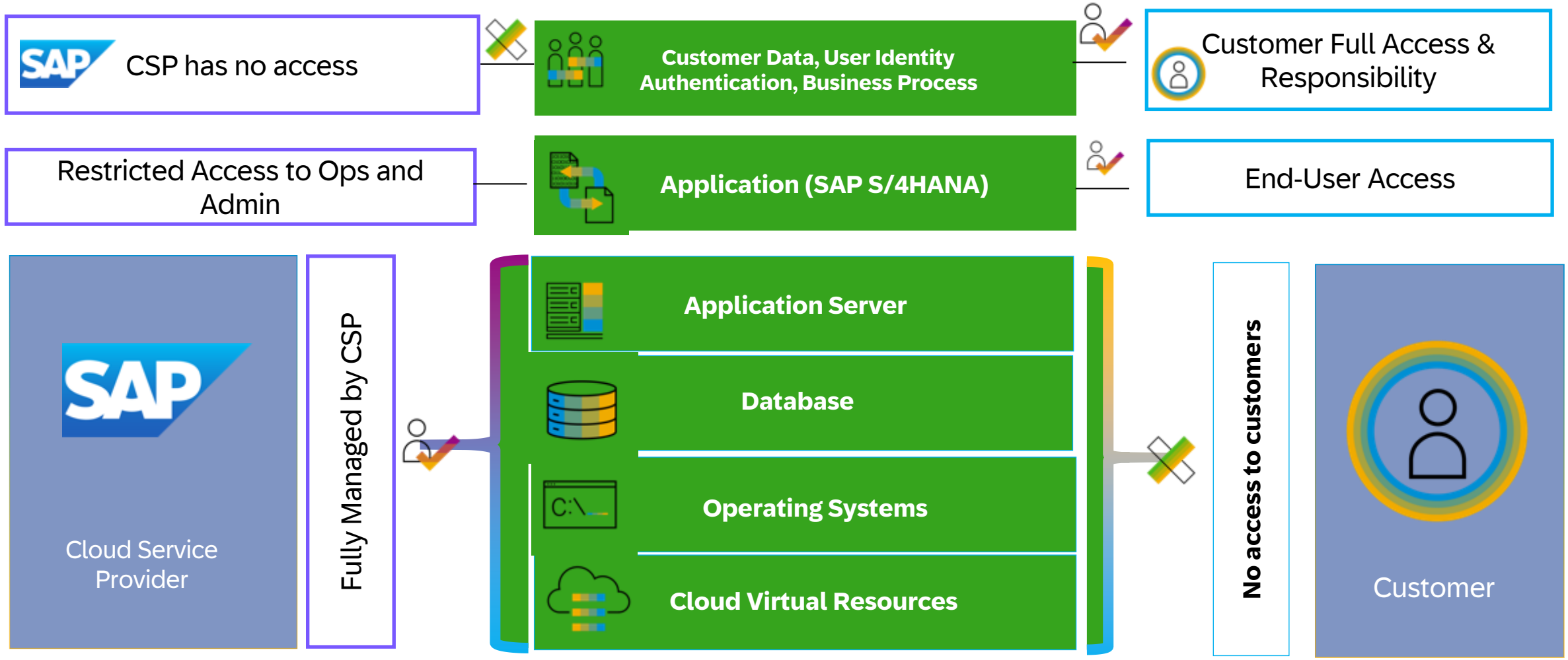
Run securely

Transparent



*Roles and responsibilities will vary depending on deployment (private, public).

Shared Access Governance



Detour: Auditing Approaches in Cloud Deployment Options

IT General Controls (ITGC) – 3 Layer Model

IT General Controls
IT Application Controls
Audit

Business Processes
ITACs

IT Applications

SAP S/4HANA

IT Infrastructure

Data Center, Server, OS

Attestation

SOX & Financial Statement Audit Certification

Quality - ISO9001 Certification

Security - ISO27001 Certification

Business Continuity - ISO22301 Certification

IT General Controls (ITGC) – 3 Layer Model

Audit

IT General Controls
IT Application Controls

Business Processes
ITACs

IT Applications
SAP S/4HANA

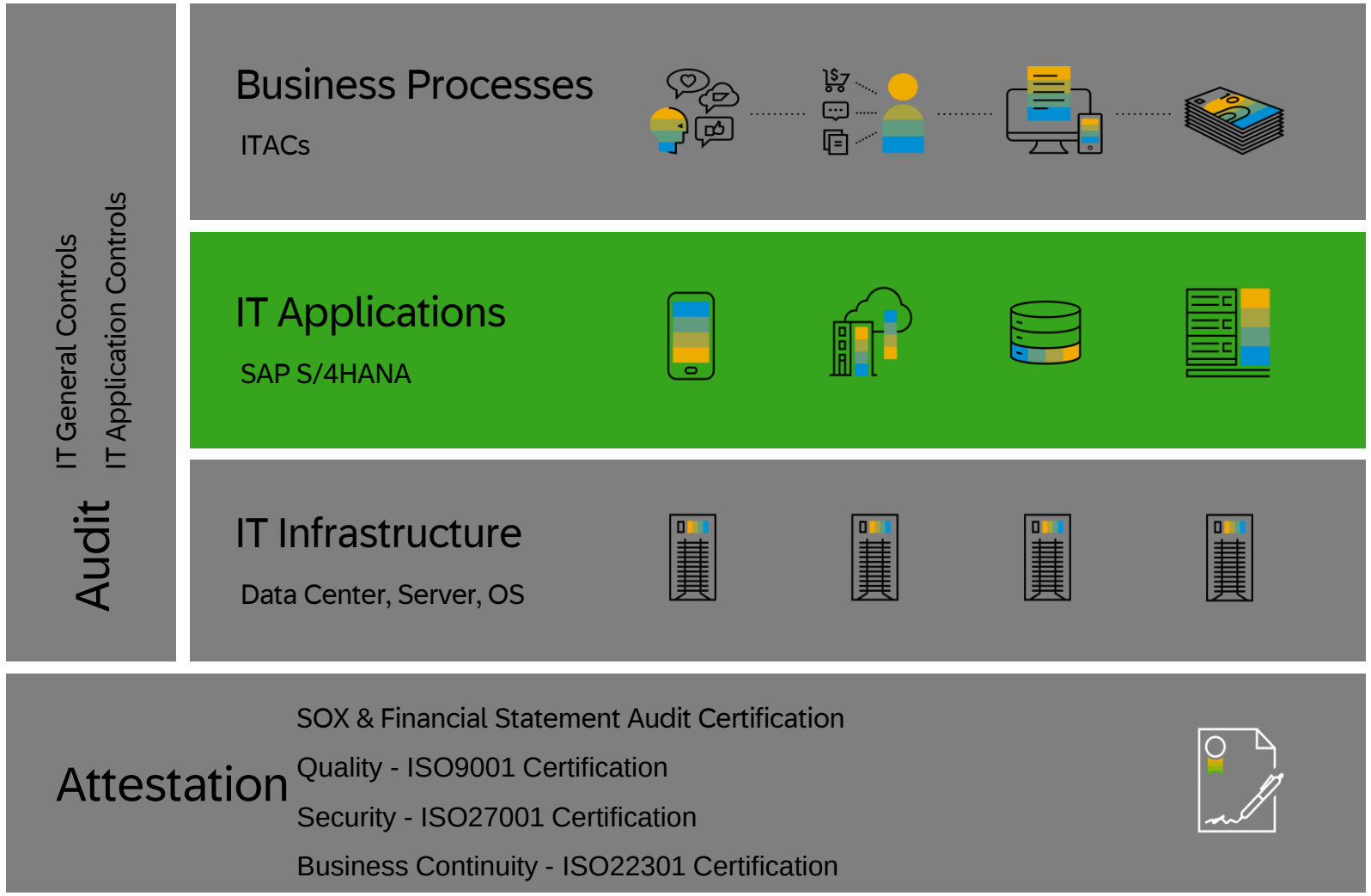
IT Infrastructure
Data Center, Serve

Attestation

SOX & Financial Statement Audit Certification
Quality - ISO9001 Certification
Security - ISO27001 Certification
Business Continuity - ISO22301 Certification

IT Application Controls (ITAC) exists and refers to transaction processing controls (→ Semi-Automated & Automated Controls). In general such controls are performed automatically by the systems and are designed to ensure the complete and accurate processing of data, from input through output. These controls are based within business specific application.

