



# SAP NIS2 - Multi Compliance Service

Public



# Disclaimer

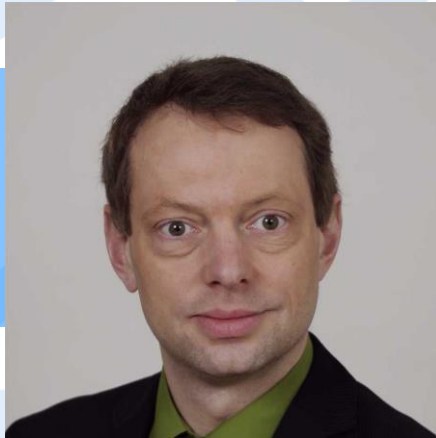
The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement 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.

# Speakers

**Michael Altmaier**



Principal Security Architect

# Agenda

- EU NIS2                      The Directive in a nutshell
- MCF                              A Framework for Multi-Compliance
- Points of View                Start for Managing Cybersecurity Compliance
- In more detail                The Assessment Point of View
- Customer Success            SAP Services for Cybersecurity Compliance

# Drivers for Managing Cybersecurity Compliance

**We aim to assist our customers in aligning their SAP security measures with regulations, widely-accepted norms, and established standards.**

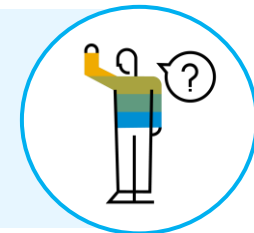
RISE or GROW with SAP and face new Cybersecurity challenges in the SAP landscape?



Impacted by new Cybersecurity regulations and must take appropriate action?



Unsure about the status of currently implemented SAP Cybersecurity measures?



Prepared for upcoming Cybersecurity compliance audits or working on existing findings?



# Implementing Compliance – The chain: Why? What? How?

WHY?

Obligations



WHAT?

Requirements




HOW?

Controls



# EU NIS2 requirements and affected industries




Effective as of 18<sup>th</sup> of October 2024:

- Registration with national authorities
- Reporting of security incidents
- Compliance with security requirements
- Regular proof of compliance (certification/audit)




**Cybersecurity Requirements:**

- Policies/guidelines
- Incident management
- Business continuity
- Supply chain security
- Training
- Asset management
- Obligation to reporting



**Strict reporting obligations:**









- Up to 24hours: Reporting of incidents
- Up to 72hours: Reporting of indicators of compromise
- Up to 1 month: Final report





**Fines:**

- Personal liability of the management board
- high fines for breaches of security measures: up to 10 Mio. Euro or 2% of global turnover

**Affected Industries since NIS1**

 Energy
  Financial market infrastructures
  Drinking water
  Digital infrastructure/networks
  Digital service providers
  Healthcare
  Transportation
  Nutrition

**Additional sectors since NIS2**

 Research
  Banking
  Space
  Chemistry
  Waste
  Post & courier services
  Waste water
  Public administration
  Industry / production
  ICT service providers

Company	# of Employees		Revenue		Balance sheet
Medium-sized	50-249	&	< 50 Mio. Euros	& / or	< 43 Mio. Euros
large	>250	&	>= 50 Mio. Euros	& / or	>= 43 Mio. Euros

\*furthermore: Companies with critical operations and public policy implications, systemic risks or cross-border impacts

# EU NIS2 minimum requirements for Cybersecurity

Facilities within the EU must implement at least the following cybersecurity measures (risk management) to protect the IT and networks of their critical services:

- Policies on risk analysis and information system security
- Prevention, detection, and handling of cyber incidents
- **Policies and procedures regarding cryptography and encryption**
- Human Resources Security
- **Access control**
- Asset management
- **Use of multi-factor authentication or continuous authentication solutions**
- Policies and procedures to assess risk management measures
- Basic cyber hygiene practices and cybersecurity training
- Use of secure voice, video, and text communication
- Use of secured emergency communication systems
- Business continuity management with backup and disaster recovery, crisis management
- Security in the supply chain, up to secure development at suppliers
- Security in the acquisition, development and maintenance of IT and network systems, incl. vulnerability management and disclosure

In the selection and implementation of measures, institutions shall use an all-hazards approach.



# MCF – A Framework for Multi-Compliance

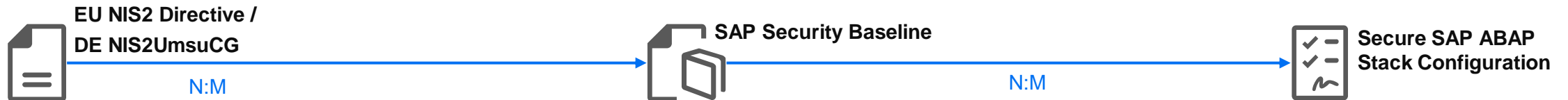
What is the relationship between  
NIS2 Directive article and ABAP profile parameter?

EU NIS2 ART. 21.2 (h) AND SNC/ENABLE = 1

# EU NIS2 Art 21.2. (h) – Direct mapping

descriptive, process-oriented, risk-focused

detailed, specific, technical, implementation-related



EU NIS2 Art. 21.2. (h)

**Policies and procedures regarding the use of cryptography and, where appropriate, encryption**

**DE NIS2UmsuCG §30 (2) Nr. 8**  
**Kryptografie und Verschlüsselung**



NETENC-A

**Encryption of ABAP**  
**Network Connections**



snc/enable = 1

snc/data\_protection/min = 3  
snc/data\_protection/max = 3  
snc/data\_protection/use = 3  
snc/accept\_insecure\_gui = U  
snc/accept\_insecure\_rfc = U

...

▪ **Direct mapping** of one regulation



# Multi Compliance Framework: Compliance & Cybersecurity Management

## Multiple Compliance Regulations

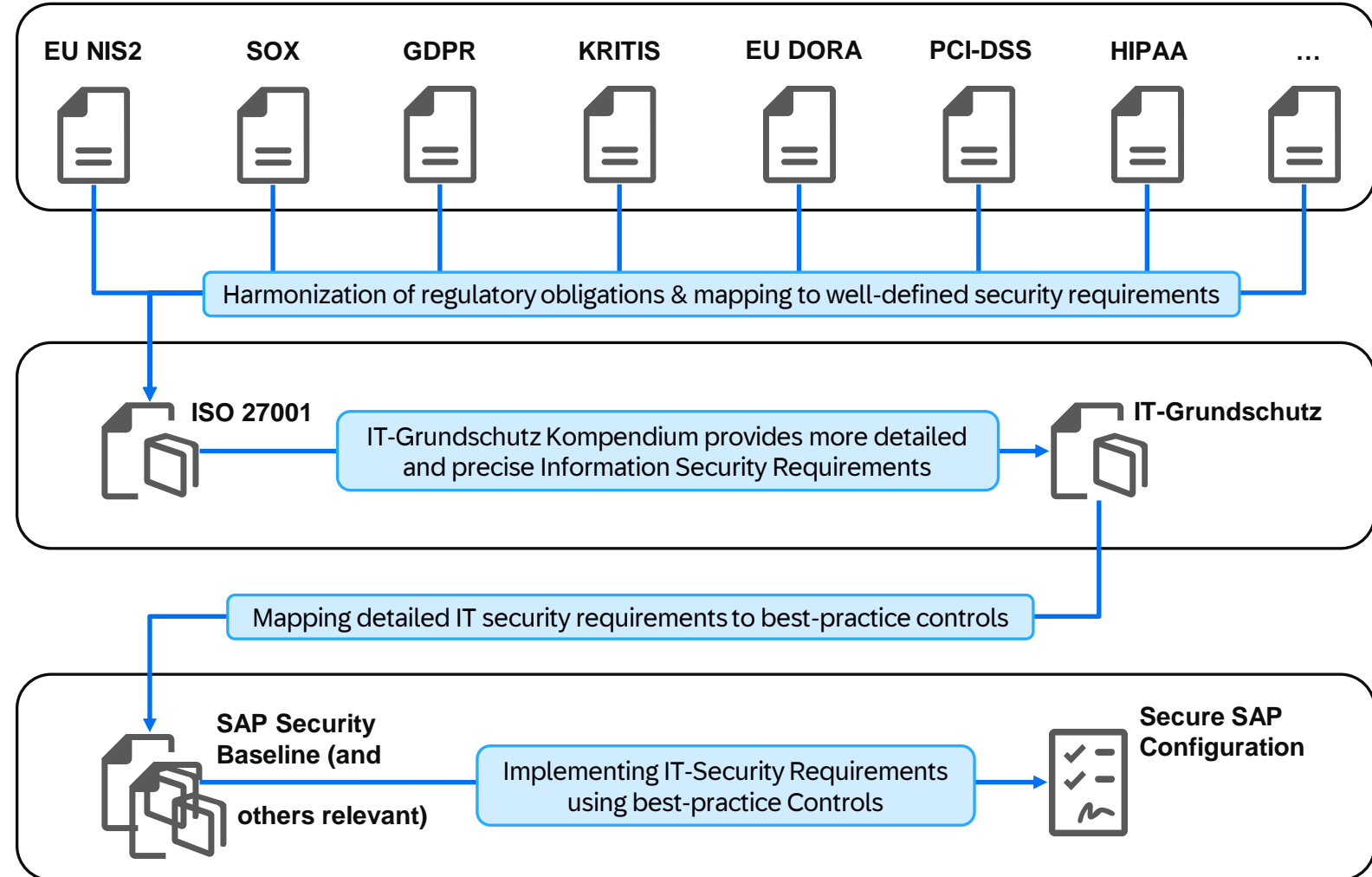
Nearly all Regulations comprise Information Security obligations

