Deloitte.

Deloitte Cybersecurity Monitoring and Dashboard

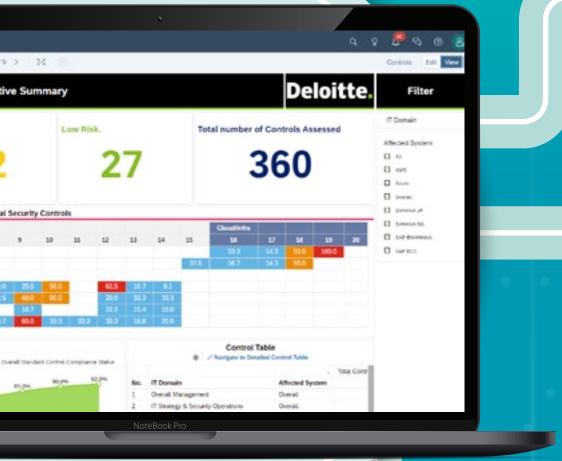
MAKING AN IMPACT THAT MATTERS since 1845

Solution overview

Vulnerabilities, security misconfigurations, and user privileges

What is it?

Deloitte has developed an asset -Cybersecurity Monitoring and Dashboard for SAP -to provide continuous visibility and transparency into the vulnerabilities and security best practices of the monitored SAP S/4 landscapes. It provides organizations easy to understand dashboards, enabling monitoring and detection of security loopholes which are very complex to achieve in a SAP environment, especially in large landscapes.



What are the benefits?

- Provide management transparency to their SAP cyber security control profiles.
- Easy-to-understand dashboard interface for continuous control monitoring cross all SAP landscapes.
- One-stop view for multiple SAP cyber data, ABAP, JAVA, Fiori and HANA DB.
- Cost savings to avoid the need to perform regular SAP vulnerability assessments and security testing.

Who's it for?

Designed for use by CIO, CRO, IT Security, Risk and Compliance, as well as Internal Audit functions to proactively mitigate SAP security risk, vulnerability, data protection, and cyber attacks.

Cybersecurity Extension in SolMan and SAC Dashboard

Leveraging on native integration with Solution Manager (SolMan), this asset deploys extension into SolMan enabling a major shift in security monitoring for SAP landscapes, without requiring additional hardware or installing additional SAP applications.

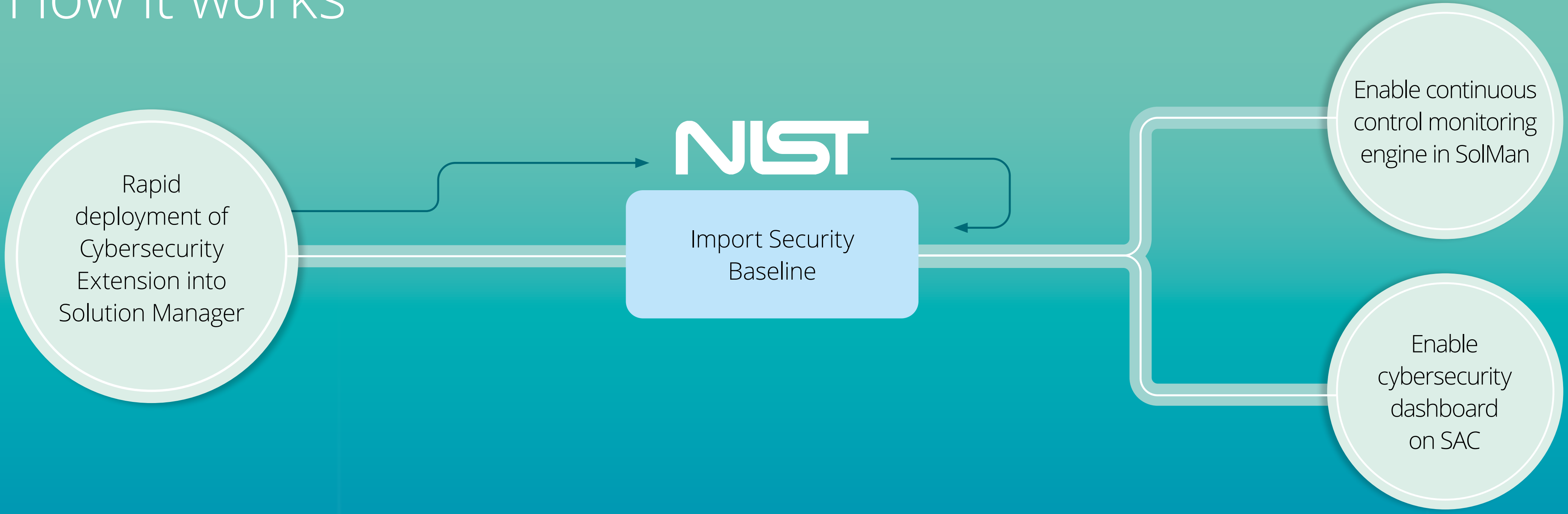
Monitor security KPIs using interactive dashboards. This asset performs scheduled scans for thousands of vulnerabilities in SAP platforms including misconfigurations, missing patches and user privileges. Security checks are benchmarked against industry standards and SAP recommendations.