IT General Controls (ITGC) on Application Level

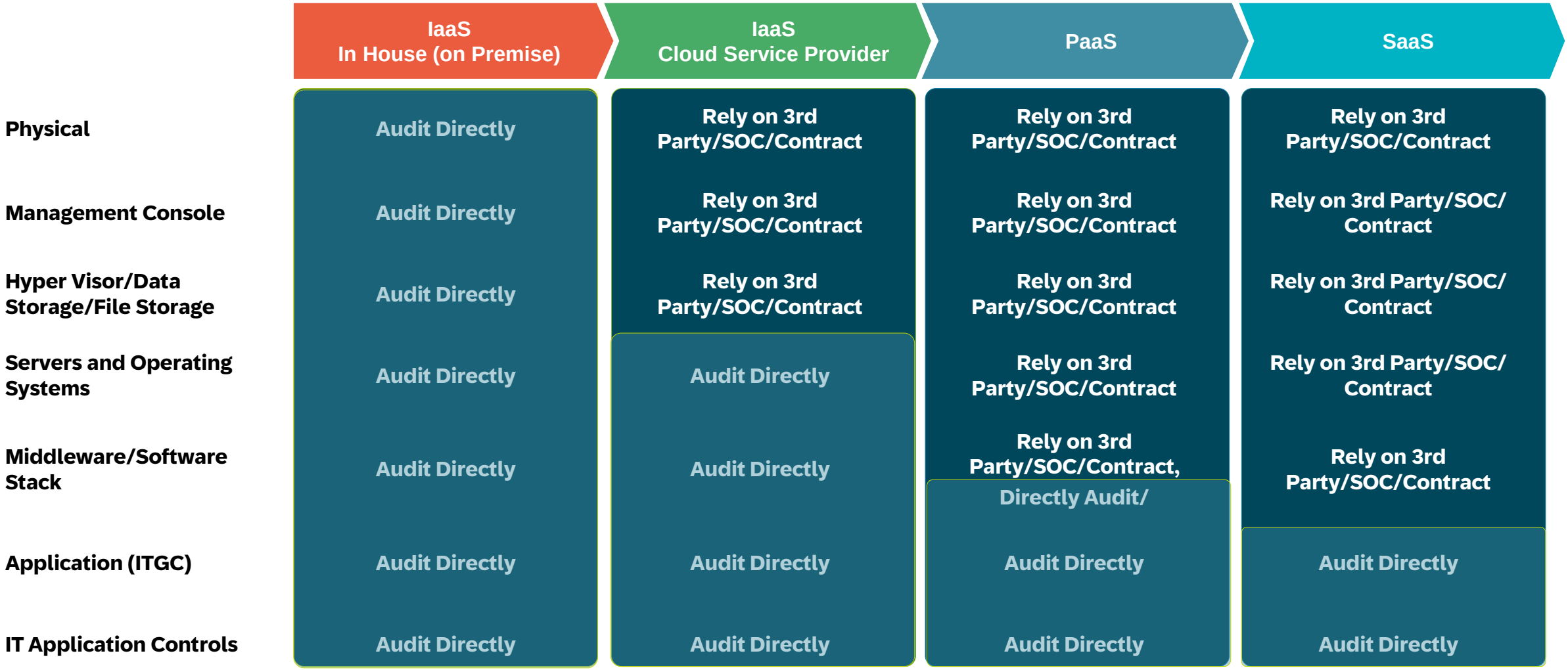


IT-related controls (ITGC) per system conducted on application-, operating system- and database-level for

- Access Management
- Change Management
- Security Configuration
- API-/Job-Monitoring

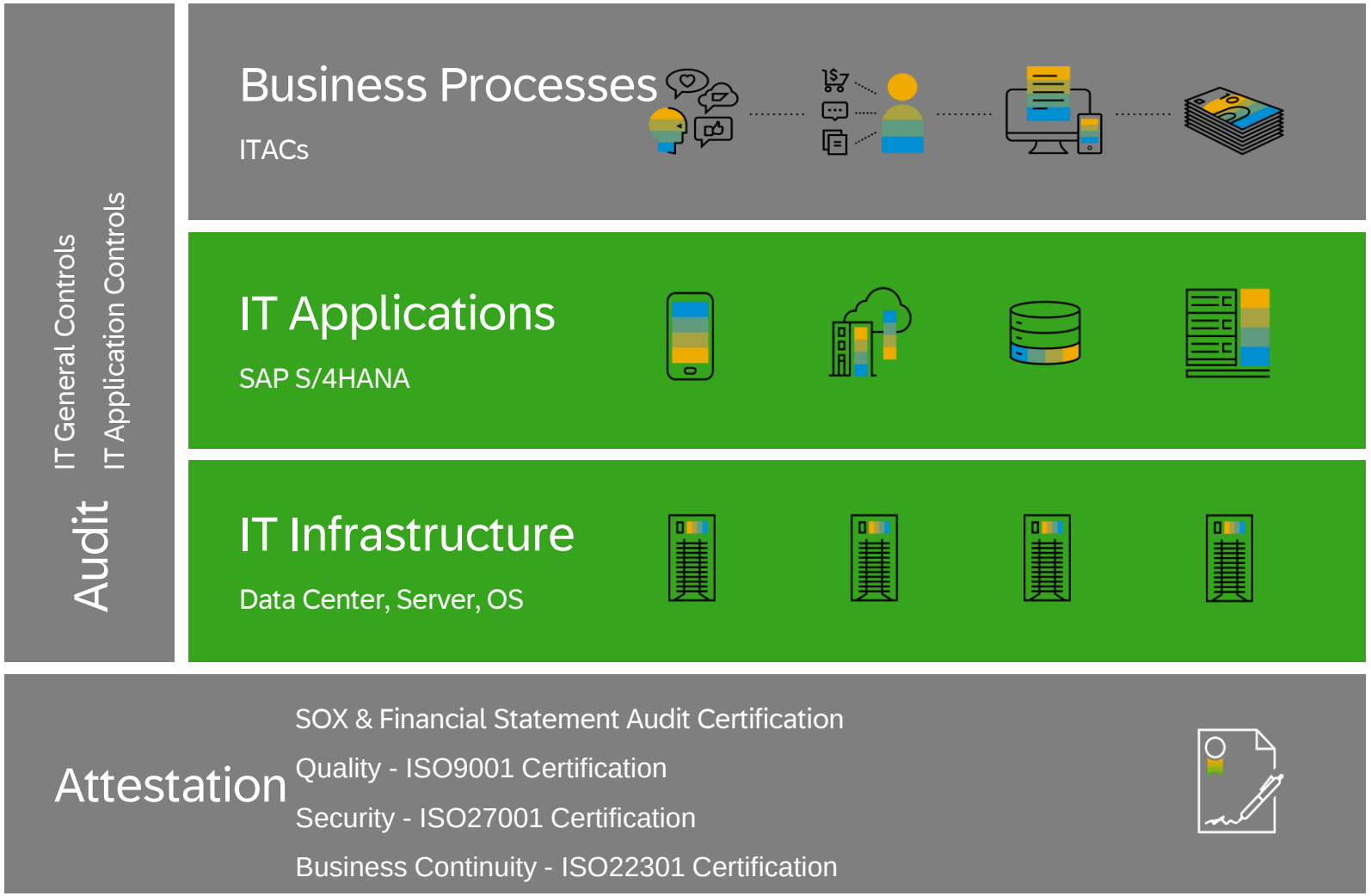
The ITGCs ensure proper development and implementation of applications, as well as the integrity of programs, data files and computer operations. They are designed to fulfill all requirements in regards to confidentiality, integrity, and availability of data.
Without effective ITGC, the reliance on our IT systems may not be possible!