## Management of Cybersecurity Compliance

Manage Cybersecurity Compliance using well-known standards

## Operational IT Security

“Compliance View” enabled operational IT Security



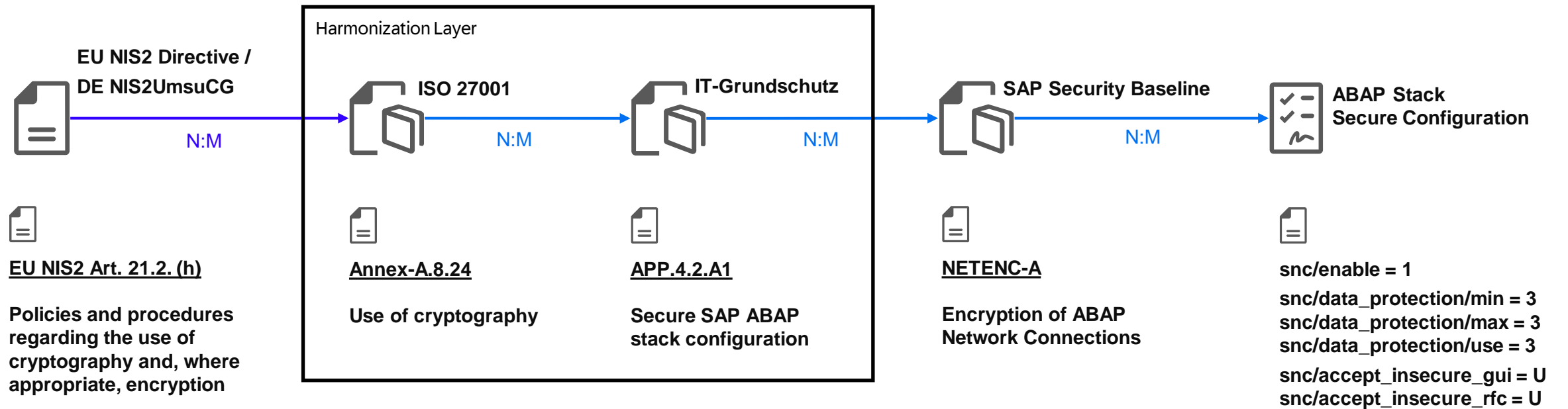
- Requirements Unification and Compliance Lifecycle Management



# The chain – from obligation to control

descriptive, process-oriented, risk-focused

detailed, specific, technical, implementation-related



**DE NIS2UmsuCG §30 (2) Nr. 8**  
Kryptografie und Verschlüsselung

SOX, GDPR, ...

Public

- Standards based MC mapping
- Including Management layer (ISMS)

# Multi Compliance Framework: Compliance & Cybersecurity Management

## Multiple Compliance Regulations

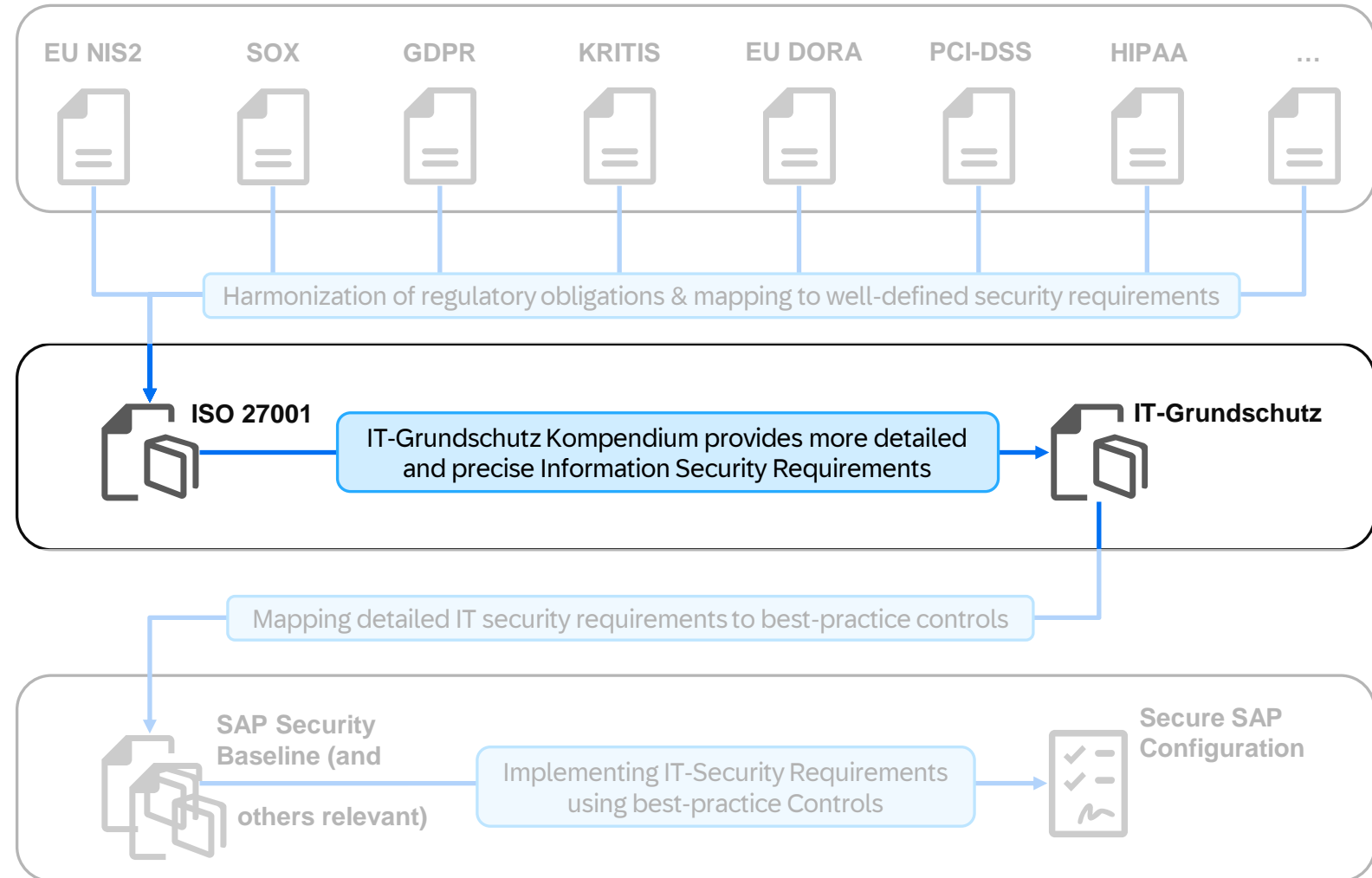
Nearly all Regulations comprise Information Security obligations