Follows best practices

- Monitoring is performed against Security Baseline, Security Notes and HotNews published by SAP and Best Practice recommended by Deloitte.
- Check points are also mapped to industry standards such as NIST Cybersecurity Framework, SOX IT controls, etc.
- Baselines will also be refreshed periodically for emerging threats and vulnerabilities. and provided as part of Deloitte's suite of services.

SAP Security Baseline NIST

How it works



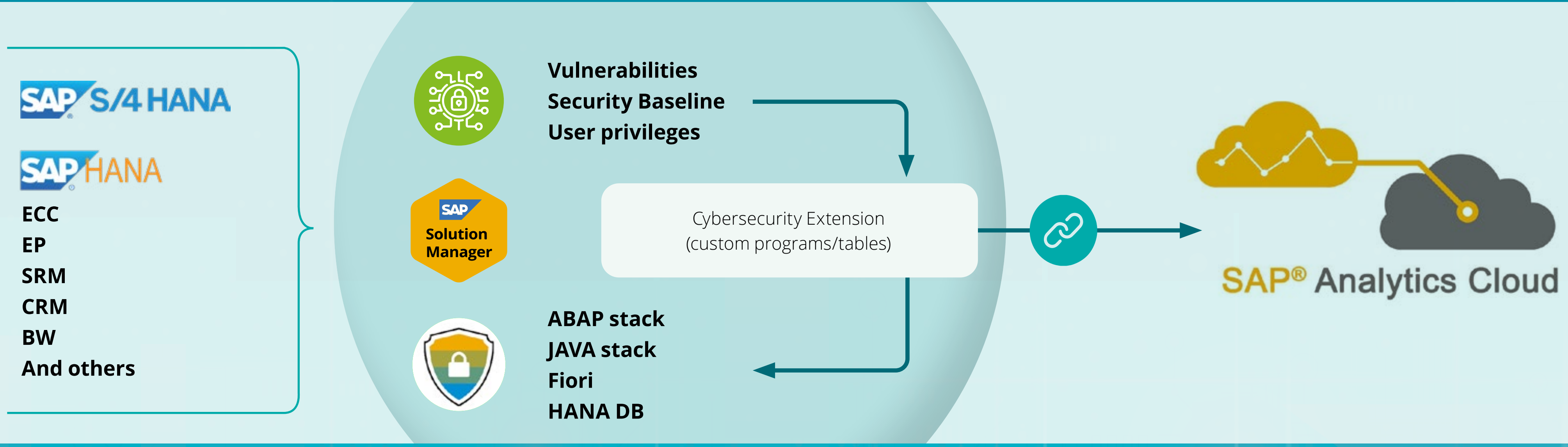
Rapid deployment of Cybersecurity Extension into Solution Manager