Cloud Service Models – Controls tested at different Layers



Typical chart that may vary depending on the Cloud Services Provider (CSP)

Evaluation of SOC1 Type2 Report for SAP S/4HANA Cloud



Scope of
SOC1 Type2 Reports

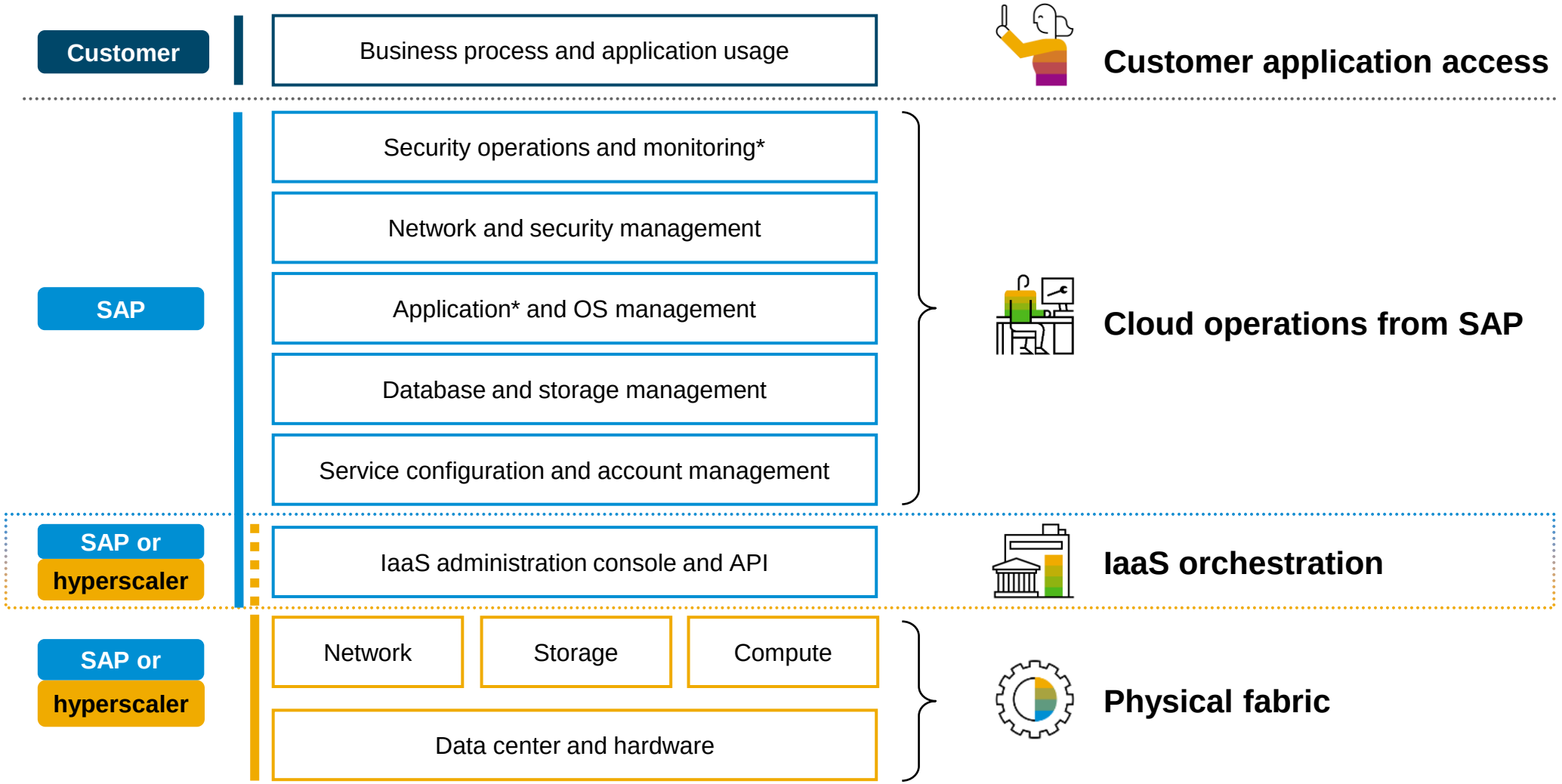
Evaluation of SOC1 Type2 Report for SAP S/4HANA Cloud

- The company is responsible to request, review and evaluate the SOC reports of cloud service providers
- This action is also audited as part of the year-end audit
- Items that need to be reviewed by the company and the IT auditors, e.g.
  - Understanding the service organization
  - Procedures performed by the service auditor report (SAR)
  - Relevant controls (not including ITGC)
  - Relevant IT-related controls (ITGC)
  - Further evaluation of relevant controls (incl. consideration of period of coverage and applicable rollforward procedures)
  - Exceptions
  - Complementary user entity controls (CUECs)
  - Subservice organizations
- SOC reports of SAP S/4HANA Cloud can be found at SAP Trust Center (https://www.sap.com/tc -> Compliance)

SAP S/4HANA Cloud shared responsibility

Run securely

Transparent

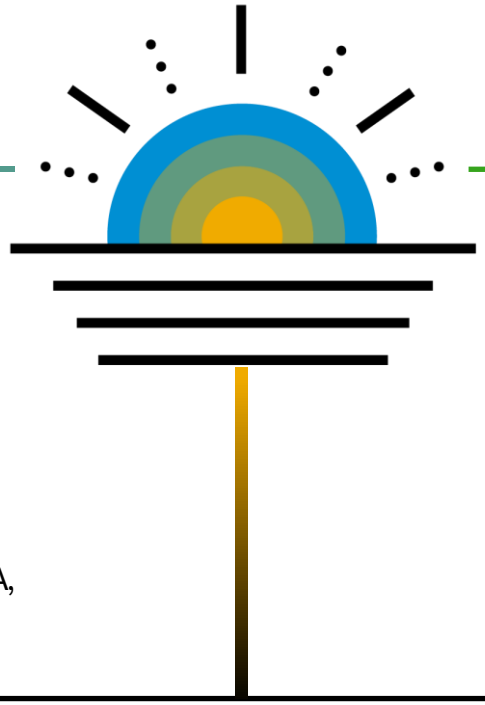


*Roles and responsibilities will vary depending on deployment (private, public).

Shared Security Responsibility Model

GROW WITH SAP

S/4HANA Cloud, Public Edition



SAP

- ✓ Resilient SaaS architecture
- ✓ Advanced Multi-Tenant Logical Separation
- ✓ Backup and restoration and Disaster Recovery
- ✓ Securing the infrastructure, operating systems, and networking, and applications
- ✓ Operational security monitoring & incident management
- ✓ Personal Data Breach Notification
- ✓ Hardening and Patching Operating Systems and solution support
- ✓ Adherence SLA and Contractual Assurance via SLA, SAP DPA, Support Policy

Customer

- ✓ Configuration of the Business Processes
- ✓ Tenant Administration and Management
- ✓ Identity Management
- ✓ Authentication and Authorisation
- ✓ Business Roles, User Groups, Access Control
- ✓ Customer Data Ownership and Protective Handling
- ✓ Compliance to Regulations
- ✓ Application Logs
- ✓ API Extension, Integration and 3rd party connectivity