## Management of Cybersecurity Compliance

Manage Cybersecurity Compliance using well-known standards

## Operational IT Security

“Compliance View” enabled operational IT Security



- **Cybersecurity is no State, but a continuous Management Process**



# DIME - Cybersecurity Compliance & Assurance point of view

## Cybersecurity Compliance Management for SAP Landscapes

### Cybersecurity Architecture, Planning and Implementation Services

Services for a comprehensive approach on Cybersecurity Compliance



Cybersecurity Architecture



Cs Compliance and Assurance



Cybersecurity Assessment

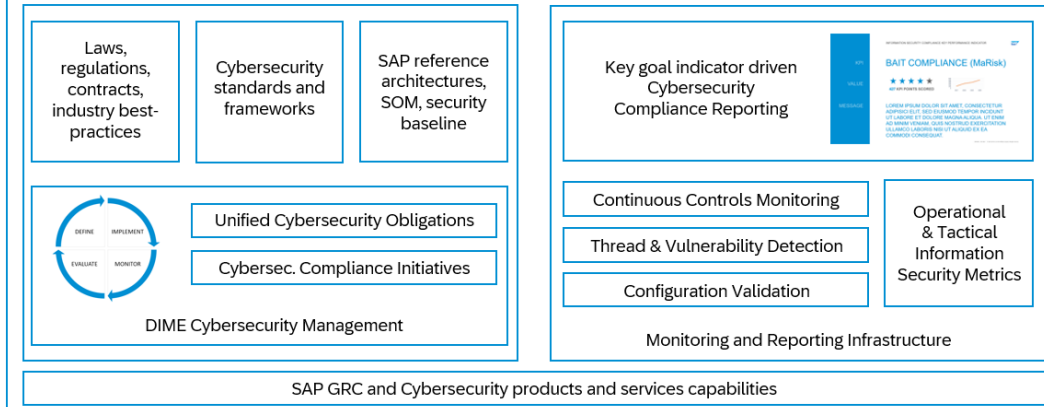
### Cybersecurity Compliance Adaption

Tailoring the Cybersecurity repository to customer landscape



ISO 27001 / IT-Grundschutz aligned repository for SAP  
Cybersecurity obligations, requirements, controls and measures

#### Cybersecurity Compliance Management and Reporting



#### SAP Cybersecurity Products and Services Capabilities

Capabilities	Services	Products
Patch Management	Cybersecurity Strategy	SAP Enterprise Thread Detection
System Hardening	Identity Access Management	SAP Focused Run
Compliant Access Management	AIRC / Infrastructure Security	SAP GRC Access Control / IAG
Identity Management	Data Protection and Privacy	SAP Cloud Identity Services
Security Incident Management	Cybersecurity Reference Architecture	SAP 3 Lines of Defense
Secure Development	Cybersecurity Implementation	SAP Code Vulnerability Analyzer

# Viewpoints on Cybersecurity Compliance



## Cybersecurity Architecture point of view

The objective to secure business processes in your SAP landscape end-to-end, leveraging all relevant capabilities of SAP's Cybersecurity and Compliance solutions and services.

---



## Cybersecurity Compliance & Assurance point of view

The need to adhere to Cybersecurity regulations, hence to rely on standards-based security and control management as well as auditing and monitoring your SAP landscape.

---



## Cybersecurity Assessment point of view

The desire for detailed insights into the Cybersecurity as-is situation, induced by uncertainty surrounding the current measures in the SAP landscape and the fear of "open flanks".



# Implementing Compliance – The chain: Why? What? How?

WHY?

Obligations




 **EU NIS2 Art. 21.2. (h)**

Policies and procedures regarding the use of cryptography and, where appropriate, encryption

WHAT?

Requirements



 **ISO 27001 Annex-A.8.24**

Use of cryptography

 **IT Grundschutz APP.4.2.A1**

Secure SAP ABAP stack configuration

HOW?

Controls



 **SAP Security Baseline NETENC-A**

Encryption of ABAP Network Connections

 **Secure SAP ABAP Stack**

```
snc/enable = 1
snc/data_protection/min = 3
snc/data_protection/max = 3
snc/data_protection/use = 3
```

...

# Viewpoints on Cybersecurity Compliance



## Cybersecurity Architecture point of view

The objective to secure business processes in your SAP landscape end-to-end, leveraging all relevant capabilities of SAP's Cybersecurity and Compliance solutions and services.

---



## Cybersecurity Compliance & Assurance point of view

The need to adhere to Cybersecurity regulations, hence to rely on standards-based security and control management as well as auditing and monitoring your SAP landscape.

---



## Cybersecurity Assessment point of view

The desire for detailed insights into the Cybersecurity as-is situation, induced by uncertainty surrounding the current measures in the SAP landscape and the fear of "open flanks".

# Security Architecture: Example



## SAP Access Control

- Identity Management
- Authorization Management



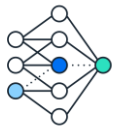
## SAP FocusedRun

- Configuration Management



## SAP Maintenance Planer

- Patch Management



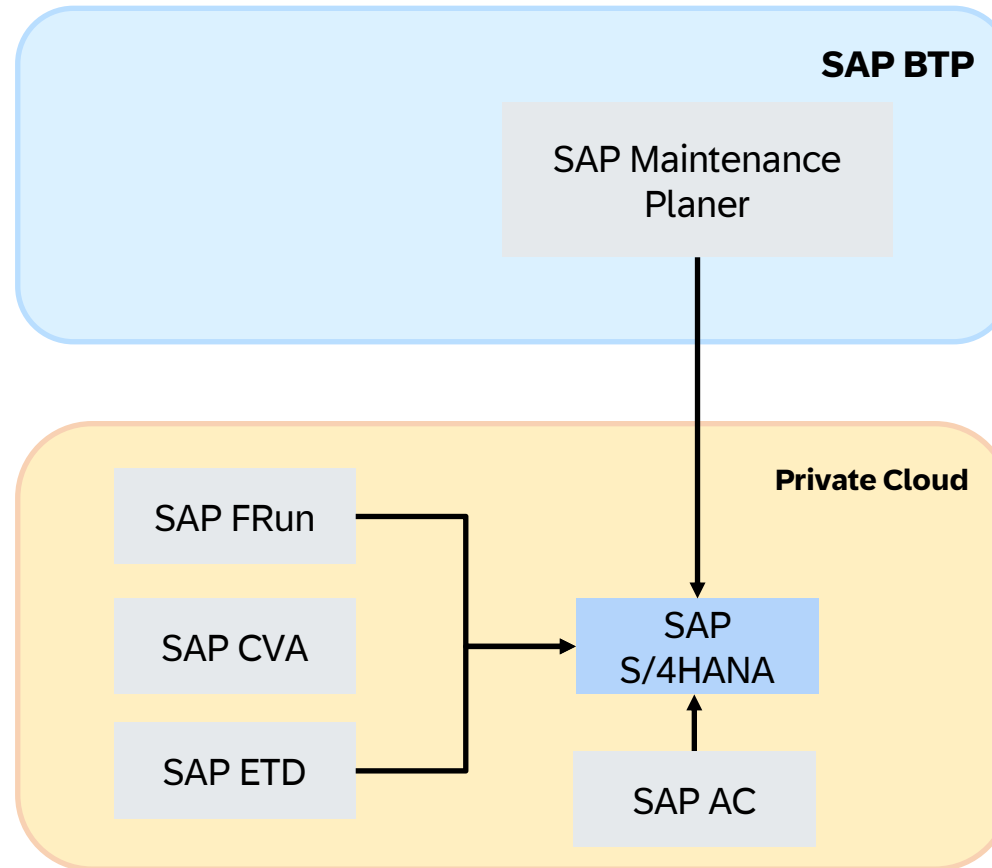
## SAP Code Vulnerability Analyzer

- Secure Development



## SAP Enterprise Thread Detection

- Security information & event management



<https://discovery-center.cloud.sap/index.html#/refArchCatalog/>

## Customer Individual Architecture Discussions:

- Cloud ALM vs. FRUN?
- SAP IAG vs. Access Controls?
- Move to ETD Cloud Edition?
- CVA OnPrem or via ABAP Cloud Platform?
- How to cover non-ABAP code?
- How to integrate all security telemetry?
- Central Reporting of findings into incident management
- How to report identified risks?

# Viewpoints on Cybersecurity Compliance



## Cybersecurity Architecture point of view

The objective to secure business processes in your SAP landscape end-to-end, leveraging all relevant capabilities of SAP's Cybersecurity and Compliance solutions and services.

---



## Cybersecurity Compliance & Assurance point of view

The need to adhere to Cybersecurity regulations, hence to rely on standards-based security and control management as well as auditing and monitoring your SAP landscape.

