

Secure Your SAP Environment

Improve Security And Reduce Operational Risks

Tobias Kutning, Senior Manager Product Management SAP, SUSE
Gabriele Fiata, Global Head of Cybersecurity Market Strategy, SAP

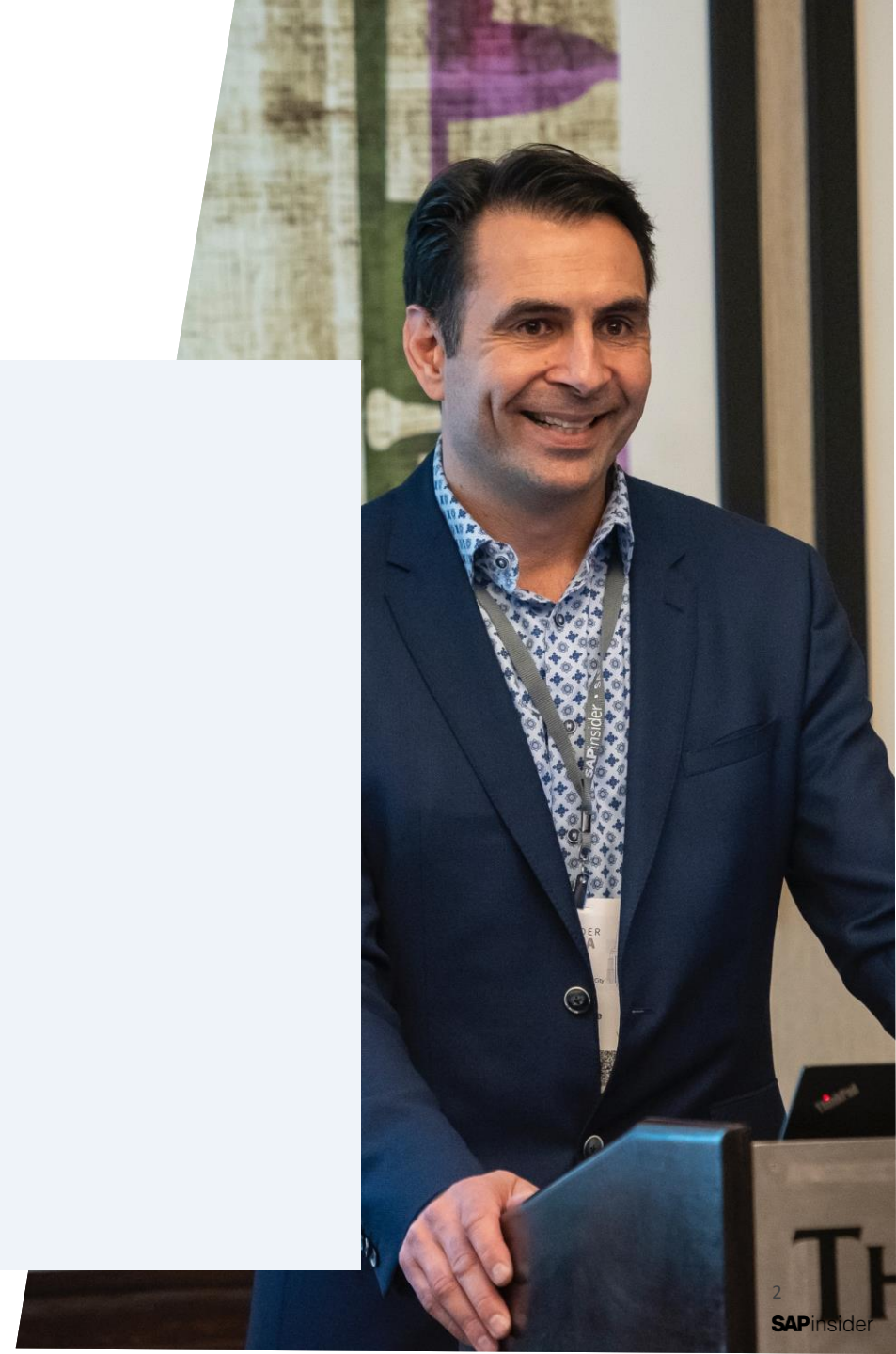
SAPinsider
Las Vegas

2023

SAPinsider

What We'll Cover

- SAP Security today
- How to improve the security for your SAP environment
- Security of the Environment layer
- Security Best-Practices
- Outlook: What's important for tomorrow?
- Wrap-up



SAP Security today

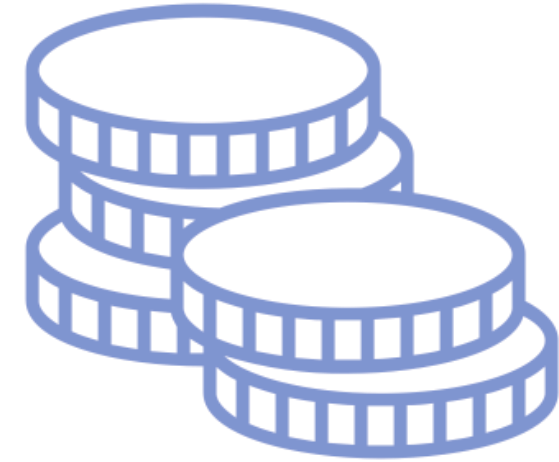


Skills Shortages and Complexity

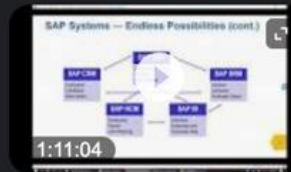


Sources: 1. IBM, number to Cost of Data Breach Report 2022; 2. Cyberseek, Cybersecurity supply/demand heatmap 2022; 3. Sophos, The State of Ransomware 2022 whitepaper

An increasing attack focus on SAP



SAP Hacking - Let Google hack your SAP System 2.0 - YouTube



Learn how to effectively protect your **SAP system** from vulnerabilities that are publicly known. Gather tips on what to...

A Red Team Approach to Targeting SAP



He leads **ERP** security testing efforts against **SAP**. ...
HackTheBox, IoT, Software Defined Radio, Hardware **hacking**,...

HACKING KIIT SAP LOGIN AND PASSWORD ... - YouTube



Authorities responsible for security should look forward to this flaw Strengthening the **system**, debug the loopholes and also...

SAP RFC Hacking - YouTube



RFC exploits are hardly new. In fact, some of the well-known exploits demonstrated below are addressed by **SAP** Notes dati...

SAP systems are worthwhile targets

- SAP systems often form the digital heart of an enterprise
- Central SAP systems like a central ERP system stores business-critical data
- Espionage, sabotage & data-theft targeted on SAP systems can have serious economical consequences for an organization
 - Data-theft: Loss of possibly business-critical data
 - Espionage: Attacks directed on specific business-critical information
 - Sabotage: Consequences of longer downtimes or successful ransomware attacks
- Investments into security of SAP landscapes are minimal compared to possible created costs in case of a successful cyber-attack

Security breaches in SAP result in

- Downtime
- Data loss
- Revenue loss
- Damage to the brand
- Lost consumer confidence

TOP Cybersecurity threats and challenges

Threats

1. Ransomware attacks
2. Credentials compromise
3. Unpatched systems
4. Weak access controls
5. Connections to other systems
6. Data exfiltration
7. Lack of end-user education
8. Custom code vulnerability
9. Cybersecurity skills gap
10. Supply chain attacks
11. Limited visibility