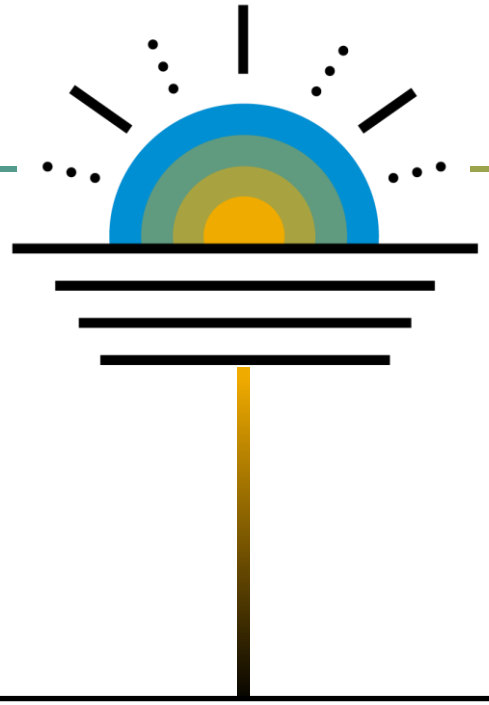
Cloud Infrastructure

- ✓ Physical Data Center Security in multiple Regions
- ✓ Resilient Network Connectivity and Availability Zones
- ✓ Underlying Physical, Virtual Infrastructure & Hypervisor
- ✓ Network Availability with built-in basic DDoS protection
- ✓ Audit, Security and Compliance on IaaS

Shared Security Responsibility Model

RISE WITH SAP

S/4HANA Cloud, Private Edition



SAP

- ✓ Resilient platform architecture (HA and DR)
- ✓ Single Tenanted Landscape
- ✓ Managed Backup and Restore
- ✓ Building Secure Virtual Machines, Operating systems, networking, HANA Database
- ✓ HANA DB Management
- ✓ Technical Managed Services (R&R Link)
- ✓ Operational Security and Managing security incidents
- ✓ 24x7 Security Monitoring
- ✓ Personal Data Breach Notification
- ✓ SLA and Support Services
- ✓ Threat Management & Patch Management

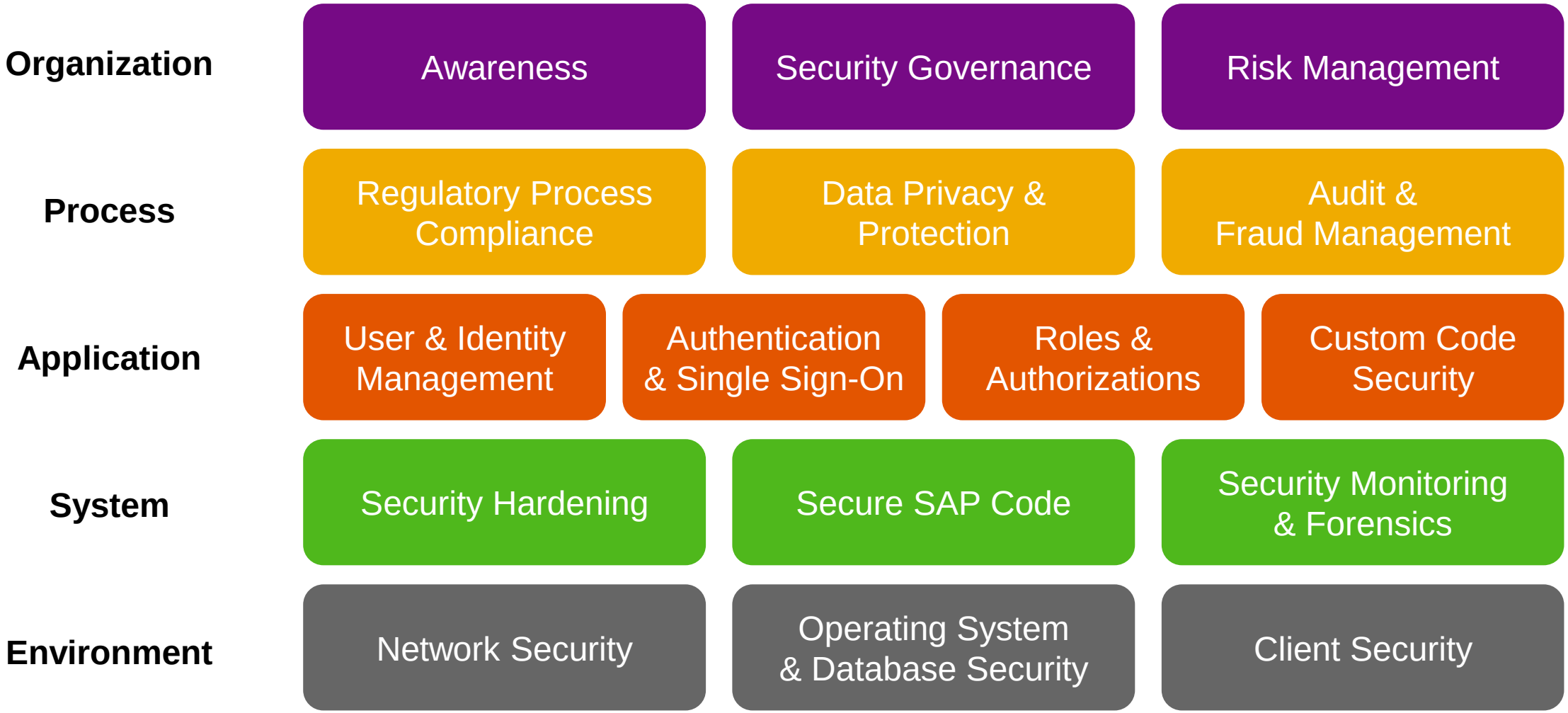
Customer

- ✓ Dedicated Private Connectivity to Hyperscaler
- ✓ Application User Identity Management
- ✓ Application User Authentication and Authorisation Management
- ✓ Application User Roles, User Groups, Access Control
- ✓ Customer Data Ownership
- ✓ Compliance to Government & Industry Regulations
- ✓ Application Security Audit Logging (SAL)
- ✓ Integration and Extensions, Custom Applications Development
- ✓ Configuration of the Customer Business Processes
- ✓ Application Change Management

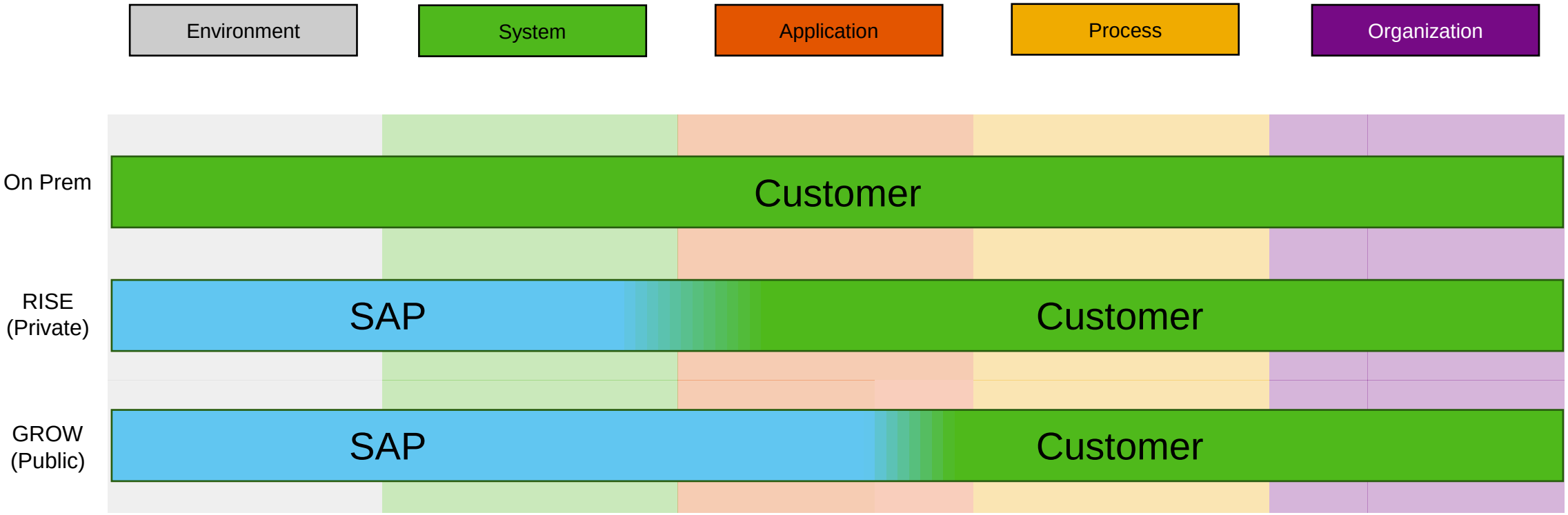
Cloud Infrastructure

- ✓ Physical Data Center Security in multiple Regions
- ✓ Resilient Network Connectivity and Availability Zones
- ✓ Underlying Physical, Virtual Infrastructure & Hypervisor
- ✓ Network Availability with built-in basic DDoS protection
- ✓ Audit, Security and Compliance on IaaS