---



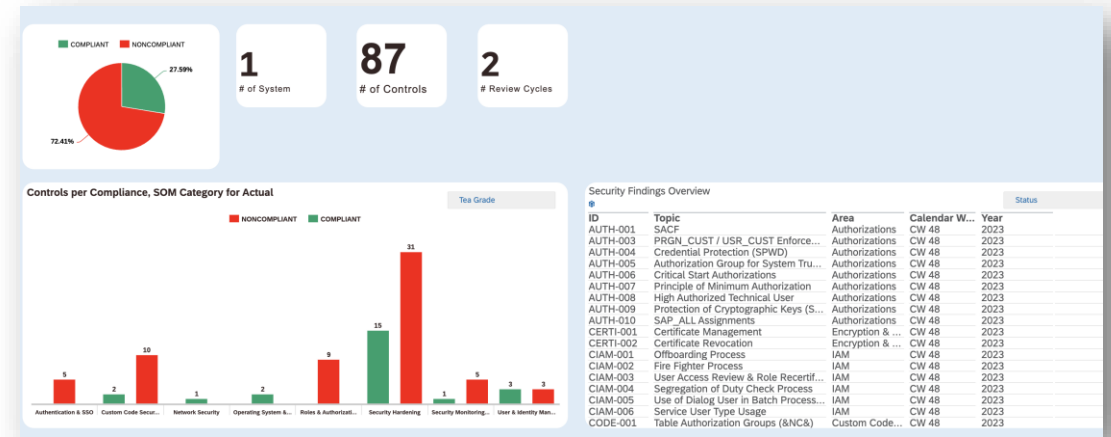
## Cybersecurity Assessment point of view

The desire for detailed insights into the Cybersecurity as-is situation, induced by uncertainty surrounding the current measures in the SAP landscape and the fear of "open flanks".

In more detail – The Assessment Point of View

# What does “Assessment Point of View” mean?

- The security assessment is an essential **comprehensive evaluation** of the security of an organization’s SAP system or landscape to identify vulnerabilities, misconfigurations, and risks.
- It is a service delivery which will be executed within 12-15 service days.
- The target is to cover all security aspects in a way, that an organization gets the transparency of its SAP systems, security strengths and weaknesses.
- It will enable the organization to implement effective measures to protect its assets and ensure the continuity of its business operations.



**Overview** Details

1 Filter

ID	Finding	Area	Calendar W...	Year	Severity	Count
CODE-010	Custom Code Security	CW 48	2023	MEDIUM	1	
CODE-011	Custom Code Security	CW 48	2023	MEDIUM	1	
CODE-012	Custom Code Security	CW 48	2023	MEDIUM	1	
INFR-001	Infrastructure & Network	CW 48	2023	OK	1	
OSSC-001	OS Security	CW 48	2023	OK	1	
OSSC-002	DB Security	CW 48	2023	OK	1	

1 Filter

ID	Finding
AUTH-001	(No Value)
AUTH-003	(No Value)
AUTH-004	(No Value)
AUTH-004	(No Value)
AUTH-005	(No Value)
AUTH-005	(No Value)

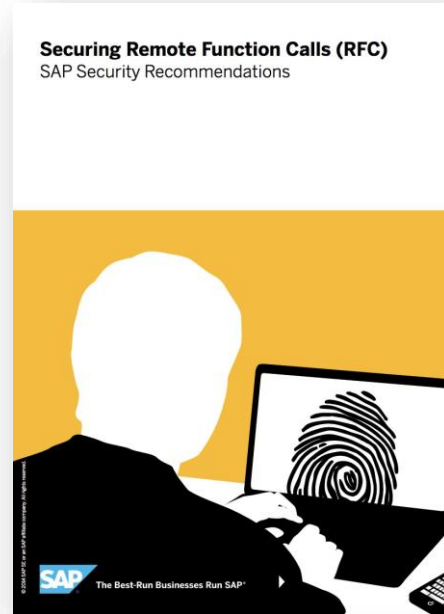
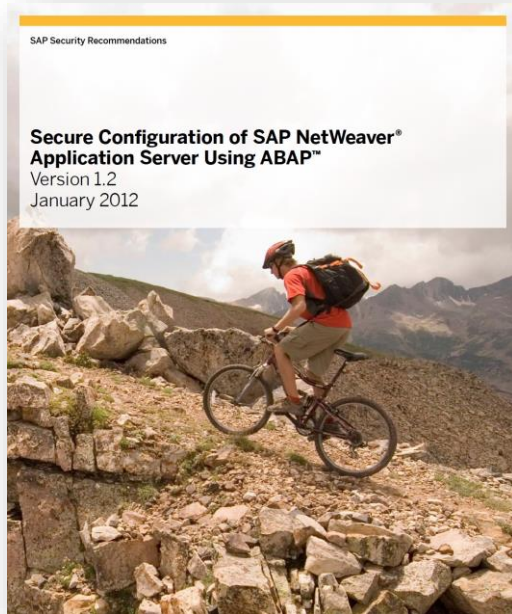
Recommended Notes

1 Filter

ID	Security Notes	Count
AUTH-001	(No Value)	1
AUTH-003	(No Value)	1
AUTH-004	(No Value)	1
AUTH-005	(No Value)	1
AUTH-006	(No Value)	1

# What is the Foundation of the Security Assessment?

- The assessment's understanding is to consider all security recommendations which are available by SAP or external security resources.
- The target is to have an agile approach where content is permanently extended and improved.



The cover features a close-up photograph of a metal door handle with a red keychain. The text below the image reads 'SAP Security Baseline Template' and 'Version 1.9'. Below this is a table showing the structure of the template based on the SAP Secure Operations Map.

The structure of the template is based on the SAP Secure Operations Map:

Security Compliance	Security Governance	Audit	Cloud Security	Emergency Concept
Secure Operation	Users and Authorizations	Authentication and Single Sign-On	Support Security	Security Review and Monitoring
Secure Setup	Secure Configuration	Communication Security	Data Security	
Secure Code	Security Maintenance of SAP Code		Custom Code Security	
Infrastructure Security	Network Security	Operating System and Database Security	Frontend Security	



Security Recommendations

Hide/Show Columns | Download Data

Component	Priority	Secure Operations Map	Title	Default Setting or Behavior	Recommendation
SAP Destination service	Recommended	Authentication & Single Sign-On	Strong Authentication	HTTP Destinations: OAuth SAML Bearer Assertion Authentication is used to implement identity propagation for interactive user sessions.	If the SystemUser was maintained for test purposes and transported to the production system, make sure that the attribute isn't maintained. This setting has been deprecated and will be removed. Use ClientCertificateAuthentication instead.

# What are the Scope Elements of the Security Assessment?

This overview shows from each scope element examples of the relevant deliverables.