Challenges

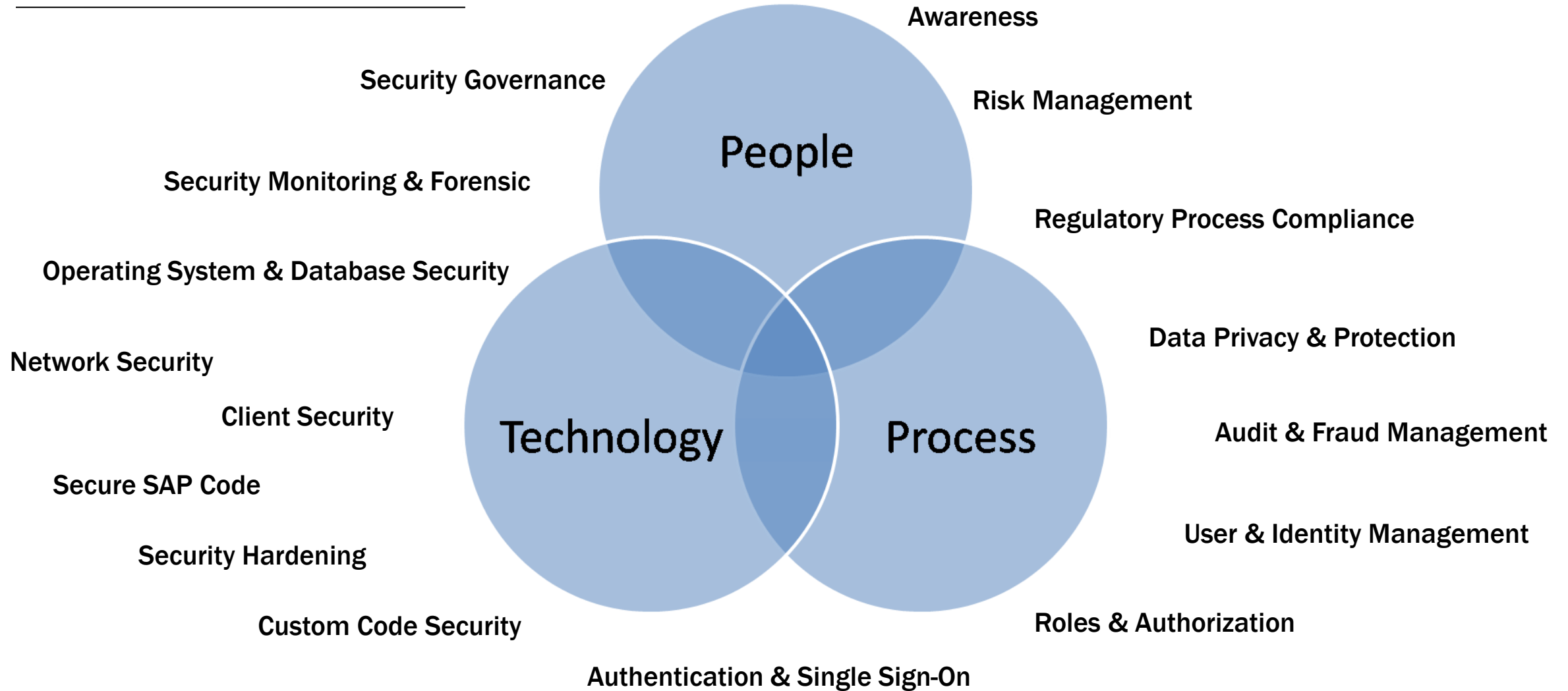
1. Detecting Potential Threats
2. Keeping Up with Patches and Updates
3. Securing custom code
4. Protecting Data
5. Auditing User Privilege
6. Avoid password misuse, sharing or compromised
7. Attract and employ cybersecurity resources
8. Monitoring user activity
9. Ensuring segregation of Duties
10. Avoid malware Downloaded Though End User Systems

¹ "Cybersecurity Threats to SAP Systems" SAPInsider, March 2022. <https://www.suse.com/c/cybersecurity-threats-to-sap-systems/>