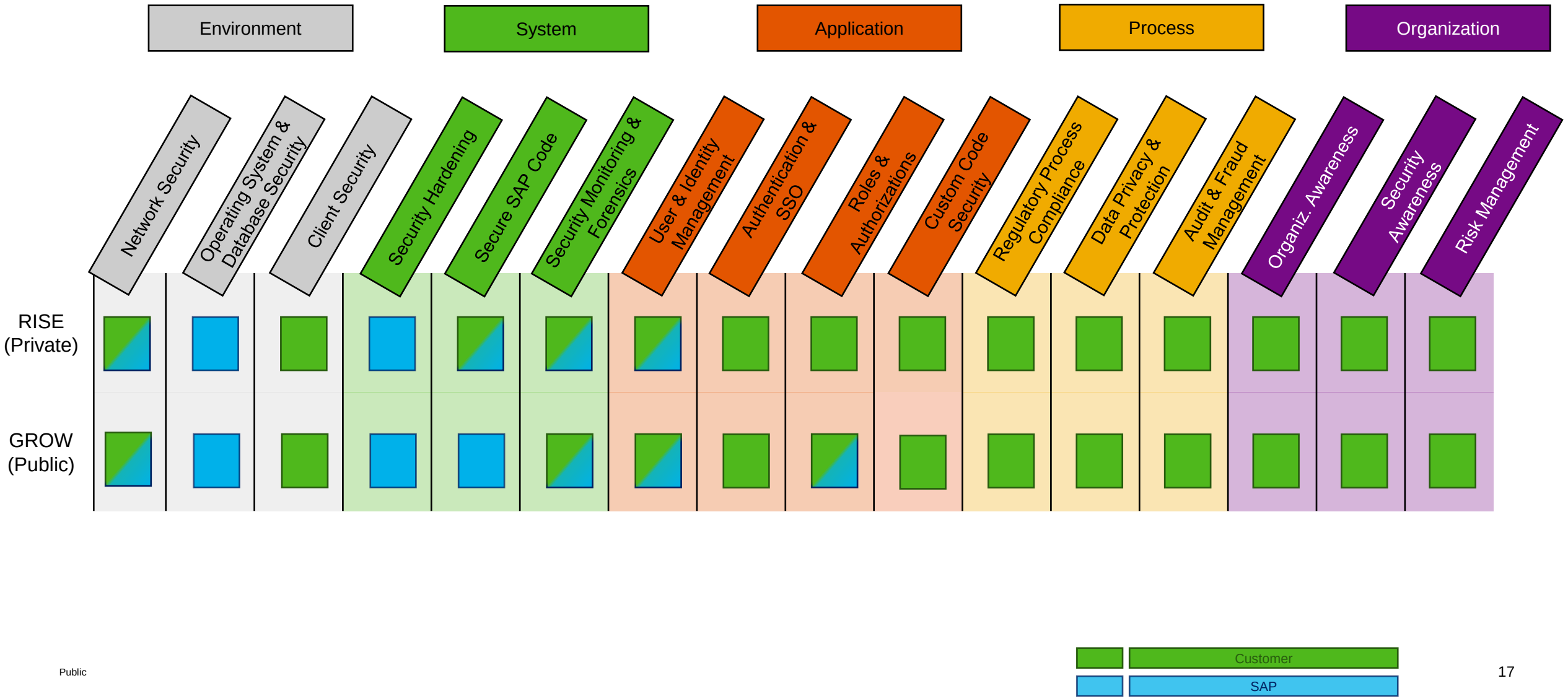
SAP Secure Operations Map



Core Responsibilities per Architectural Setup



Core Responsibilities per Architectural Setup



Core Responsibilities per Architectural Setup - Environment

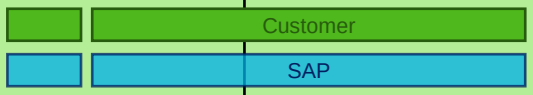
	Network Security	Operating System & Database Security	Client Security
RISE (Private) GROW (Public)	• Setting up trust boundaries network separation. • Setting up system landscape such as Load Balancers, Web Dispatchers, setting up Security Groups, ABAP, SAP HANA – Tenant DB, System DB • Encrypt end-to-end data in transit with TLS 1.2 and Data at Rest with AES-256-bit encryption. • Generate customer specific encryption keys to encrypt data at rest during the deployment • SAP manages cloud networking within the SAP S/4HANA cloud, public edition setting up trust boundaries. The Internet have built-in network level DDOS protection enabled • Customer is responsible for setting up secure integration for inbound and outbound communications to 3rd party systems and configuring trust between systems. • Full control over encryption key, its life cycle in Customer Controlled Encryption Key (CCEK) with SAP Data Custodian KMS service. This is an optional service requiring a separate license.	• Security of the SaaS platform architecture through advanced multi-tenant logical separation, security patching, managing backup and restoration, as well as securing infrastructure elements such as operating systems, networking, and applications. • Additionally, SAP handles cloud (Hyperscaler) account management, operational security monitoring, incident management, personal data breach notifications, hardening and patching operating systems, application and providing solution support. • Customer can additionally monitor infrastructure logs. Only if customer buys logserv (RISE)	• Clients like SAPGUI or SAP Business Client (RISE) or web browser (GROW) • Configuration, control and monitoring of the client or execution rules for browsers • End point security