## Secure Configuration

Parameter Evaluation

Key and certificate Management

Attack Surface Reduction

RFC Protection

## Infrastructure

Design & Architecture

Network Segmentation

Encryption Strategies

Web Dispatcher Setup

## Code Security

Custom Code Vulnerabilities

Custom Code Quality Management

3<sup>rd</sup> Party Code Security

ABAP Code Principles

## Web Security

Attack Surface Reduction

Trusted Network Zones & Clickjacking

Encryption Enforcements

Secure Web Integration

## Patch Management

HotNews & Prio High Security Notes

Patch Management Strategy

Service Pack Strategy

DB, OS, Host Agent Validation

## Cyber Security Strategy

Logging & Monitoring Strategy

Detection and Recovery Processes

Forensic Strategy

Business Process Threat Detection

## Authorization Principles

Design & Concepts

Critical Authorizations & Combinations

Creation and Maintenance Process

Special Access & Recertification

## Authentication & Single Sign-On

Password Security

Single Sign-On Strategy

Hash Protection

Multi-Factor Authentication

## Integration Security

Secure Integration Strategy

RFC and Web Service Communication

Zero Trust Strategy

External Access Strategy

## Cloud Strategy

Cloud Integration

Baseline configuration

Cloud configuration validation

Cloud Application Lifecycle

## Security Processes

Threat Management Processes

Identity and Access Management

Vulnerability Management Process

Central Monitoring & Configuration validation

## Identity & Access Management

Provisioning Strategy

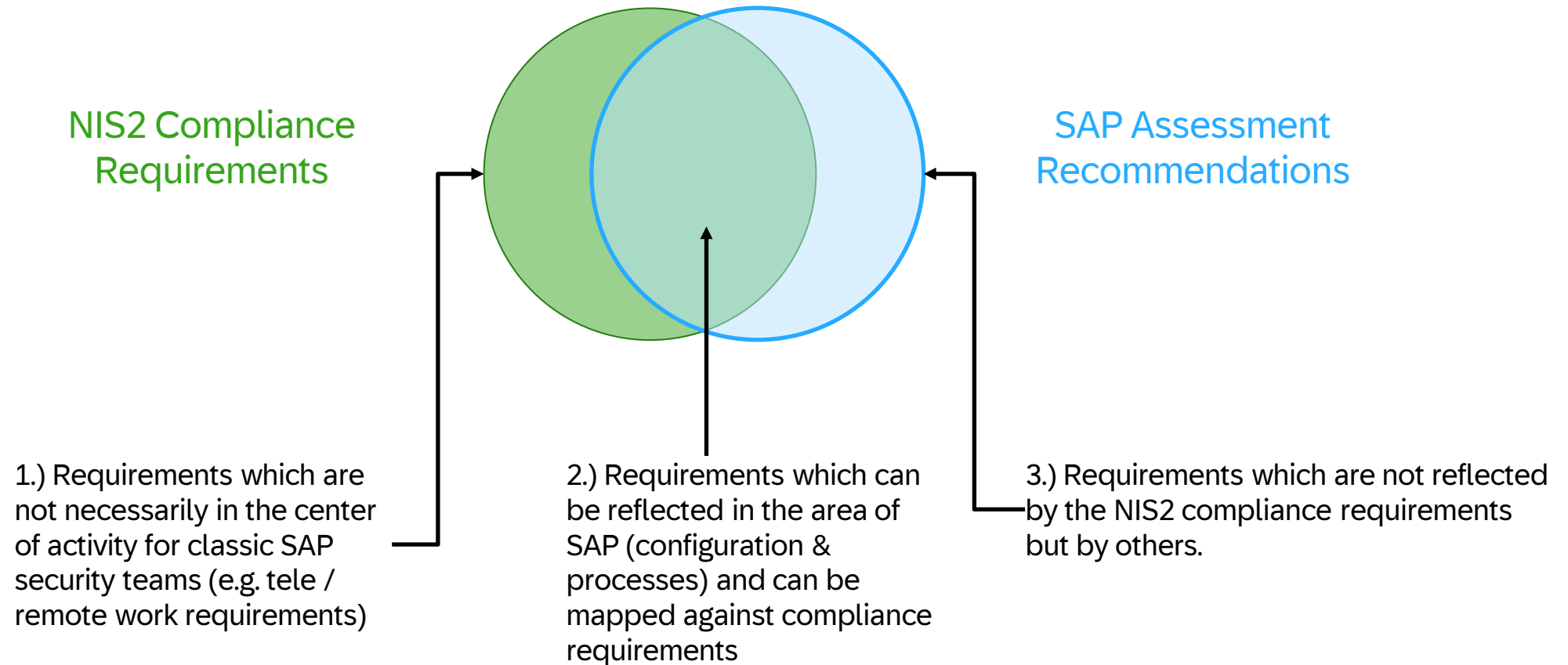
Compliant User Management

Administration Concepts



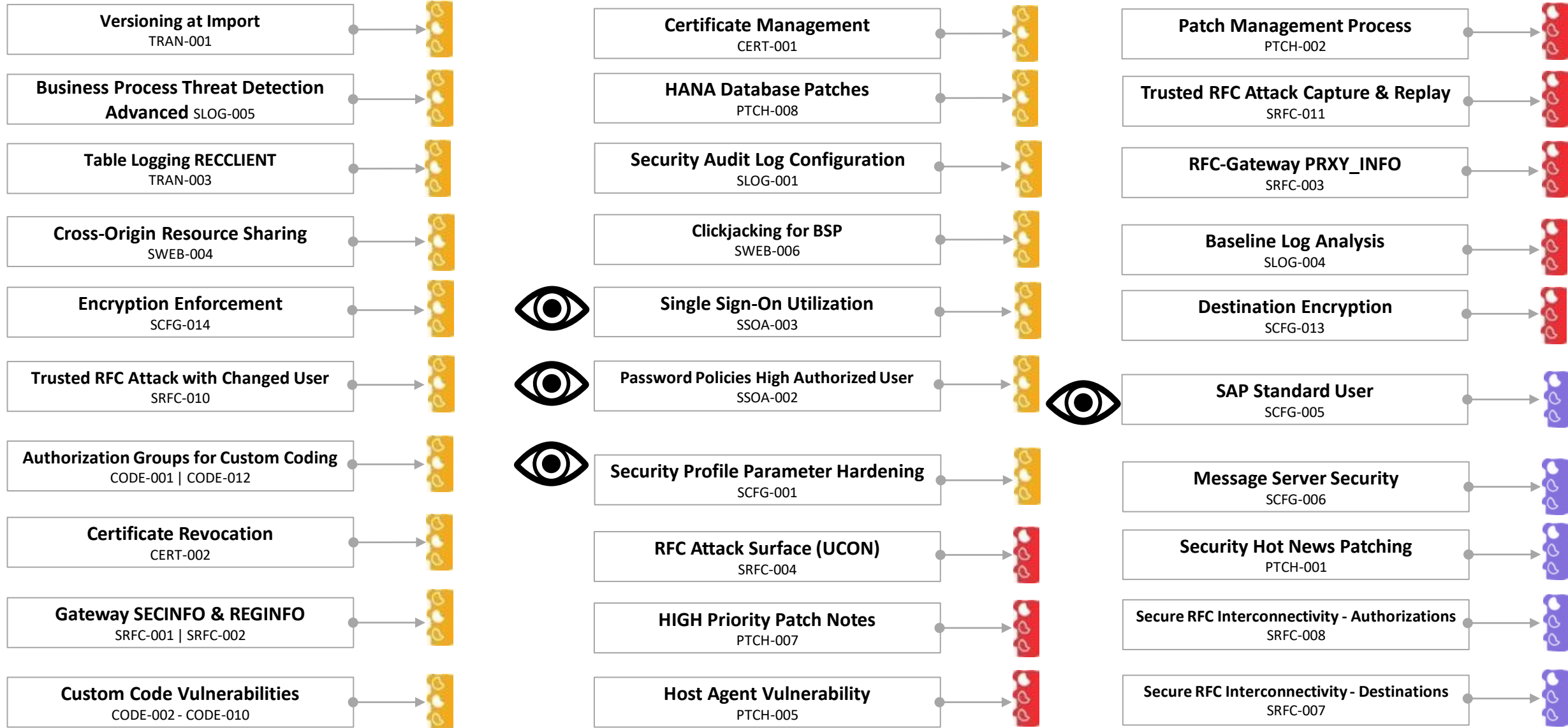
# Customer´s Security Requirements

- **TARGET:** With the Cybersecurity and Compliance Management Service we are bringing together SAP´s recommendations with the compliance requirements and additional customer requirements.