How to improve the security for your SAP environment

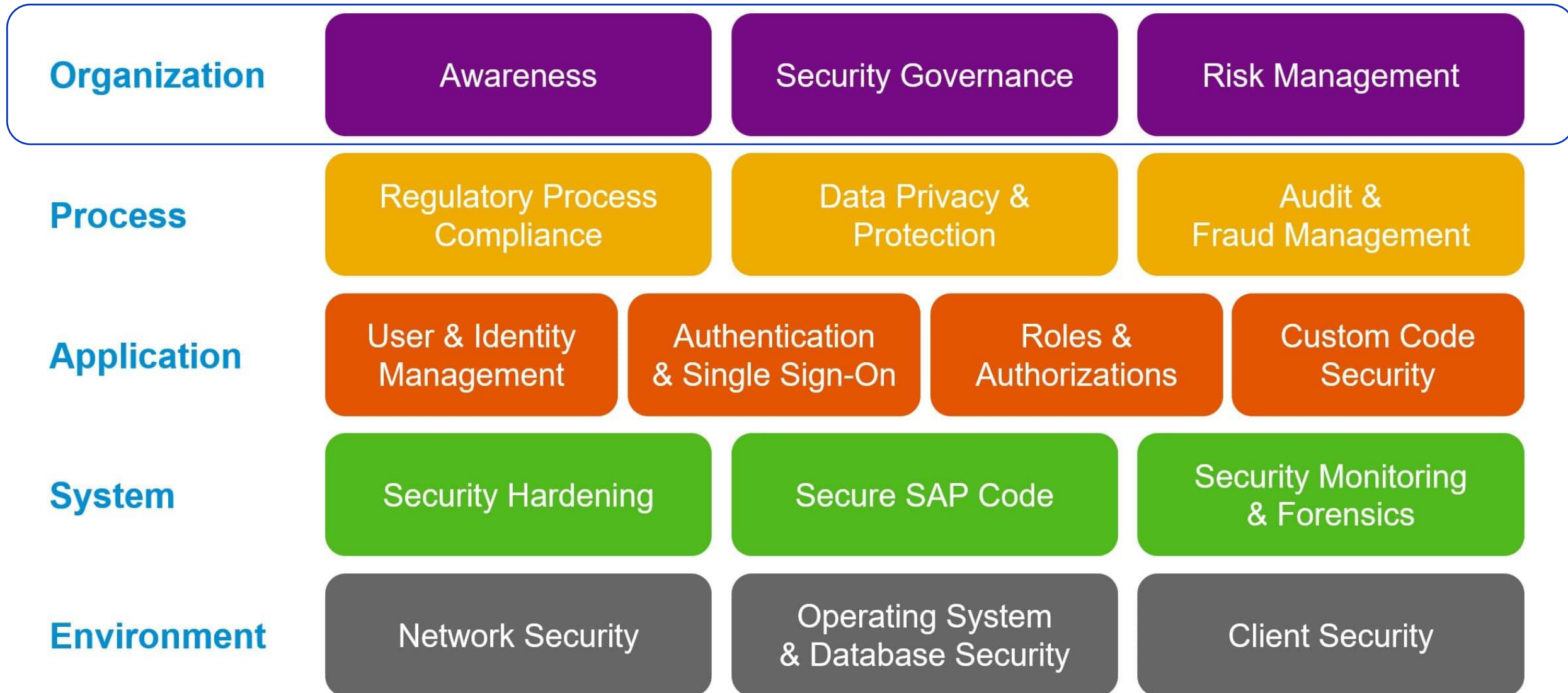


Three dimensions of IT security



Cybersecurity & Compliance

Secure Operations Map



Organization

Awareness

Security Mindset

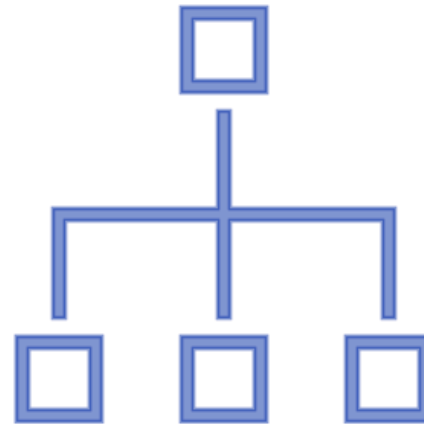


Policies Trainings Testing

Accountability

Security Governance

Risk and Control Matrix

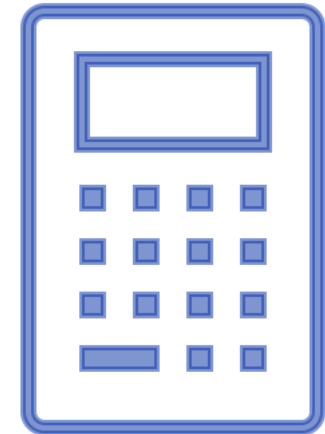


Network OS SAP

Consistency

Risk Management

Risk Framework

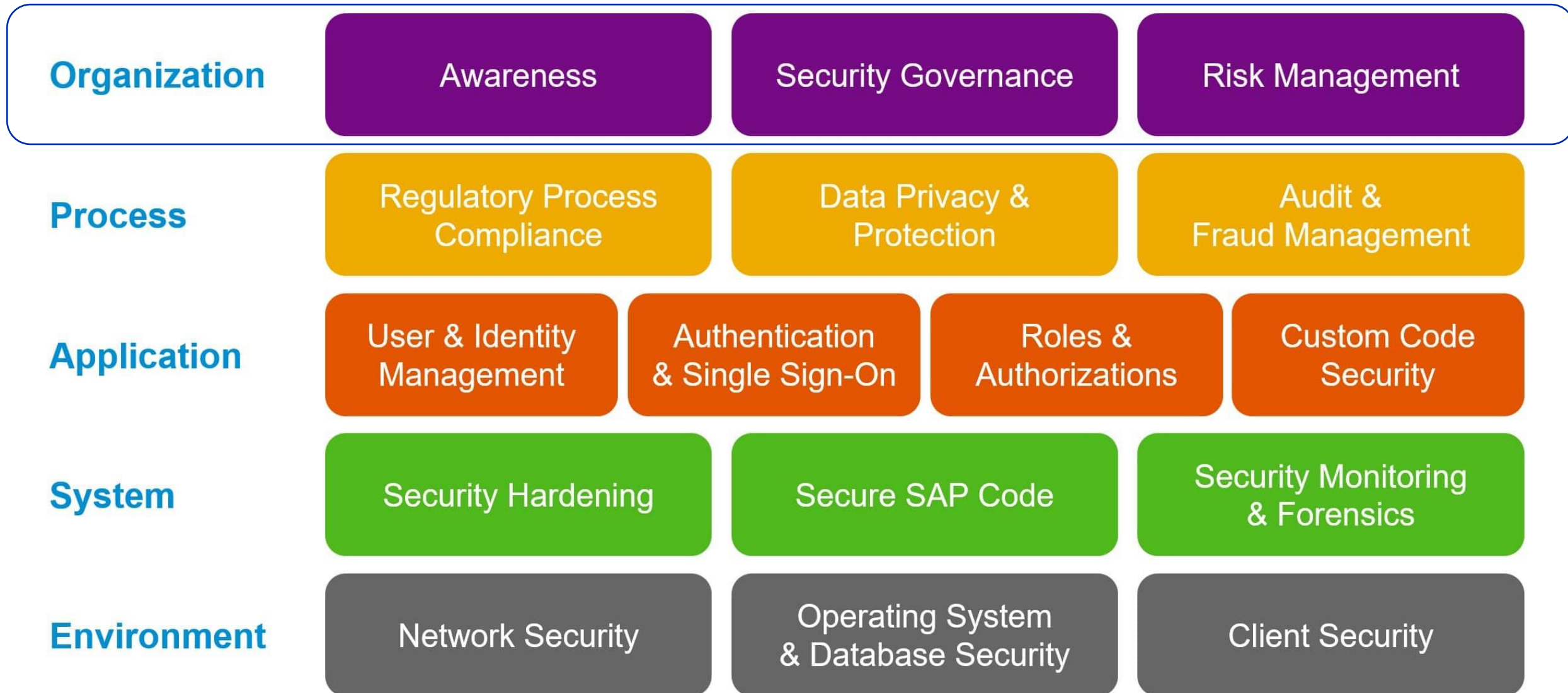


Identify Assess Mitigate

Quantification

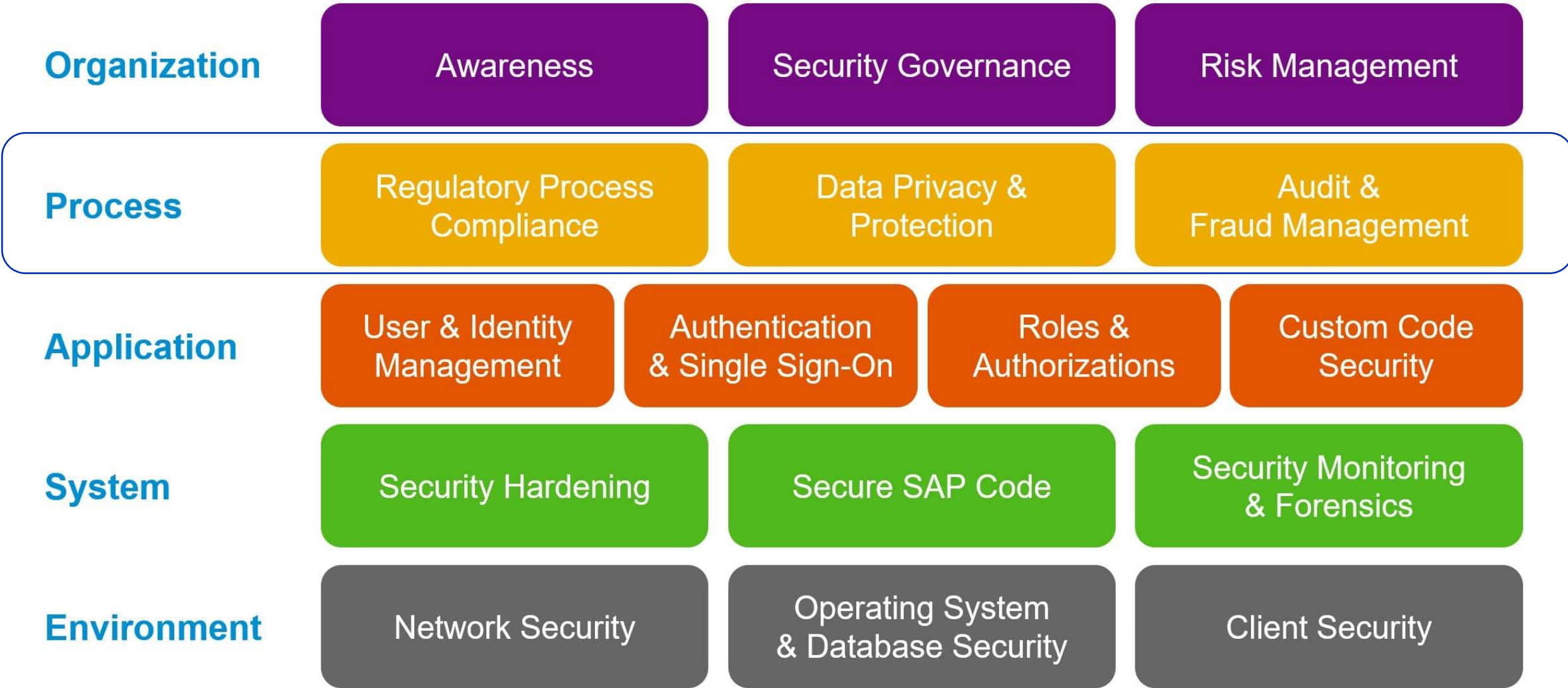
Cybersecurity & Compliance

Secure Operations Map



Cybersecurity & Compliance

Secure Operations Map



Process

Regulatory Process Compliance

Map regulations to controls



HIPAA Basel II / III SOX

Compliance

Data Privacy & Protection

Breach notification system

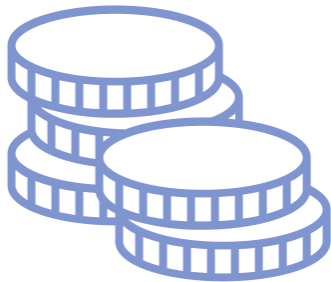


GDPR CCPA LGPD
NDB PDPB

Trust & Confidentiality

Audit & Fraud Management

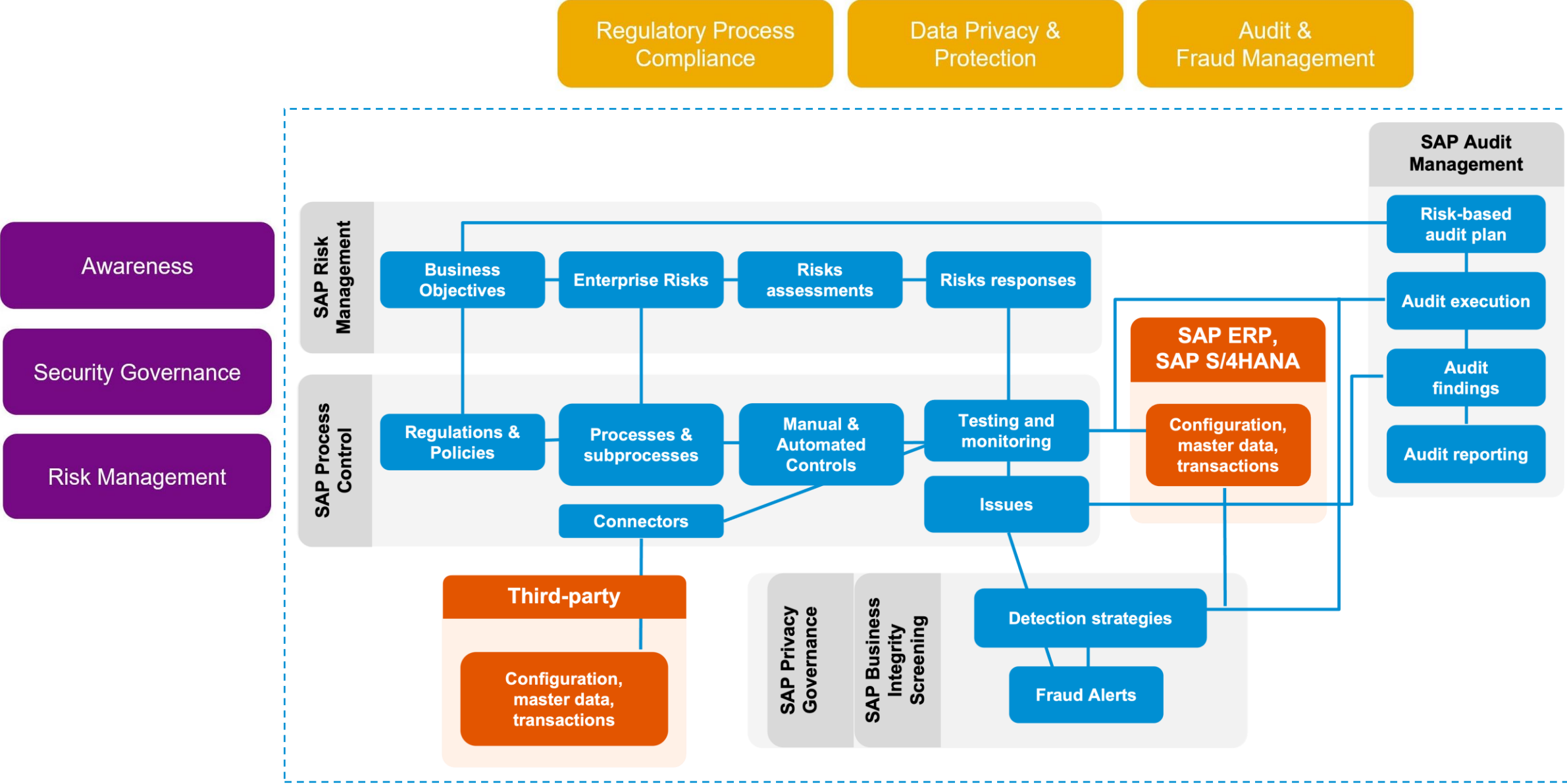
Audit Framework



Internal Audit External Audit Fraud Management

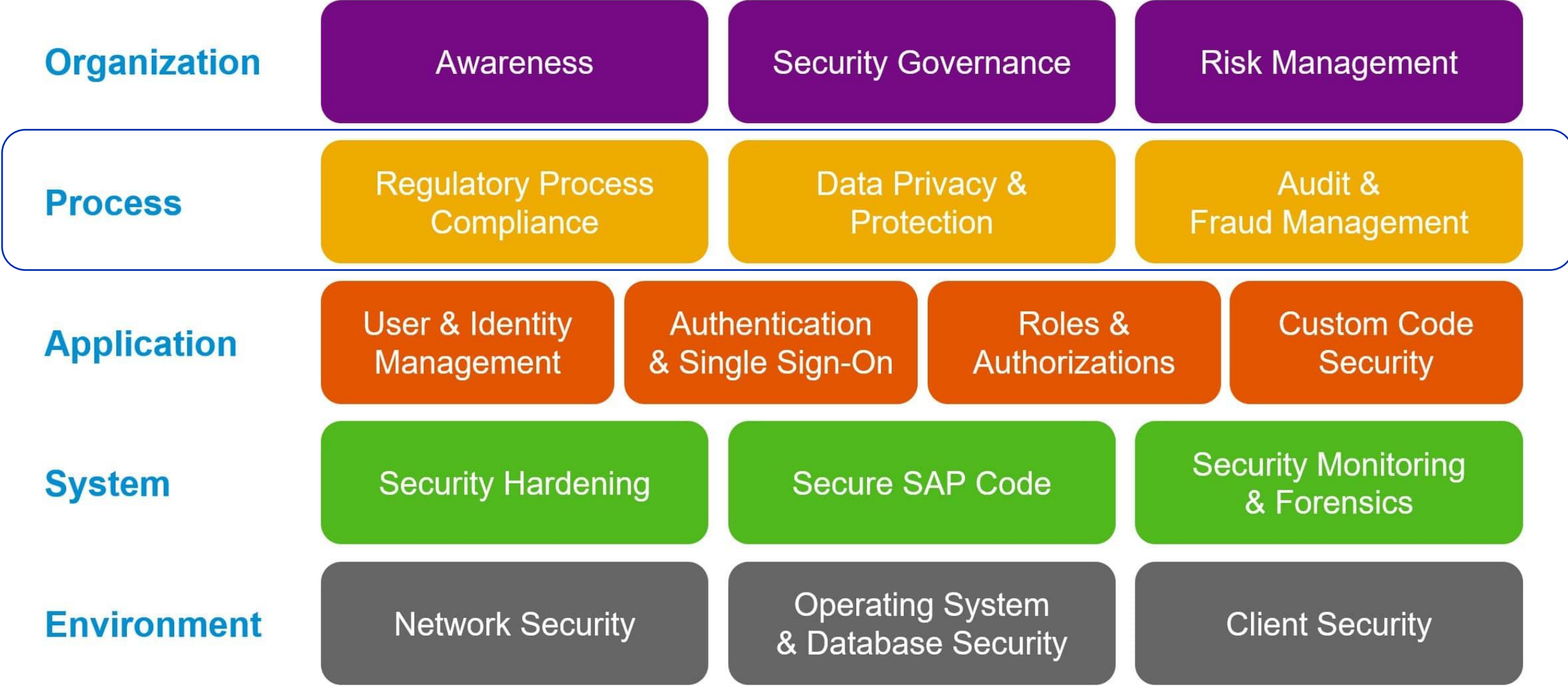
Assurance

Organization & Process



Cybersecurity & Compliance

Secure Operations Map



Cybersecurity & Compliance

Secure Operations Map