Core Responsibilities per Architectural Setup - System

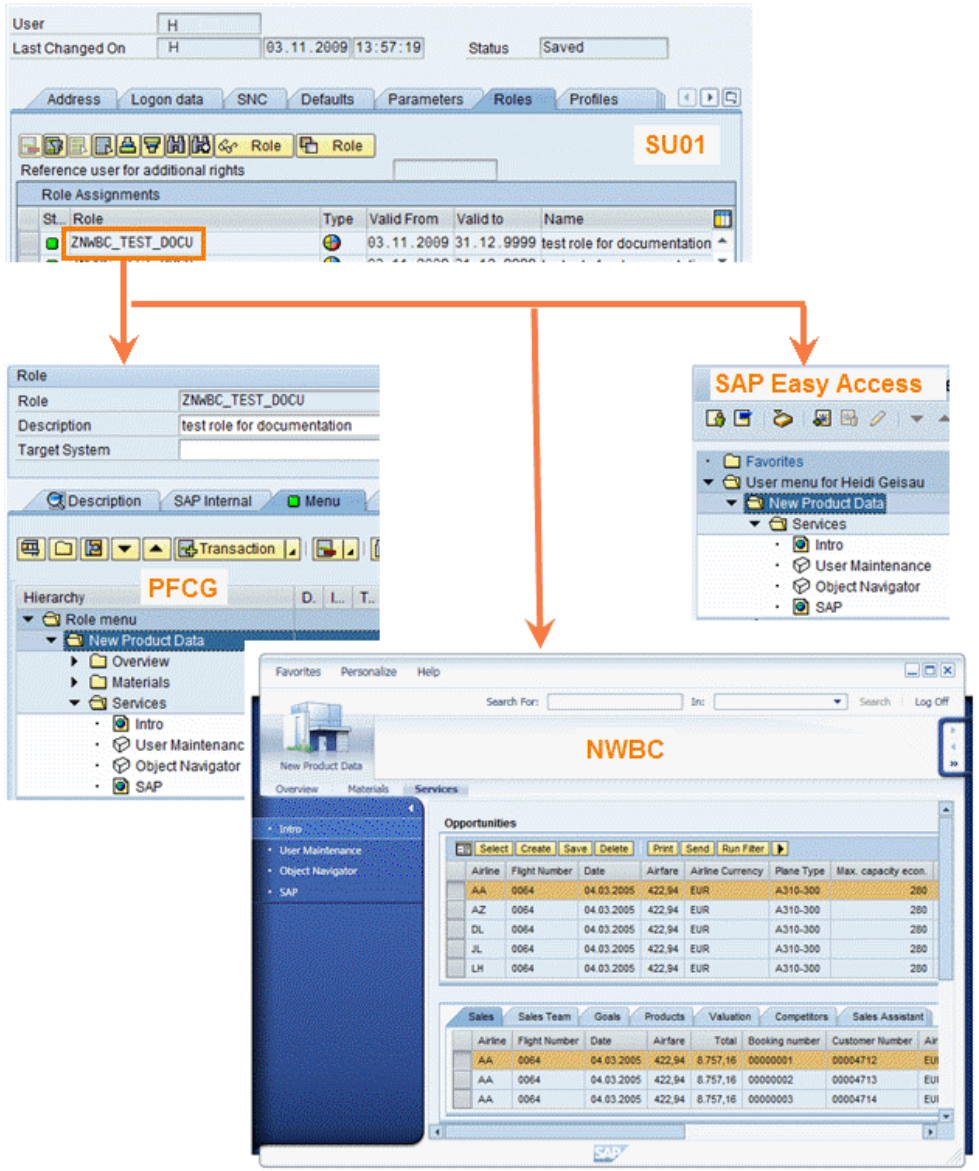
	Security Hardening	Secure SAP Code	Security Monitoring & Forensics
RISE (Private) GROW (Public)	• Customer needs to open a ticket to SAP to implement • Perform regular vulnerability management and penetration testing of the SaaS platform. • SAP maintains default security setting for session timeouts for UI, ABAP, Backend. Additional default settings include Business user Login via IAS, Retention, Read Access Logging, Certificates Auto-update etc.	• Customer need to look and select what the need and open ticket to patch system. • SAP performs changes. • CAS as an optional service for assessment, analyze etc… • Validate and revise the authorization concept following functional upgrades. • Perform regular patches for OS, Application and DB and for functional enhancement • SAP follows Secure Software Development Lifecycle approach to application development ensuring that application is secure, free from known malicious code	• Responsible for reviewing security audit logs such as technical user level logins and retrieval of such logs via API. • Review of logs such as Change documents, Read access logs, Authorization trace logs, SAP support user request logs • Customer can additionally monitor infrastructure logs. Only if customer buys logserv (service) • Maintain 24×7 Security Monitoring • Collect and Correlate Platform logs. • Define Security Use cases for automatic alerting. • Maintain Security Incident and Event Management Platform. • Monitoring in S/4 HANA is limited to client 000.

Core Responsibilities per Architectural Setup - Application

	User & Identity Management	Authentication & Secure Login Service	Roles & Authorizations	Custom Code Security
RISE (Private)	• Customer needs his corporate identity management solution. • SAP provides cloud identity managed service	• Provide SAP Cloud Identity Services (SAP BTP) for authentication and SSO integration with customer IDP configuration needs to be handled by customer.	• Customer is fully in charge of roles and authorizations in the working client. • Customer create ticket for SAP to access their production client	• Customer must manage custom code
GROW (Public)	• Customer needs his corporate identity management solution. • SAP provides cloud identity managed service	• Provide SAP Cloud Identity Services (SAP BTP) for authentication and SSO integration with customer IDP • configuration needs to be handled by customer. • The responsibility of delegating authentication to customer's own Corporate Identity Provider (IDP) and configuring SAP Identity Authentication Services as an Identity Proxy lies	• Configure Role Based Access Control (RBAC) of SAP Cloud Admin Users via Cloud Access Manager (CAM) • Defines Business Roles using SAP templates and Configure Role Based Access Control to Business Users • Customer create ticket for SAP to access their production client	• Customer must manage custom code



Comparison: Roles and Authorization



Maintain Business Roles

Billing Specialist - Projects Edit | Display Changes After Upgrade | Display Restrictions | Display Restriction Overview | Display Restrictions (Deprecat

92_SAP_BR_PROJ_BILLG_SPCLST

Write Access: Restricted
Read Access: Restricted
Value Help Access: Restricted

Changed By: Example Administrator
Changed On: 2023-10-19, 16:57:58

Editing Status: Active
Exported: No

General Role Details | Business Catalogs (10) | Business Users (0) | Launchpad Spaces (0)

General Data

Business Role ID:* 92_SAP_BR_PROJ_BILLG_SPCLST
Business Role Description: Billing Specialist - Projects
Business Role Long Text:

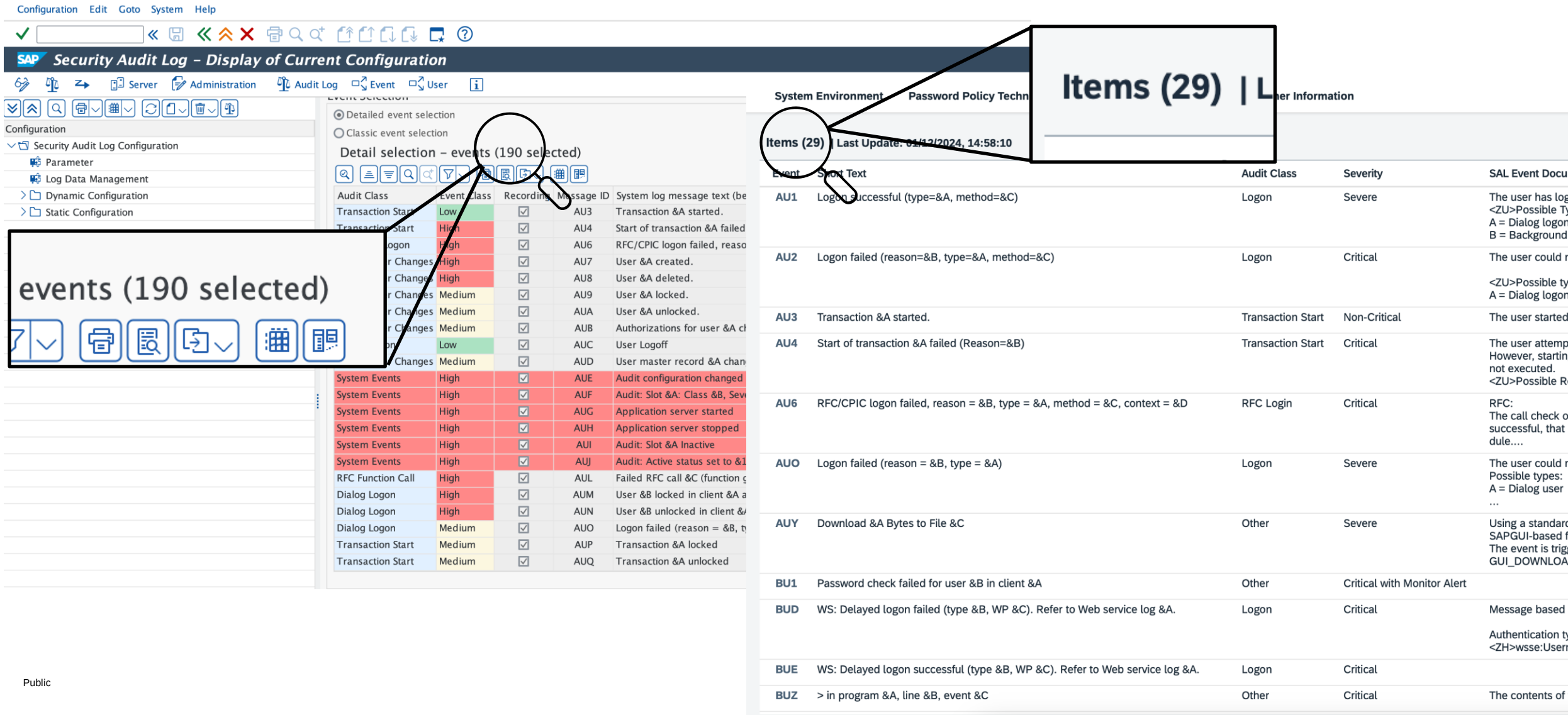
Access Categories

Write, Read, Value Help: Restricted
Read, Value Help: Restricted
Value Help: Restricted