# SAP Security Review Service Extract

## Overview Secure Environment & System



# SCFG-001 | Profile Parameter Hardening



Baseline	Parameter	Value As-Is	Value To-Be	Compliance	
0	ICM05	icm/security_log	LOGFILE=/usr/sap/GE0/D01/log/dev_icm_sec-%y-%m-...	LOGFILE=access_sec_%y-%m,LEVEL=3,MAXSIZEKB=5000...	Not Compliant
1	ICM08	is/HTTP/show_detailed_errors	FALSE	FALSE	Compliant
2	ICM10	icm/trace_secured_data	FALSE	FALSE	Compliant
3	ICM11	icm/accept_remote_trace_level	0	FALSE	Compliant
4	ICM13	ssl/ciphersuites	135:PFS:HIGH::EC_P256:EC_HIGH	550:PFS:HIGH:TLS_FALLBACK_SCSV::EC_HIGH+EC_OPT	Not Compliant
5	ICM14	ssl/client_ciphersuites	150:PFS:HIGH::EC_P256:EC_HIGH	550:PFS:HIGH:TLS_FALLBACK_SCSV::EC_HIGH+EC_OPT	Not Compliant
6	ICM15	csi/enable	1	1	Compliant
7	ICM24	icm/HTTPS/client_sni_enabled	TRUE	TRUE	Compliant
8	RFCC6	auth/rfc_authority_check	6	6	Compliant
9	RFCC7	ucon/rfc/active	1	1	Compliant
10	RFCC8	rfc/selftrust	1	0	Not Compliant
11	RFCC10	rfc/reject_expired_passwd	1	1	Compliant
12	RFCC11	icm/accept_remote_trace_level	0	0	Compliant
13	RFCC12	sec/ral_enabled_for_rfc	0	1	Not Compliant
14	SS05	service/protectedwebmethods	SDEFAULT	SDEFAULT	Compliant
15	SAPGUI01	sapgui/user_scripting	FALSE	FALSE	Compliant
16	SAPGUI02	sapgui/user_scripting_per_user	FALSE	TRUE	OK
17	SAPGUI03	sapgui/user_scripting_disable_recording	FALSE	FALSE	Compliant
18	ETD01	dtd_event_sender/enable	off	on	OK
19	PPA1	login/min_password_diff	3	2	Compliant
20	PPA2	login/min_password_digits	1	1	Compliant
21	PPA3	login/min_password_lng	8	8	Compliant
22	PPA4	login/min_password_letters	1	1	Compliant
23	PPA5	login/min_password_lowercase	1	1	Compliant
24	PPA6	login/min_password_uppercase	1	1	Compliant
25	PPA7	login/min_password_specials	0	1	Not Compliant
26	PPA8	login/password_compliance_to_current_policy	0	1	Not Compliant
27	PPA10	login/password_downwards_compatibility	0	0	Compliant
28	PPA11	login/failed_user_auto_unlock	0	0	Compliant
29	PPA12	login/fails_to_user_lock	3	6	Compliant
30	PPA13	login/password_change_waittime	1	1	Compliant
31	PPA14	login/password_expiration_time	90	90	Compliant
32	PPA15	login/password_history_size	15	5	Compliant
33	PPA16	login/password_max_idle_initial	14	14	Compliant
34	PPA17	login/password_max_idle_productive	0	91	Not Compliant
35	PPA19	login/password_hash_algorithm	encoding=RFC2307,algorithm=ISSHA-1,iterations...	encoding=RFC2307,algorithm=ISSHA-512,iteration...	Not Compliant
36	PPA20	login/show_detailed_errors	0	0	Compliant
37	PPA21	login/disable_cplic	0	1	Not Compliant
38	PPA22	login/fails_to_session_end	3	3	Compliant
39	SSOA1	login/ticket_expiration_time	08:00	8	Compliant
40	SSOA2	login/ticket_only_by_https	1	1	Compliant
41	SSOA3	login/ticket_only_to_host	1	1	Compliant
42	SSOA4	login/create_sso2_ticket	3	1	Not Compliant
43	SSOA5	login/accept_sso2_ticket	1	1	Compliant
44	OPPA1	rdisp/accept_remote_trace_level	0	0	Compliant
45	OPPA2	rec/client	OFF	ALL	Not Compliant
46	SAL1	rsau/enable	1	1	Compliant
47	SAL3	rsau/user_selection	1	1	Compliant
48	SAL4	rsau/integrity	1	1	Compliant
49	SAL14	rsau/log_peer_address	0	1	Not Compliant
50	SSC1	system/secure_communication	ON	ON	Compliant

Baseline	Parameter	Value As-Is	Value To-Be	Compliance	
51	RGS4	gw/reg_no_conn_info	255	255	Compliant
52	RGS5	gw/acl_mode	1	1	Compliant
53	RGS6	gw/monitor	0	1	Not Compliant
54	RGS7	gw/resolve_phys_addr	0	1	Compliant
55	RGS9	gw/sim_mode	0	0	Compliant
56	RGS10	gw/rem_start	SSH_SHELL	DISABLED	Not Compliant
57	SNC1	snc/enable	1	1	Compliant
58	SNC2	snc/data_protection/max	3	3	Compliant
59	SNC3	snc/data_protection/min	3	3	Compliant
60	SNC4	snc/data_protection/use	3	3	Compliant
61	SNC6	snc/accept_insecure_cplic	1	0	Not Compliant
62	SNC7	snc/accept_insecure_gui	1	U	Not Compliant
63	SNC9	snc/accept_insecure_rfc	1	0	Not Compliant
64	SNC10	snc/permit_insecure_start	1	0	Not Compliant
65	SNC11	snc/force_login_screen	0	0	Compliant
66	SNC14	snc/only_encrypted_gui	0	1	Not Compliant
67	SNC15	snc/only_encrypted_rfc	0	1	Not Compliant
68	RCB4	rfc/callback_security_method	3	3	Compliant
69	LWEG3	ict/set_HTTPOnly_flag_on_cookies	0	0	Compliant
70	ICM06	icm/HTTP/logging_0	PREFIX=/,LOGFILE=/usr/sap/GE0/D01/log/http-%y-%...	PREFIX=/, LOGFILE=icmhttp.log, FILTER=SAPSM...	Not Compliant
71	ICM28	icm/HTTP/logging_client_0	PREFIX=/,LOGFILE=/usr/sap/GE0/D01/log/http-clie...	PREFIX=/,LOGFILE=access-\$(SAPSYSTEMNAME)-client...	Not Compliant
72	ICM29	ict/cors_enabled	0	1	Not Compliant
73	ICM31	icm/HTTP/trace_info	FALSE	FALSE	Compliant
74	ICM32	ict/allow_space_before_colon	FALSE	FALSE	Compliant
75	ICM33	ict/reject_expired_passwd	0	1	Not Compliant
76	MSS2	ms/monitor	0	0	Compliant
77	MSS3	ms/admin_port	0	0	Compliant
78	MSS4	ms/http_logging	1	1	Compliant
79	MSS5	ms/HTTP/logging_0	PREFIX=/,LOGFILE=/usr/sap/GE0/D01/log/ms-http-...	SWITCHTF=day,LOGFORMAT=%t %a %u %r %s %b %(Host)	Not Compliant
80	RGS11	gw/logging	ACTION=Ss LOGFILE=gw_log-%y-%m-%d SWITCHTF=day ...	ACTION=SPXMZ	Not Compliant
81	DYN01	dynp/checkskip1screen	OFF	ALL	Not Compliant
82	SAL15	rsau/selection_slots	10	10	Compliant
83	AUTO1	auth/object_disabling_active	N	N	Compliant
84	AUTO2	auth/check/calltransaction	2	3	Not Compliant
85	SAPGUI04	sapgui/nwbc_scripting	FALSE	FALSE	Compliant
86	SAPGUI05	sapgui/user_scripting_set_readonly	FALSE	FALSE	Compliant
87	SAPGUI06	sapgui/user_scripting_force_notification	FALSE	TRUE	Not Compliant
88	ABAP02	abap/ext_debugging_possible	0	2	Not Compliant
89	ICM26	is/HTTP/show_server_header	FALSE	FALSE	Compliant
90	ACL01	service/http/acl_file	NaN	needs to be manually checked - 1495075 - Access...	Not Compliant
91	ACL02	service/https/acl_file	NaN	needs to be manually checked - 1495075 - Access...	Not Compliant
92	XX01	abap/path_normalization	ext	EXT	Compliant
93	MISC01	rdisp/TRACE_HIDE_SEC_DATA	on	ON	Compliant
94	MISC02	rdisp/gui_auto_logout	1800	3600	Compliant
97	MISC07	ixm/dtd_restriction	prohibited	prohibited	Compliant



# SSOA-002 | Password Policies & Technical User



## Finding:

- There is currently no enhanced protection policy in place for critical users like SAP Standard User, High Authorized Technical User and Fire Fighters or SAP administrators. The possibility to overwrite and strengthen the system wide security policy with Security Policies is not in use.
- Several login profile parameter are currently not set to extend the complexity of end user passwords. E.g. could the password length of the current global default of 8 extended to the maximum for technical user.

## Business Implication:

- Stronger security policies – especially for critical and high authorized users – are mitigating the risk of penetration and misuse of those user accounts.
- User impersonation could allow access to high critical and high authorized user accounts which could lead to an impact to system integrity and availability as well as data confidentiality and integrity.

## Recommendation:

- Strengthen the login profile parameter to extend the password complexity with Transaction SECPOL. As of SAP\_BASIS release 7.31 Security Policies can be used to configure user specific password rules. For example it is recommended that for technical or service accounts the password length is refined with: `MIN_PASSWORD_LENGTH ≥ 30`.
- Evaluate the risk and usage of high authorized user accounts and consider the usage of special security policies.
- Follow the Single Sign-On strategy and deactivate passwords if the SSO login is enabled.

The screenshot shows the SAP Security Policy Overview table. The table has three columns: Security Policy, Short Text, and Changed On. The table is currently empty.

Security Policy	Short Text	Changed On



# SSOA-003 | Single Sign-On Utilization

## Single Sign-On Strategy



### Finding:

- Single Sign-On is generally considered in the current setup but dialog user logs are showing that there are still user accounts using passwords for logon.
- An extensive use of SAML2 for web applications is documented and in use whereas SAPGUI should be tunneled via the Business client. The usage of secure authentication mechanisms like with X.509 certificates or Kerberos for SAPGUI doesn't seem to-be in use at the moment.

### Business Implication:

- An end-to-end Single Sign-On strategy avoids password challenges like:
  - Weak password hashes
  - Weak passwords
  - Password renewal and delivery actions
  - Protection of password hash tables
- Without a consistent Single Sign-On enablement a solution which operates onPrem and in the cloud is not ready for modern hybrid scenarios. Passwords are always a common target for common cyber attacks.