Organization

Awareness

Security Governance

Risk Management

Process

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

Security Monitoring
& Forensics

Environment

Network Security

Operating System
& Database Security

Client Security

Application

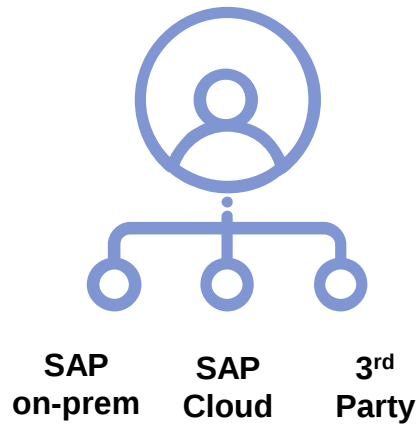
User & Identity
Management

Authentication
& Single Sign-On

Roles &
Authorizations

Custom Code
Security

Centralized & Controlled IAM



Consistency

True Identity Verification



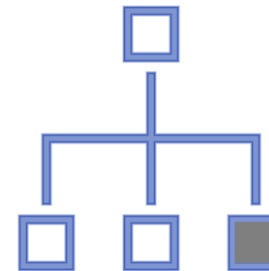
Multi Factor
Authentication

Risk-based
Authentication

Single
Sign-on

Agility + Security

Simple Role Design



Location
1

Location
2

Location
3

Harmonization

E2E Code Security



Secure
Architecture

Secure
Development

Secure Code
Scanning

Proactive Vulnerability Mngmt

Application

User & Identity Management

Authentication & Single Sign-On

Roles & Authorizations

Custom Code Security



User administration

Automate user provisioning across landscapes in a compliant manner



Risk-based and MFA

Secure authentication, with additional validations when required



Role design

Optimize role definition and streamline governance



Analyzing vulnerabilities

Detect potential code vulnerabilities across applications.