Others

Price Category: Core
Business Role Template ID: SAP_BR_
Leading Business Role ID:
Is Leading Business Role:
Exposed to SAP BTP:

Comparison: Security Audit Log Events



Comparison: Password Policies

Configuring Password Policies

Passwords for the authentication of users are subject to certain rules. These rules are defined in the password policy. Identity Authentication provides you with two predefined password policies, in addition to which you can create and configure up to three custom password policies.

You have the following options for a password policy:

- Standard
  (Predefined) Use this option to set special rules for changing, resetting, and locking a password.

  Note
  This is the default setting. It meets the minimum strength requirements.

- Enterprise
  (Predefined) Use this option to set enhanced password management features. It's stronger than the standard policy, but weaker than the custom one.

- Custom
  (Configurable) Use this option to set the strongest password management features for the password policy. It's the responsibility of the tenant administr
  configure the custom password policy stronger than the standard and enterprise ones.

  Remember
  This option is only possible if you've configured a custom password policy in the administration console for SAP Cloud Identity Services. For more inf
  see Configure Custom Password Policy.

Password Policy Requirements

Requirement	Standard	Enterprise	Custom
Content of password	▪ Minimum length of 8 characters; ▪ Maximum length of 255 characters; ▪ Characters from at least three of the following groups:	▪ Minimum length of 8 characters; ▪ Maximum length of 255 characters; ▪ Characters from at least three of the following groups:	▪ Minimum length of 8 cha ▪ Maximum length of 255 ▪ Characters from betwee the following groups:

Configure Custom Password Policy

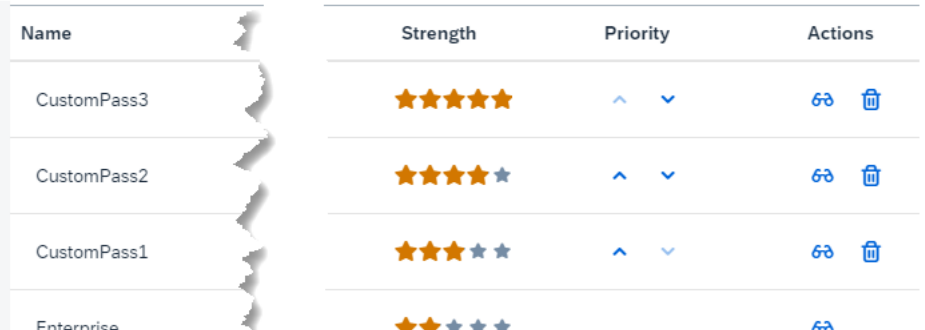
Tenant administrators can create and configure a custom password policy for scenarios where Identity Authentic

Context

Identity Authentication provides you with two predefined password policies, in addition to which you can create

The custom password policy by default must be stronger than the enterprise policy, which in turn is stronger tha administrator to configure the custom password policy stronger than the standard and enterprise ones. Each pas visualized by stars in the administration console for SAP Cloud Identity Services. The strength specifies the prio be enforced for password checks.

It is not possible to have password policies with one and the same strength. Once created and saved, the tenan in the administration console, thus changing the strength assigned to the custom password policies.



Core Responsibilities per Architectural Setup - System

	Regulatory Process Compliance	Data Privacy & Protection	Audit & Fraud Management	Organize. Awareness	Security Awareness	Risk Management
RISE (Private)						
GROW (Public)						

Customer

SAP

Built-In Security

SAP S/4HANA Cloud

S/4HANA Cloud security features

Secure access
- SAP Business Technology Platform Identity Authentication Service
- Supports single sign-on with X509, SAML
- Two factor authentication
- Supports SAP & 3rd party identity provider

Manage users and permissions
- SAP Business Technology Platform Identity Provisioning Service
- Simplified configuration of authorizations with delivered catalogs and role templates

Detect attacks
- SAP Security audit logs shared with customers for further analysis

Secure communication & encryption
- Secure communication by encryption in transit
- Encryption of data at rest using SAP HANA capabilities

SAP managed security configuration
- Enforce Secure by default
- Automated security patch deployment
- Secure customer access points
- Protection against malicious attachments

Data Protection Feature
- Relevant security safeguards
- Support for fulfilling data subject requests
- Ability to segregate personal data using organizational attributes
- Personal data deletion capabilities
- Inbuilt auditing capabilities
- Advanced authorization concepts

Embedded Data Privacy Tools
- Information Retrieval Framework (IRF)
- Information Lifecyle Management (ILM)
- Read Access Logging (RAL)