### Recommendation:

- It is recommended to move on with the SSO rollout to enforce SSO for all users on all channels. Because there are always use cases where direct GUI access is required it is also recommended to use SSO for key users with SSO.
- Single Sign-On should be established for all Frontend-Channels as well as for administrative use.
- [320991 - Error codes during logon \(list\)](#)

Event	Event Status	Event Short Text	Category	Event Weighting	SAL Event Documentation
AU1		Logon successful (type=&A, method=&C)	Logon	Severe	<p>The user has logged onto the system.</p> <p>&lt;ZU&gt;Possible Types (= Access types):&lt;/&gt;            A = Dialog logon (SAP GUI)            B = Background job start            H = HTTP logon            U = User switch (internal call)            * = Password check (API, internal call)            M = SMTP            P = ABAP Push Channel (APC)            E = Build of a shared object area (internal call)            O = AutoABAP (internal call)            T = Server startup procedure (internal call)            V = SAP start service (internal call)            J = JAVA virtual machine (internal call)            W = BGRFC watchdog (internal call)</p> <p>&lt;ZU&gt;Possible methods (=authentication modes):&lt;/&gt;            P = Password            T = Logon ticket            t = Assertion ticket            X = X.509 certificate            S = SNC            R = RFC ticket            A = Authorized impersonation (background processing)            E = External (EXTID)            U = User switch            s = HTTP security session            Z = SAML2            1 = SAML1            o = OAuth2            N = SPNego            a = APC session</p> <p>If a user type or a method is not listed here, you might find more information in SAP Note 320991. A minimum kernel patch level is required to record the method. For more information, see SAP Note 1789518.</p>

SAP System	AS Instance	Date	Time	Cl.	Message ID	User	Terminal	Peer	TCode	Program	Audit Log Msg. Text	Note	Variable 1	Variable 2	Variable 3
GE0	syge04saps01_GEO_01	13.02.2023	06:53:54	300	AU1	90020199	PC27A...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	07:09:31	300	AU2	90023529	PC27A...	19.	SESS.	SAPMSYST	Logon failed (reason=1, type=A, method=P)		A	1	P
GE0	syge04saps01_GEO_01	13.02.2023	07:09:38	300	AU2	90023529	PC27A...	19.	SESS.	SAPMSYST	Logon failed (reason=1, type=A, method=P)		A	1	P
GE0	syge04saps01_GEO_01	13.02.2023	07:10:16	300	AU1	91999977	PC27A...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	07:12:28	300	AU1	90023529	PC27A...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	08:04:03	300	AU1	ELIASA	SCG01...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	08:36:23	300	AU1	92000122	PC2AT...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	08:37:02	302	AU1	MALLAVARAMP	PC0UD...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	09:14:33	300	AU1	92000122	PC2AT...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	09:21:06	302	AU1	KANDPALX	PC27L...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	09:21:56	302	AU2	90018379	PC2AX...	19.	SESS.	SAPMSYST	Logon failed (reason=1, type=A, method=P)		A	1	P
GE0	syge04saps01_GEO_01	13.02.2023	09:22:15	300	AU1	KANDPALX	PC27L...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	09:22:38	302	AU2	90018379	PC2AX...	19.	SESS.	SAPMSYST	Logon failed (reason=1, type=A, method=P)		A	1	P
GE0	syge04saps01_GEO_01	13.02.2023	09:23:05	302	AU2	90018379	PC2AX...	19.	SESS.	SAPMSYST	Logon failed (reason=1, type=A, method=P)		A	1	P
GE0	syge04saps01_GEO_01	13.02.2023	09:39:18	800	AU1	AE_ZALDIE5	C11-S...	10.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	09:40:27	300	AU1	91999976	PC27L...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	09:44:17	300	AU1	CENTOFB	PC2AT...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	09:51:26	300	AU1	92000107	PC2AT...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	10:01:16	300	AU1	92000122	PC2AT...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	10:03:38	300	AU2	ELIASA	SCG01...	19.	SESS.	SAPMSYST	Logon failed (reason=1, type=A, method=P)		A	1	P
GE0	syge04saps01_GEO_01	13.02.2023	10:03:44	300	AU1	ELIASA	SCG01...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	10:06:48	302	AU1	OSS_USER	dewdf...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P
GE0	syge04saps01_GEO_01	13.02.2023	10:10:10	302	AU1	91999977	PC27A...	19.	S000	SAPMSYST	Logon successful (type=A, method=P)		A	0	P



# SCFG-005 | SAP Standard User



## Finding:

- The standard user setup was also reviewed in the ECR system. In this system was SAP\* not protected and a login with the default password was possible.
- Additionally, are RFC connections in this system available which are pointing to central systems like the DSMS which is again connected to other production systems. These security misconfigurations are representing a serious attack chain.

## Business Implication:

- The misuse of DDIC in batch jobs or interfaces is a target to misuse to elevate privileges within the system or remote systems. Due to the broad privileges of this user the system and its data could be fundamentally affected.

## Recommendation:

- Setup SAP System recommendation to check the status of all SAP Standard Users permanently.
- Execute real-time alerting once standard users are getting unlocked and used.
- Replace DDIC within Batch job processing and RFC communication.

The screenshots illustrate the findings and configurations related to the SAP standard user issue:

- Check the Passwords of Standard Users in All Clients:** Shows a table of standard users across clients. Key entries include:
 

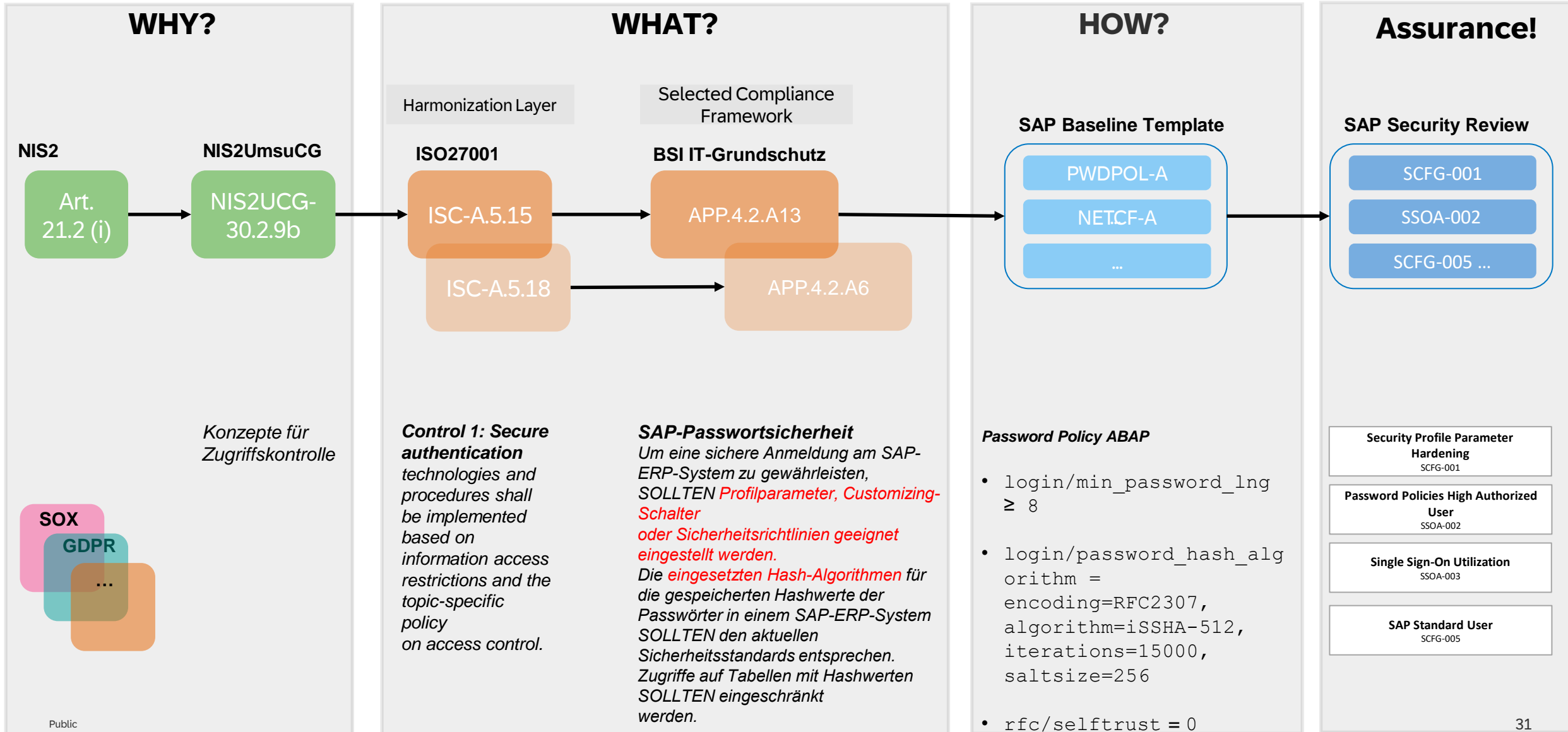
Client	User	Lock	Password Status	Reason for User Lock
000	DDIC	🔒	Exists; Password not trivial.	
	SAP*	🔒	Does not exist. Logon possible with p/w PASS. See Note 2383	
	SAPCPIC	🔒	Exists; Password not trivial.	Locked by administrator
	TMSADM	🔒	Exists; Password not trivial.	
001	DDIC	🔒	Exists; Password not trivial.	Locked by unsuccessful logons
	SAP*	🔒	Exists; Password not trivial.	Locked by administrator
	SAPCPIC	🔒	Exists; Password not trivial.	
	TMSADM	🔒	Does not exist.	
066	DDIC	🔒	Does not exist.	
	EARLYWATCH	🔒	Exists; Password not trivial.	
	SAP*	🔒	Does not exist. Logon possible with p/w PASS. See Note 2383	
	SAPCPIC	🔒	Does not exist.	
	TMSADM	🔒	Does not exist.	
210	DDIC	🔒	Exists; Password not trivial.	
	SAP*	🔒	Exists; Password not trivial.	
	SAPCPIC	🔒	Exists; Password not trivial.	
	TMSADM	🔒	Password PASSWORD is well known	
- Display Profile Parameter Details:** Shows metadata for the parameter `login/no_automatic_user_sapstar`. Key values include:
 