Access analysis

Detect and remediate segregation of duties and critical access risks



Single sign-on

Authenticate users and enable a secure, near-seamless experience

Product: SAP Cloud Identity Access Governance

Product: SAP Access Control

Product: SAP Code Vulnerability Analyzer



Privileged access

Centrally manage critical or temporary access

Product: SAP Cloud Identity Access Governance

Product: SAP Access Control

Product: SAP Identity Services

Product: SAP Single Sign-On (for SAP GUI)

Cybersecurity & Compliance

Secure Operations Map

Organization

Awareness

Security Governance

Risk Management

Process

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

Security Monitoring
& Forensics

Environment

Network Security

Operating System
& Database Security

Client Security

Cybersecurity & Compliance

Secure Operations Map

Organization

Awareness

Security Governance

Risk Management

Process

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

Security Monitoring
& Forensics

Environment

Network Security

Operating System
& Database Security

Client Security

Security Hardening

Centralized Security Configuration



Security
Settings
Maintenance

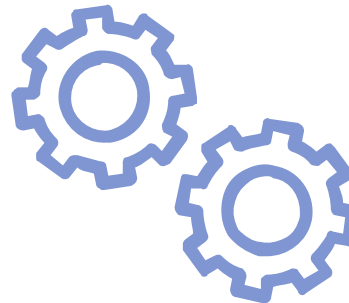
Security
Features
Activation

System
Interfaces
Security

Minimize attack surface

Secure SAP Code

Regular Security Patching



Monitor
Security
Notes

Install
Support
Packages

“Patch
Tuesday”

Keep the systems up to date

Security Monitoring & Forensics

Threat Detection Measures



24/7 System
Monitoring

Suspicious
Activity
Analysis

Anomaly
Detection

Identify and Neutralize Attacks

Security Hardening



Security Configuration

Detect potential vulnerabilities across applications, and monitor security configurations

Product: SAP Focused Run

Product: SAP Cloud Application Lifecycle Management



Data in the public cloud

Provide transparency and manage data in the public cloud

Product: SAP Data Custodian,

Product: SAP Data Custodian key management service

Secure SAP Code



Security Patching

Assess and implement recommended security updates

Product: SAP Focused Run

Product: SAP Cloud Application Lifecycle Management

Security Monitoring & Forensics



Application monitoring

Monitor core application logs for anomalous activity and relevant events

Product: SAP Enterprise Threat Detection



Data Masking and logging

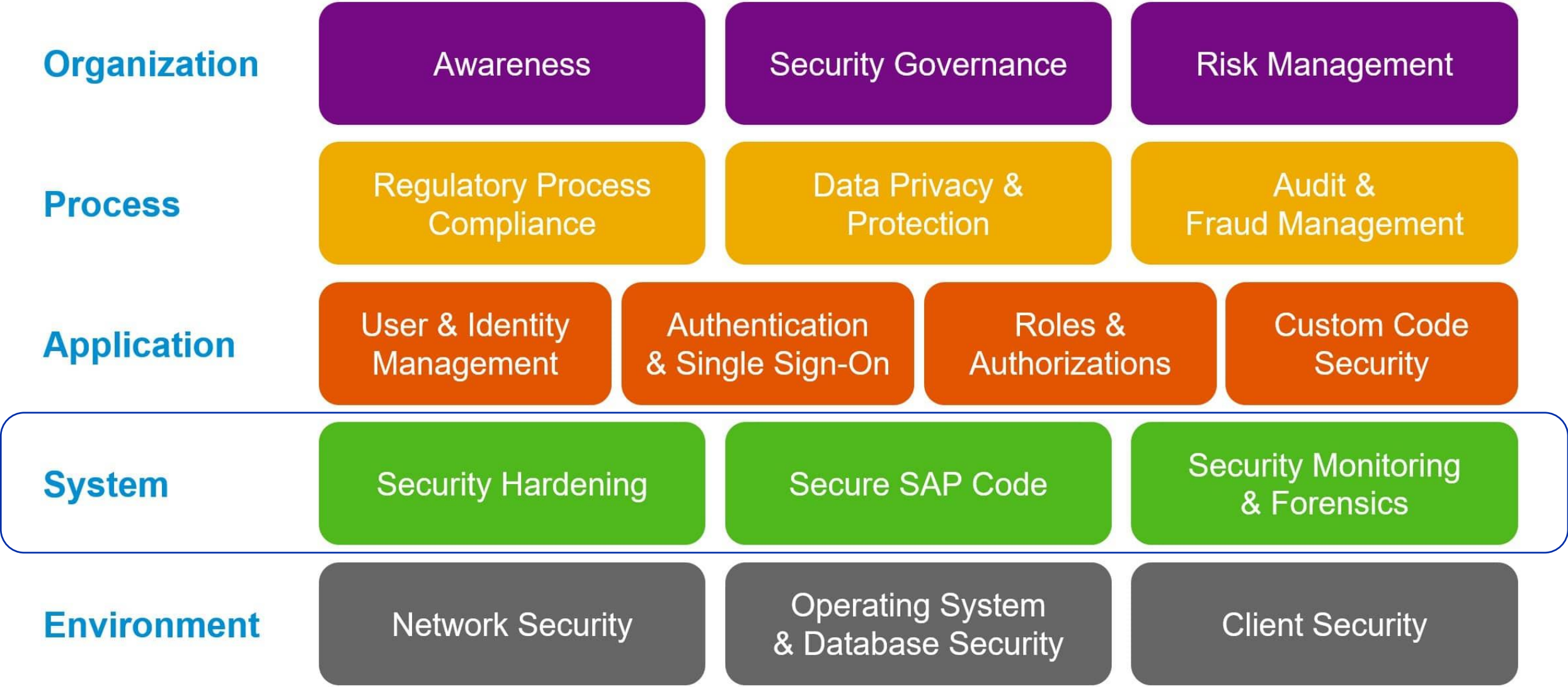
Deploy capabilities to better manage data protection and privacy

Product: UI data protection

masking, UI data protection logging

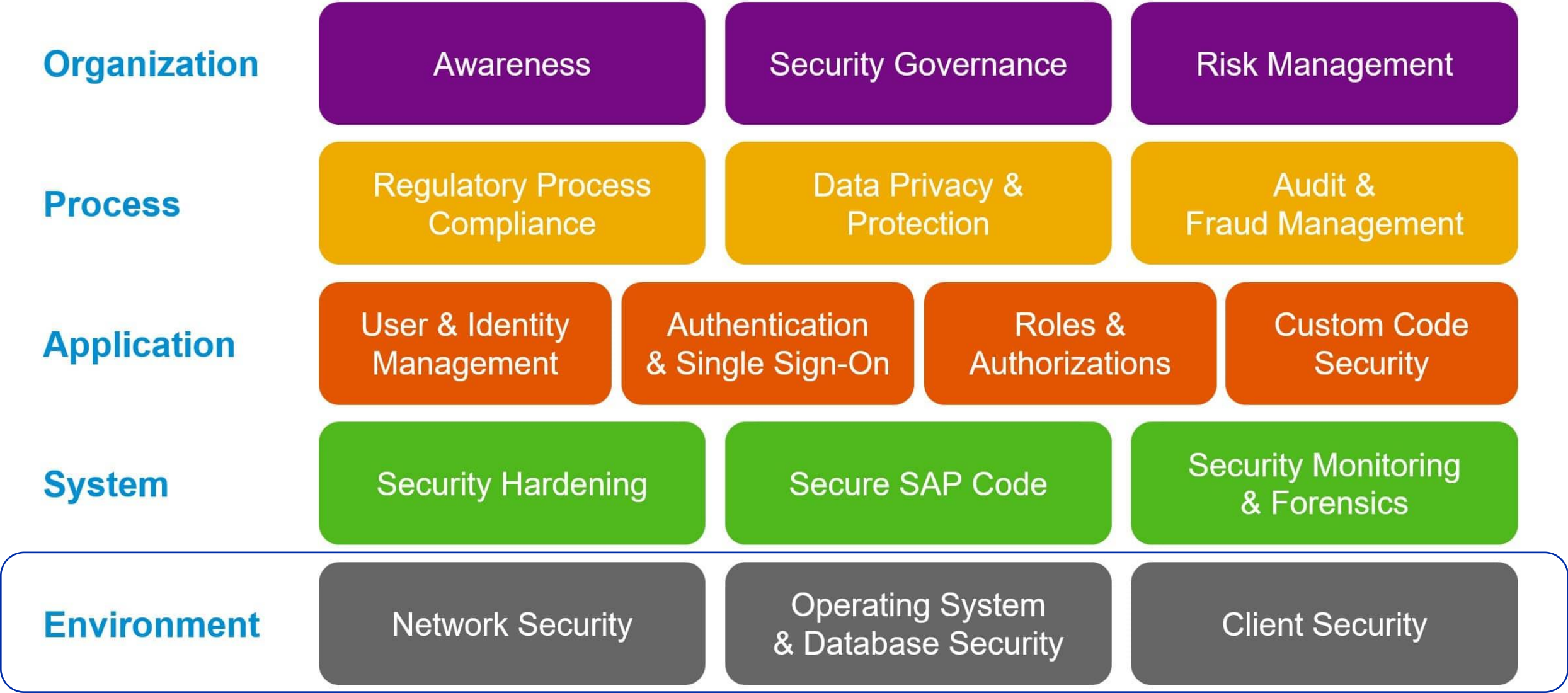
Cybersecurity & Compliance

Secure Operations Map



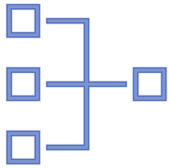
Cybersecurity & Compliance

Secure Operations Map



SAP Operations Map - Environment Layer

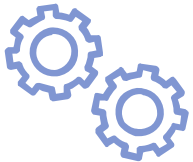
The “Environment” layer = non-SAP technical environment of SAP cloud offerings, solutions and systems.