Protect your SAP S/4HANA Cloud

Act securely

Our customers

RISE with SAP

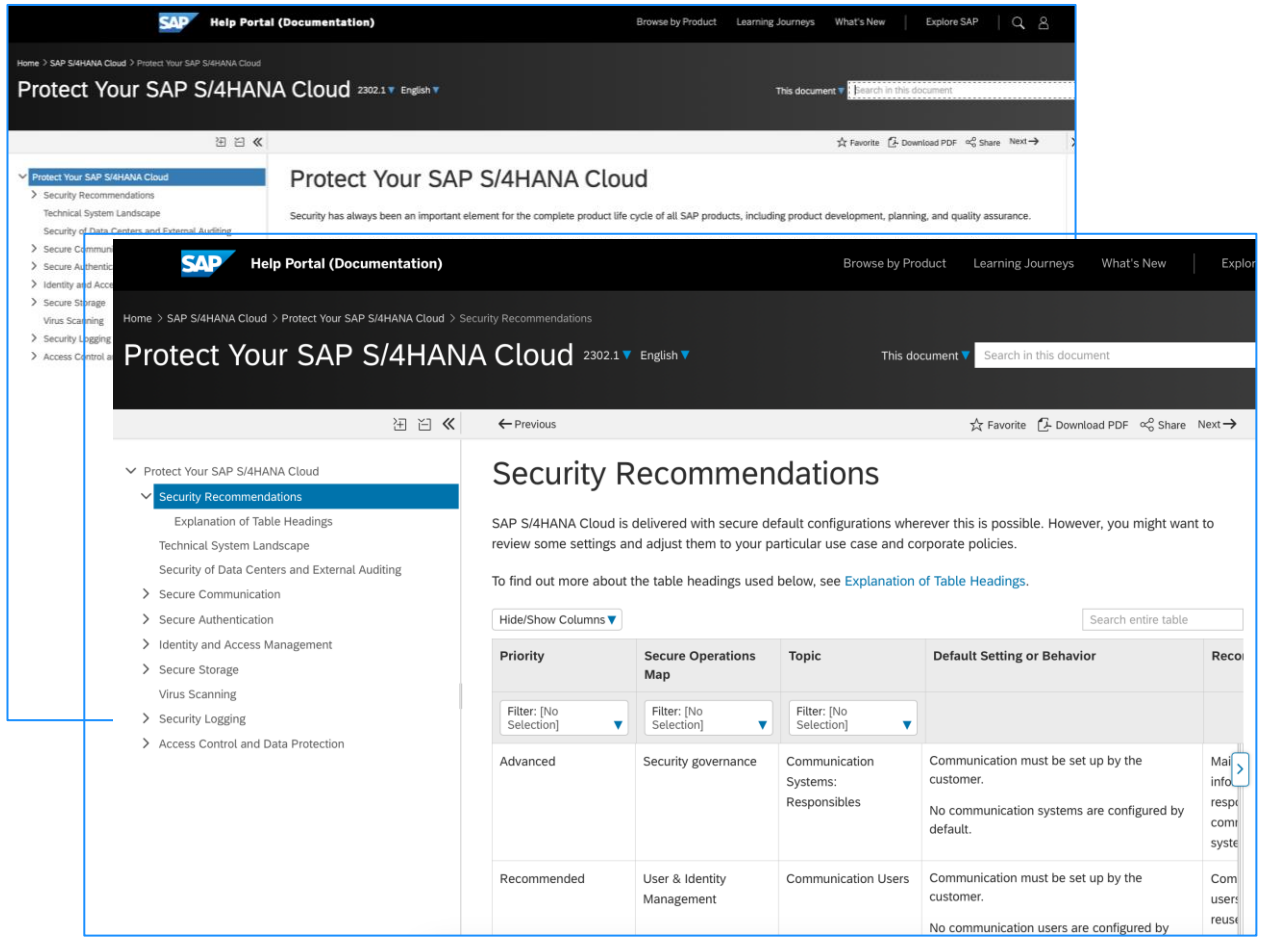
help.sap.com

PUBLIC
Document Version: 3.0 – 2023-05-26

Security Guide for SAP S/4HANA 2022

THE BEST RUN SAP

GROW with SAP



Additional Security
Services and Solutions

Identity and Access Governance

SAP Sustainability

SAP Fieldglass

SAP IBP

SAP Cloud Identity Services

SAP SuccessFactors

SAP Concur

SAP Ariba

SAP Authorization and Trust Management Service

- Manage user authorizations and trust to identity providers

SAP Cloud Identity Services - Identity Authentication

- Single sign-on for cloud- and hybrid-scenarios (SAML 2.0)
- Authentication methods Form, SPNEGO, Social, or two-factor

SAP Cloud Identity Services - Identity Provisioning

- Identity Lifecycle Management for SAP's cloud applications
- supports SCIM2.0 (System for Cross-Domain Identity Management

SAP Cloud Identity Access Governance

- Access-request, -design, -analysis, -certification
- Role design
- Privilege access management
- Segregation of duty

Public Cloud

On Prem

SAP S/4HANA

SAP S/4HANA Cloud, private edition

SAP Single Sign-On

- Secure authentication and communication
- Simplification and productivity

SAP Identity Management

- Business-driven compliant entire identity life cycle
- Hiring, substitution, promotion, termination

SAP Access Control

- Segregation of duty
- Manage access
- Monitor, analyze, maintain, provide, certify

Cyber Security and Data Protection

SAP SuccessFactors

SAP Concur

SAP Fieldglass

SAP IBP

SAP Ariba

SAP Sustainability

Public Cloud

On Prem

SAP S/4HANA

SAP S/4HANA Cloud, private edition

SAP Enterprise Threat Detection + Cloud Edition

- SIEM solution tailored to the needs of SAP applications
- Effectively identify and analyze threats in SAP applications

SAP Data Custodian

- Monitor and report on data access, storage, movement, processing, and location
- Create and enforce data access, location, movement, and processing policies
- Key management

Identity Access Governance

SAP Focused Run

- Security Configuration Management
  SAP S/4HANA, SAP HANA, SAP NetWeaver & J2EE
- Patch Management

SAP Code Vulnerability analyzer

- Identify and remedy security vulnerabilities in ABAP custom code

Checkmarx

Fortify

UI Masking and logging

- Protect sensitive information in the user interface layer
- Block or log data access
- Secure & refine access

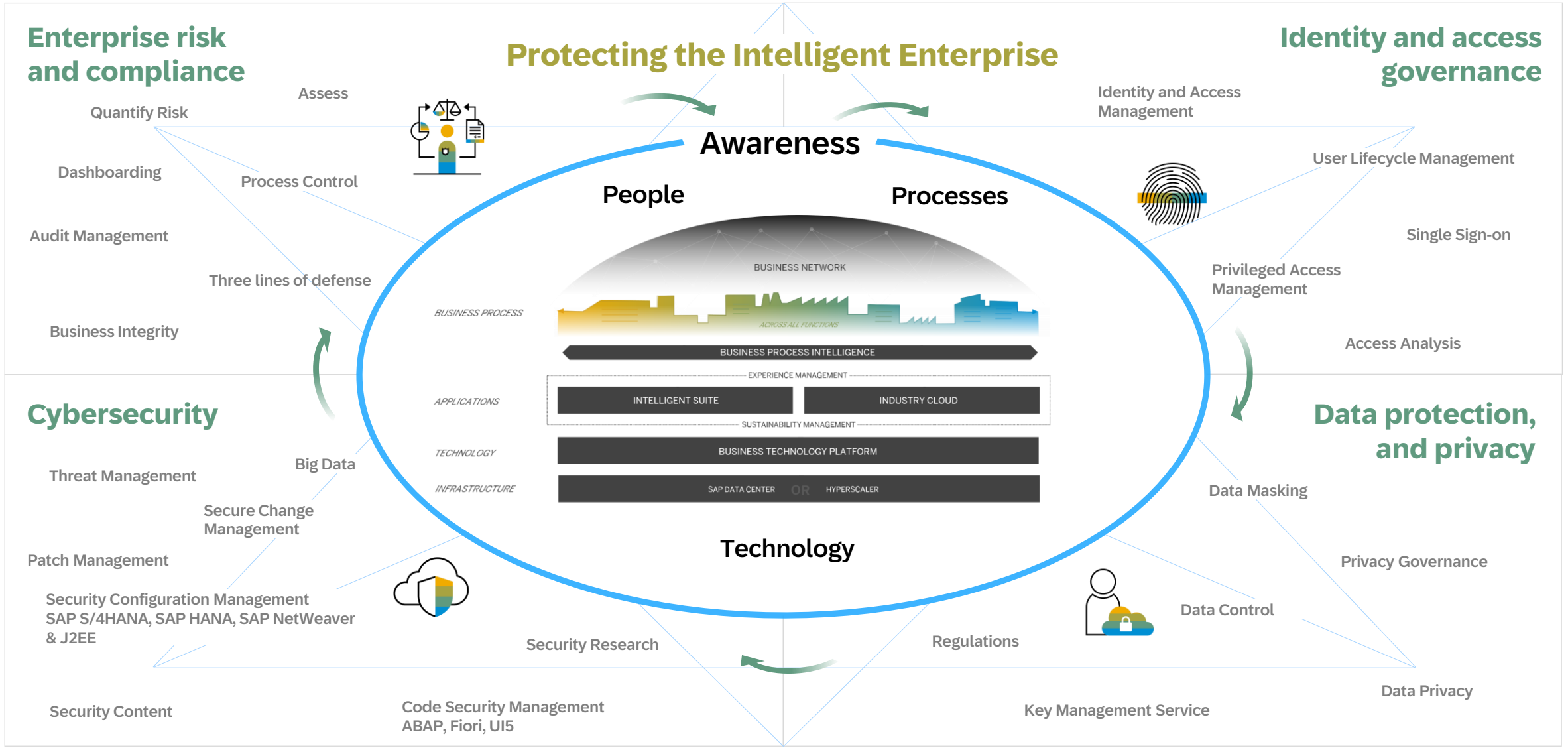
Thank you.

Contact information:

Arndt Lingscheid
a.lingscheid@sap.com

THE BEST RUN SAP

SAP Depth and Breadth, supporting the Intelligent Enterprise



Follow us

www.sap.com/contactsap

THE BEST RUN SAP