Property	Value
Name	login/no_automatic_user_sapstar
Type	Logical Expression
Parameter Group	Login
Parameter Description	Control of the automatic login user SAP*
System-Wide Parameter	No
Dynamic Parameter	No
Vector Parameter	No
Has Subparameters	No
Check Function Exists	No
Expansion Level	1
Kernel Default	1
Default Profile	0
Instance Profile	0
Current Value	0
- RFC Destination USE\_DSM5-ECR-210-COMM:** Shows configuration for an RFC destination pointing to a central system. Key settings include:
  - Remote Logon:
  - Connection Type: 3 | ABAP Connection
  - Description 1: \*GENERATED\*
  - Logon Procedure: Language EN, Client 210, User DSM\_COMM\_ECR, PW Status saved.
  - Trust Relationship: No
  - Status of Secure Protocol: SNC (Inactive)
- Structure Editor: Display PROFILES from Entry 1:** Shows a table of profiles:
 

Profile Name	Description	Category
BAPIPROF	BAPIPTXT	B
SAP_ALL	All SAP System authorizations	C A



# EXAMPLE: NIS2 to Security Baseline Mapping



# Cybersecurity Compliance Management services

## SAP Store Service

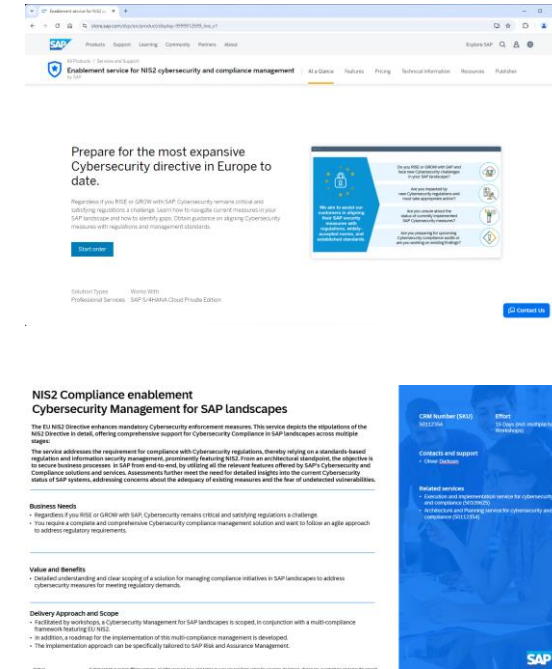
- Enablement service for NIS2 Cybersecurity and Compliance Management
- SAP Store URL: <https://store.sap.com/dcp/en/>

## Architecture and planning service for cybersecurity and compliance

- Service Scope : Cybersecurity Compliance Management (CSCM enablement)
- Service URL: [Architecture and planning service for cybersecurity and compliance](#)

## Related publications

- SAP Community blog:  
<https://community.sap.com/t5/technology-blogs-by-sap/sap-enablement-service-for-nis2-cybersecurity/ba-p/13637332>
- LinkedIn blog:  
<https://www.linkedin.com/pulse/nis2-stands-most-expansive-cybersecurity-directive-europe-derksen-xcupf/>





# NIS2 Compliance enablement Cybersecurity Management for SAP landscapes

The EU NIS2 Directive enhances mandatory Cybersecurity enforcement measures. This service depicts the stipulations of the NIS2 Directive in detail, offering comprehensive support for Cybersecurity Compliance in SAP landscapes across multiple stages:

The service addresses the requirement for compliance with Cybersecurity regulations, thereby relying on a standards-based regulation and information security management, prominently featuring NIS2. From an architectural standpoint, the objective is to secure business processes in SAP from end-to-end, by utilizing all the relevant features offered by SAP's Cybersecurity and Compliance solutions and services. Assessments further meet the need for detailed insights into the current Cybersecurity status of SAP systems, addressing concerns about the adequacy of existing measures and the fear of undetected vulnerabilities.

---

## Business Needs

- Regardless if you RISE or GROW with SAP, Cybersecurity remains critical and satisfying regulations a challenge.
- You require a complete and comprehensive Cybersecurity compliance management solution and want to follow an agile approach to address regulatory requirements.

---

## Value and Benefits

- Detailed understanding and clear scoping of a solution for managing compliance initiatives in SAP landscapes to address cybersecurity measures for meeting regulatory demands.

---

## Delivery Approach and Scope

- Facilitated by workshops, a Cybersecurity Management for SAP landscapes is scoped, in conjunction with a multi-compliance framework featuring EU NIS2.
- In addition, a roadmap for the implementation of this multi-compliance management is developed.
- The implementation approach can be specifically tailored to SAP Risk and Assurance Management.

### CRM Number (SKU)

50112354

### Effort

15 Days (incl. multiple half-day Workshops)

### Contacts and support

- Oliver Derksen

### Related services

- Execution and implementation service for cybersecurity and compliance (50109625)
- Architecture and Planning service for cybersecurity and compliance (50112354)

# Enablement service for NIS2 Compliance Management

The EU NIS2 Directive enhances mandatory Cybersecurity enforcement measures, for instance by stipulating early incident reporting, broadening risk management strategies, and specifying a new level of executive responsibility for Cybersecurity.

We will delve into and discuss the potential impacts of NIS2 requirements on SAP landscapes, utilizing S/4HANA as an illustrative case study, and presenting an approach to sustainably manage cybersecurity regulations in general, with a special emphasis on NIS2.

---

## Business Needs

- Regardless if you RISE or GROW with SAP, Cybersecurity remains critical and satisfying regulations a challenge.
- NIS2 stands for the most expansive Cybersecurity directive in Europe to date.
- Identify approaches to address requirements affecting SAP landscapes, raising from this new regulation.

---

## Value and Benefits

- Gain detailed insights into the Cybersecurity Points of View supporting the definition of a roadmap establishing a NIS2 compliant SAP landscape.
- Obtain how to align Cybersecurity measures with regulatory requirements and supportive standards for managing Cybersecurity.
- Learn how to navigate current measures in your SAP landscape and to identify “open flanks”.

---

## Delivery Approach and Scope

- This service will be delivered as an introductory workshop.
- The session will outline the Cybersecurity Points of View and provide outlook for the determination of a roadmap how to move on in establishing a NIS2 compliant SAP landscape.

CRM Number (SKU)

50164685

Effort

Two hours virtual workshop

## Contacts and support

- Oliver Derksen

## Related services

- Execution and implementation service for cybersecurity and compliance (50109625)
- Architecture and Planning service for cybersecurity and compliance (50112354)

# Thank you!

**Michael Altmaier**

Principal Security Architect  
Michael.Altmaier@SAP.com