- **Network Security:**



- **Client Security**



- **Operating System**

- Insufficient security level puts the applications running on top at risk.

Source: [SAP Secure Operations Map](#)

The role of the Operating System



- ❑ Examples of the most common attack vectors on SAP systems are getting:
 - a.) user access to SAP applications
 - b.) administrative access to SAP databases
 - c.) access to the Operating System of SAP applications & databases**
 - d.) a combination of the three above

- ❑ Operating System = critical layer of on-premises or cloud installations

- ❑ Most SAP systems nowadays run on Enterprise Linux Operating Systems

- ❑ Command-line access via a privileged Linux user + additional SAP credentials lead to full access and control of an SAP system

Breaking into an SAP Server on the OS level

- ❑ Server Operating Systems are among the most common targets for hacker attacks

- ❑ Attacks to an OS can come
 - ... from outside of a system to break into it
 - ... and/or on the system to gain more privileges (like of the root or <sid>adm user)

- ❑ Attacks may
 - exploit vulnerabilities of the Software stack
 - use stolen user credentials, e.g. from administrators

- ❑ Goal is to gain sufficient privileges to access an SAP application on the OS level (i.e. become root or <sid>adm user)

"Must have" Security Features of an Enterprise Linux OS for SAP Applications

☐ Secure Supply Chain

- Security certifications like FIPS-140-2, CC EAL 4+, STIG & more

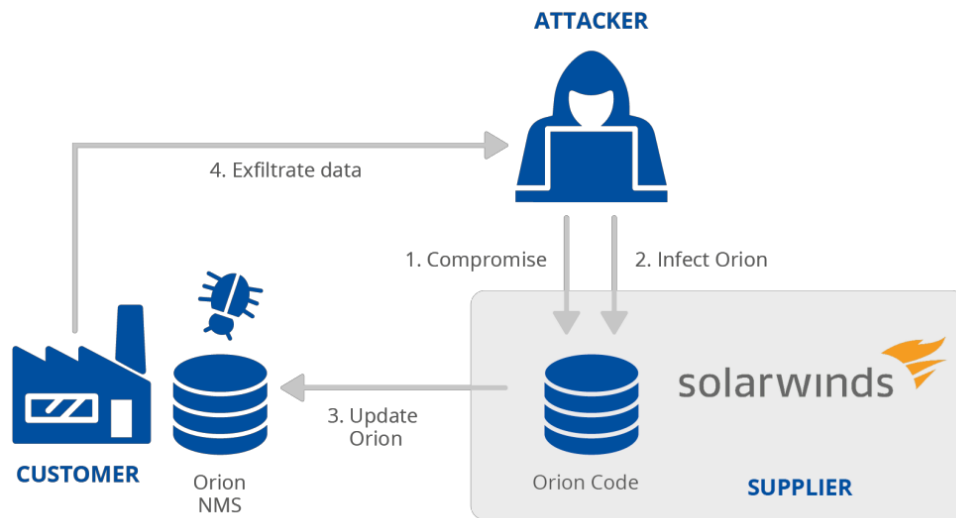
☐ Patching:

- Guarantees of security patches across the whole release cycle
- Kernel und Userspace Live Patching allowing installing security fixes without downtime.

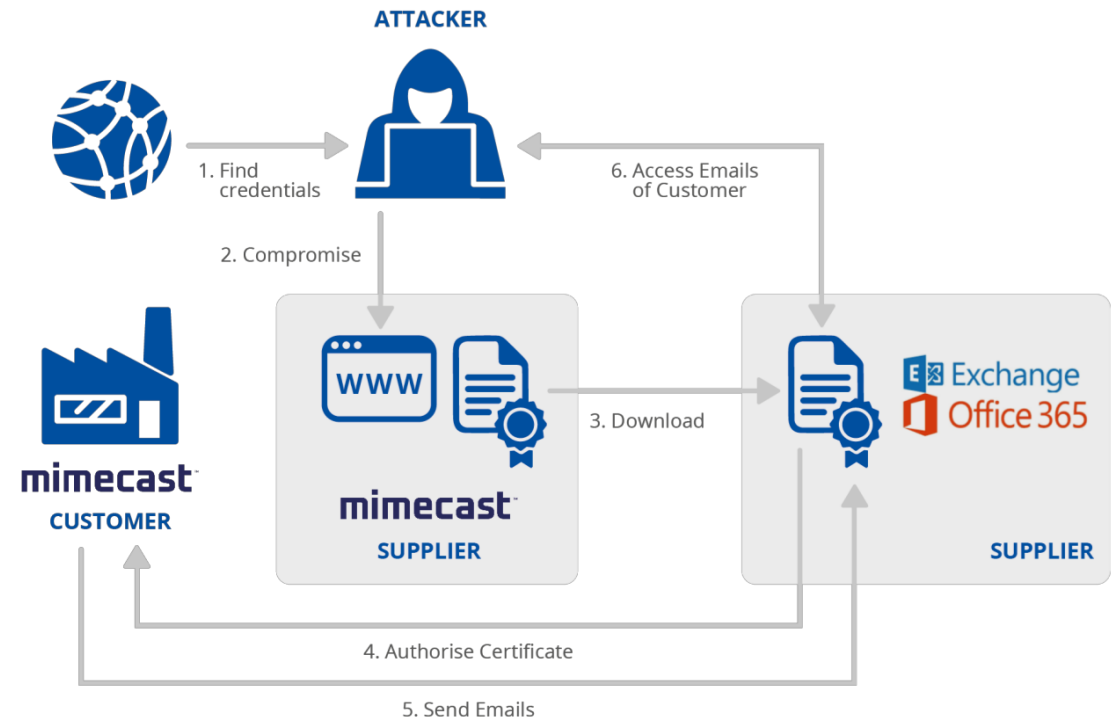
☐ OS Security Hardening for SAP & Best Practice Guides

Secure Supply Chain – Prominent Attacks

Solarwinds



Mimecast



Source: ENISA Threat Landscape for Supply Chain Attacks, Jul. 2021

Secure Supply Chain - Why Security Certifications



SUSE is making Linux “Enterprise ready”



Enterprises need to demonstrate Risk Avoidance / Compliance



One Risk is Security



Security needs to be demonstrated



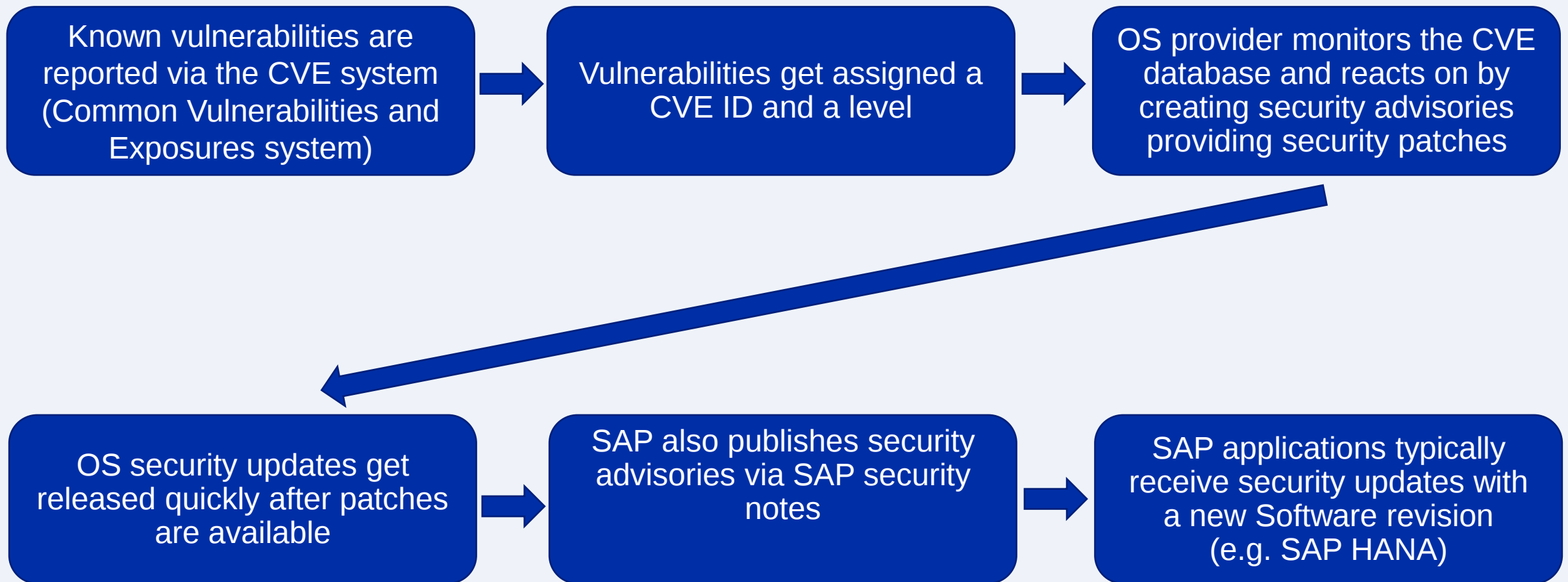
Making Security “Enterprise ready” is certifying Product/Processes



Solution: Common Criteria / EAL4+, FIPS 140-3, Google SLSA



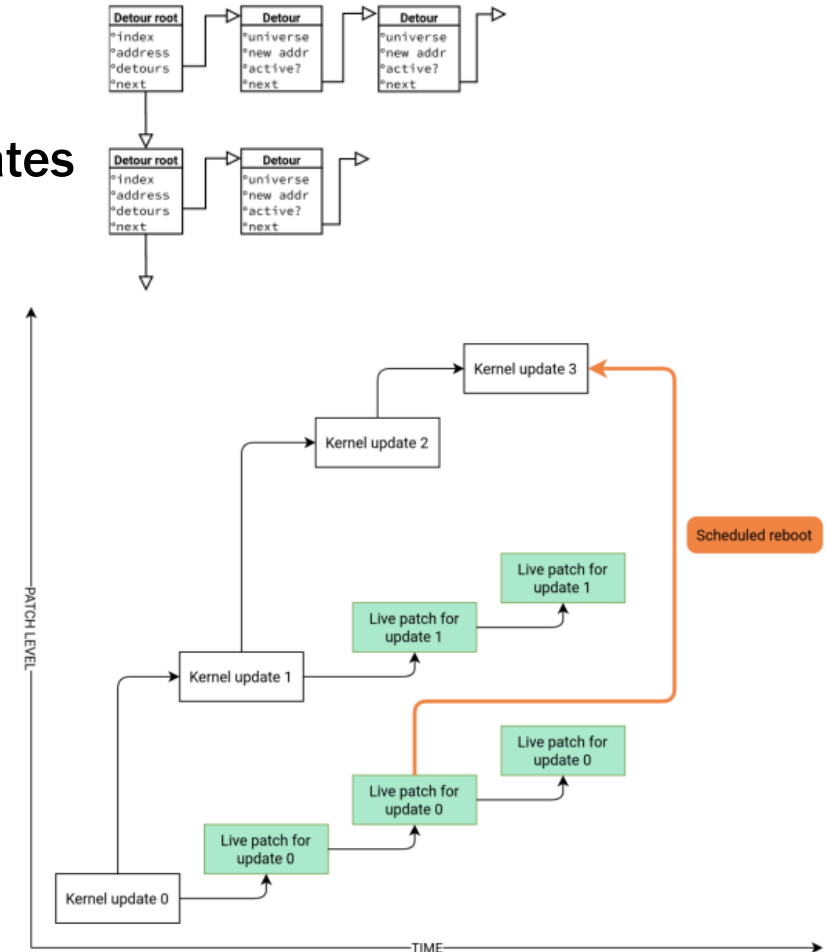
Vulnerabilities and security patches – how it works



Note: Other third-party Software (like backup or monitoring Software) might have different processes

Patching, Live Patching and Seamless Maintenance

- ❑ Security patches often require a downtime of SAP systems
- ❑ Strategies needed, to minimize the downtime during security updates
- ❑ Implement kernel & userland live patching features (apply kernel & library security fixes with no downtime)
- ❑ The SAP certified Linux OS High Availability solutions for SAP S/4HANA should support seamless maintenance procedure
- ❑ Security patches should be distributed locally, e.g. through the Linux OS Management console
- ❑ Automate Patching Process with Tools like SUSE Manager



> 95 % of all kernel issues with a CVSSv3 score of 7 or higher were fixed with Live Patching!

OS Hardening

Hardening



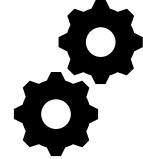
- Configuring a system for secure use.
- Limit usage of system to allowed computing

Compliance



- Fulfill legal requirements
- Follow predefined standards
- Keep Chain of Trust

Facilitation



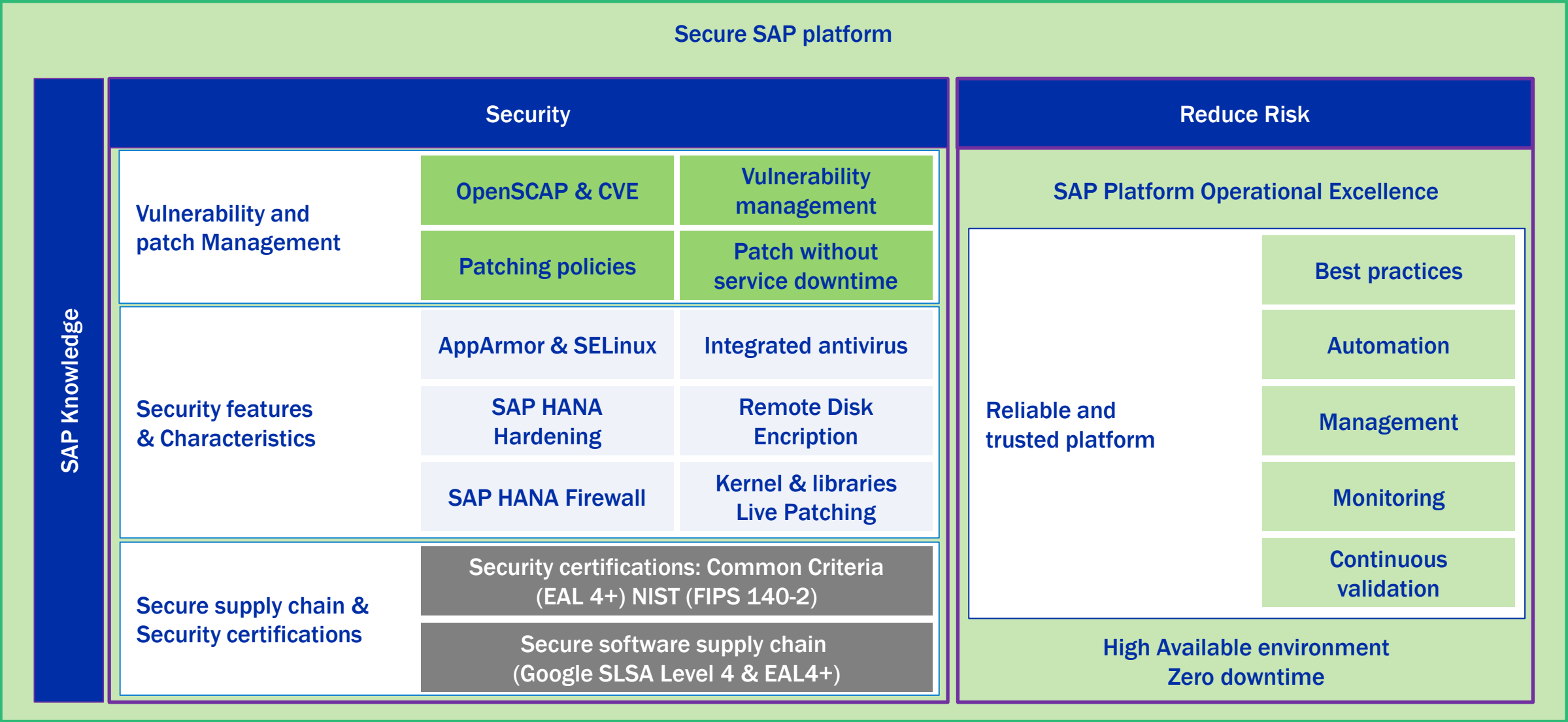
- System Setup
- Configuration
- Audit



Defense Information Systems Agency

- SLES 15 Security Technical Implementation Guide
 - 230 rules enabled upstream
 - Ansible + Shell script remediation
 - Official SUSE package: scap-security-guide

Secure SAP Platform



Security Best-Practices



IT security requires a holistic approach

The 18 Center-of-Internet-Security (CIS) Critical Security Controls



1: Inventory and Control of Enterprise Assets ●●○

2: Inventory and Control of Software Assets

3: Data Protection ●●○

4: Secure Configuration of Enterprise Assets and Software ●●○

5: Account Management ●●○

6: Access Control Management ●●○

7: Continuous Vulnerability Management ●●○

8: Audit Log Management ●●○

9: Email and Web Browser Protection ○

10: Malware Defenses ●○

11: Data Recovery ●

12: Network Infrastructure Management ●

13: Network Monitoring and Defense ●●○

14: Security Awareness and Skills Training ○

15: Service Provider Management ●●○

16: Application Software Security ●○

17: Incident Response Management

18: Penetration Testing ●●○

On-Premise vs. Cloud vs. Hybrid

● = Customer ● = Service Provider ● ● = Shared responsibility

Topic	On-Premise	IaaS	SaaS	Hybrid
Physical Security	●	●	●	● ●
Cloud Connectivity incl. Encryption	-	●	●	●
Network Security	●	● ●	●	● ●
Operating System Security	●	●	●	● ●
Application Patching	●	●	●	● ●
Account, User, Authorization Mgmt.	●	●	●	●
End-Point/Client Security	●	●	●	●
Data Encryption	●	●	●	● ●
Monitoring / Security Auditing & Logging Tools (SIEM)	●	●	● ●	● ●
User Training	●	●	●	●



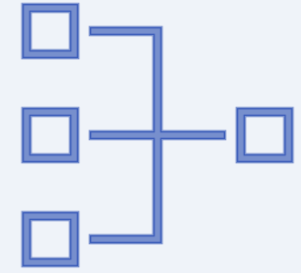
Regardless of deployment model, it's essential to have strong security practices in place.

Security Best Practices - Client



- ☐ Regular updates of OS and applications / Remove unused software / Perform regular backups
- ☐ Up to date antivirus software / Usage of firewalls
- ☐ Strong and unique passwords / Enabling multi-factor authentication
- ☐ Security awareness trainings & data protection policies
- ☐ Configure web browsers to enforce security policies
- ☐ Control external devices - policies and tools for controlling external devices, such as USB drives.
- ☐ Configuration control - standard configuration for clients, enforced through policy and automation
- ☐ Monitoring / Security Auditing & Logging Tools (SIEM)
- ☐ ...

Security Best Practices - Network



- ☐ Secure connections: direct/dedicated, VPN
- ☐ Use Firewalls / Intrusion detection and access controls, monitor and block unauthorized access.
- ☐ Implement network zoning & segmentation
- ☐ Encrypt data (in transit / at rest) – prevent interception or access by unauthorized parties.
- ☐ Conduct regular security assessments - identify and mitigate any vulnerabilities or risks.
- ☐ Use strong authentication / Keep systems, software and firmware up to date.
- ☐ ...

Security Best Practices - Operating System Level



- ☐ Keep SAP servers always up-to-date (use live-patching to reduce downtimes)
- ☐ Follow the SAP certified enterprise Linux Security Best-Practices
- ☐ Monitor changes made on the system
- ☐ Centralized Security and Event Management (SIEM) - audit functionality / forward security event logs
- ☐ Storage encryption - enable data-volume-encryption, data-redo-log encryption and backup encryption
- ☐ Only allow ssh public/private key-authentication, disallow passwords, disable login via root user
- ☐ Don't allow SAP PROD or QA systems to access the Internet, get updates from local mirrors
- ☐ Use the SAP HANA firewall to better protect against remote server attacks
- ☐ ...

Security Best Practices - Finding the right balance between security & usability

- ❑ Danger of over-engineering IT security leading to a drop in usability
- ❑ Security over-engineered environments tend to animate users to create work-arounds, examples:
 - Too frequently required password changes lead users to repeat passwords using a pattern
 - Complicated login procedures lead users to stay logged-in as long as possible



Evaluate which security mechanisms have a high impact in security vs. potential drop of usability

In doubt, decide for higher security instead of better usability

Security Best Practices - Investments in SAP Security

- ❑ Balance organizational security and security technology investments
- ❑ Obtain help from specialized externals if necessary to deal with the high complexity
- ❑ Security requires investments on a regular basis
 - Security frameworks must regularly be adapted to latest developments
 - Perform regular SAP security audits and penetration tests (e.g. yearly)
 - New SAP systems should be configured already with latest high security standards in mind
 - Open-Source Software can be a secure & cost-effective alternative commercial tools and appliances
- ❑ SLES for SAP already ships with a broad variety of security features with no additional costs

Outlook: What's important for tomorrow?

Technology

- **Dealing with security requirements on a steady increasing complexity of SAP landscapes**
- **Security for containerized SAP applications & Kubernetes**
- **Improved security concepts with a new generation of containerized Linux Operating Systems**
- **Stronger focus on security of APIs for SAP applications**
- **Automation of security related tasks**

Data

- **Confidential Computing - encryption end to end**
- **Increasing data sovereignty - sovereign clouds for mission-critical SAP systems)**

Wrap-up



Where to Find More Information

- **Operating System Security Hardening Guide for SAP HANA on SLES 15**
https://documentation.suse.com/sbp/sap/pdf/OS_Security_Hardening_Guide_for_SAP_HANA_SLES15_color_en.pdf
- **SUSE Security**
<https://www.suse.com/support/security/>
- **Maintenance of HA Clusters**
<https://www.suse.com/c/sap-hana-maintenance-suse-clusters/>
- **SAP HANA Security**
<https://www.sap.com/products/technology-platform/hana/features/security.html>
- **SAP Secure Operations Map**
https://support.sap.com/content/dam/support/en_us/library/ssp/offerings-and-programs/support-services/sap-security-optimization-services-portfolio/SAP_Secure_Operations_Map.pdf

Key Points to Take Home

- ❑ **IT Security for SAP is more important than ever due to:**
 - higher degree of digitalization
 - increasing number of directed and undirected attacks
- ❑ **Security always requires a holistic approach**
 - covering every aspect of an IT environment, technically and organizational
- ❑ **Security in the SAP space is often a shared responsibility**
 - especially in Cloud or hosting scenarios – customers should always be aware of this fact.
- ❑ **The Operating System layer of SAP Software stacks is a well-known target**
 - second ranked after breaking into SAP applications and databases
 - SLES for SAP ships with many security features already build in
- ❑ **Take advantage of Best Practices Guides like SAP Secure Operations Map or SUSE Best Practice Guides**

Thank you! Questions?



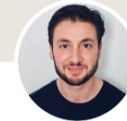
Tobias Kutning
Senior Manager Product Management SAP @
SUSE



Meet me at SAPinsider SUSE booth #1015

tobias.kutning@suse.com

<https://www.linkedin.com/in/tobias-kutning/>



Gabriele Fiata
Enterprise Risk Management & Cybersecurity



Meet me at SAPinsider SAP booth

gabriele.fiata@sap.com

<https://www.linkedin.com/in/gabrielefiata/>

Please remember to complete your session evaluation.

SAPinsider



SAPinsider.org

PO Box 982Hampstead, NH 03841
Copyright © 2023 Wellesley Information Services.
All rights reserved.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Wellesley Information Services is neither owned nor controlled by SAP SE.

SAPinsider comprises the largest and fastest growing SAP membership group worldwide, with more than 600,000 members across 205 countries.