NIST

Import Security Baseline

Enable continuous control monitoring engine in SolMan

Enable cybersecurity dashboard on SAC



ECC
EP
SRM
CRM
BW
And others

Vulnerabilities
Security Baseline
User privileges

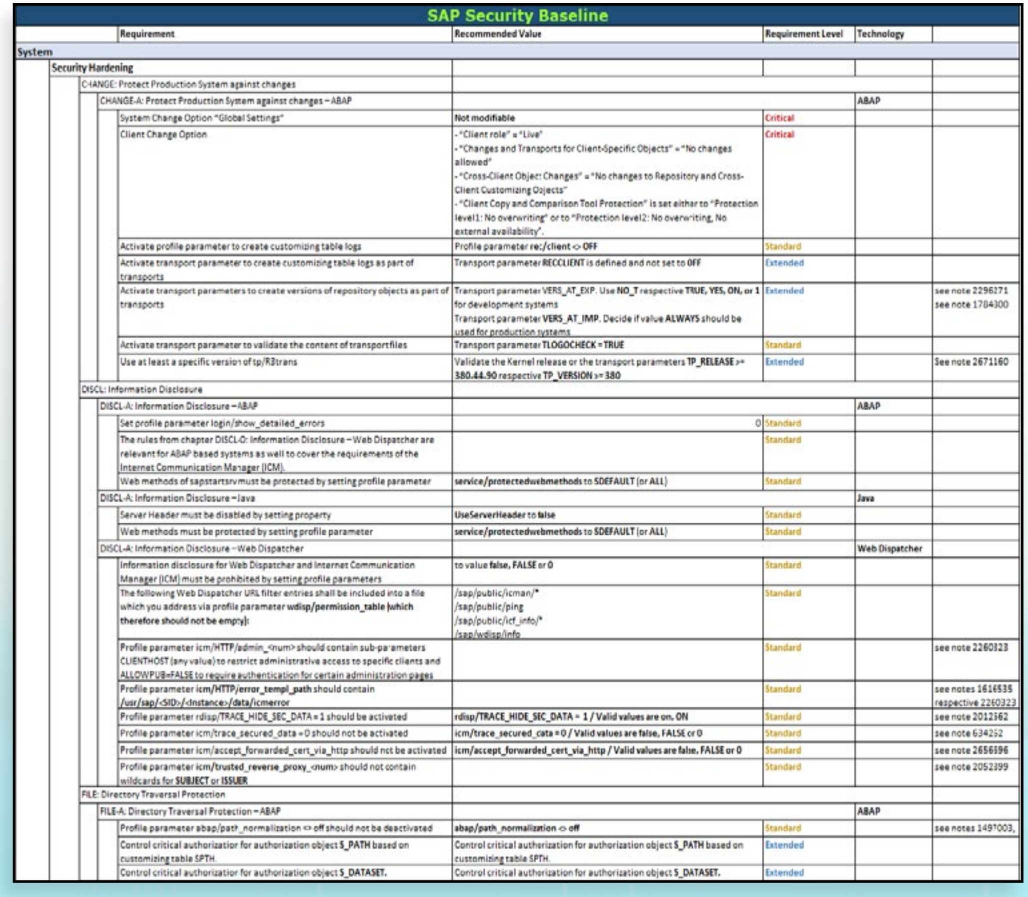
Cybersecurity Extension (custom programs/tables)

ABAP stack
JAVA stack
Fiori
HANA DB

Security Monitoring Coverage | 300+ control points

Category	Number of control points
ABAP	
Audit Settings	11
Other	68
SAP Notes	14
Security Hardening	98
Security Policy	19
User Security & Authorizations	46
HANA	
Audit Settings	3
HANA	6
Other	6
SAP Notes	3
Security Policy	9
User Security & Authorizations	6
JAVA	
Audit Settings	4
SAP Application Server JAVA	18
SAP Notes	2
Security Hardening	4
Security Policy	19
User Security & Authorizations	2
Total Control Assessment	**338**

Example of control points on SAP security hardening

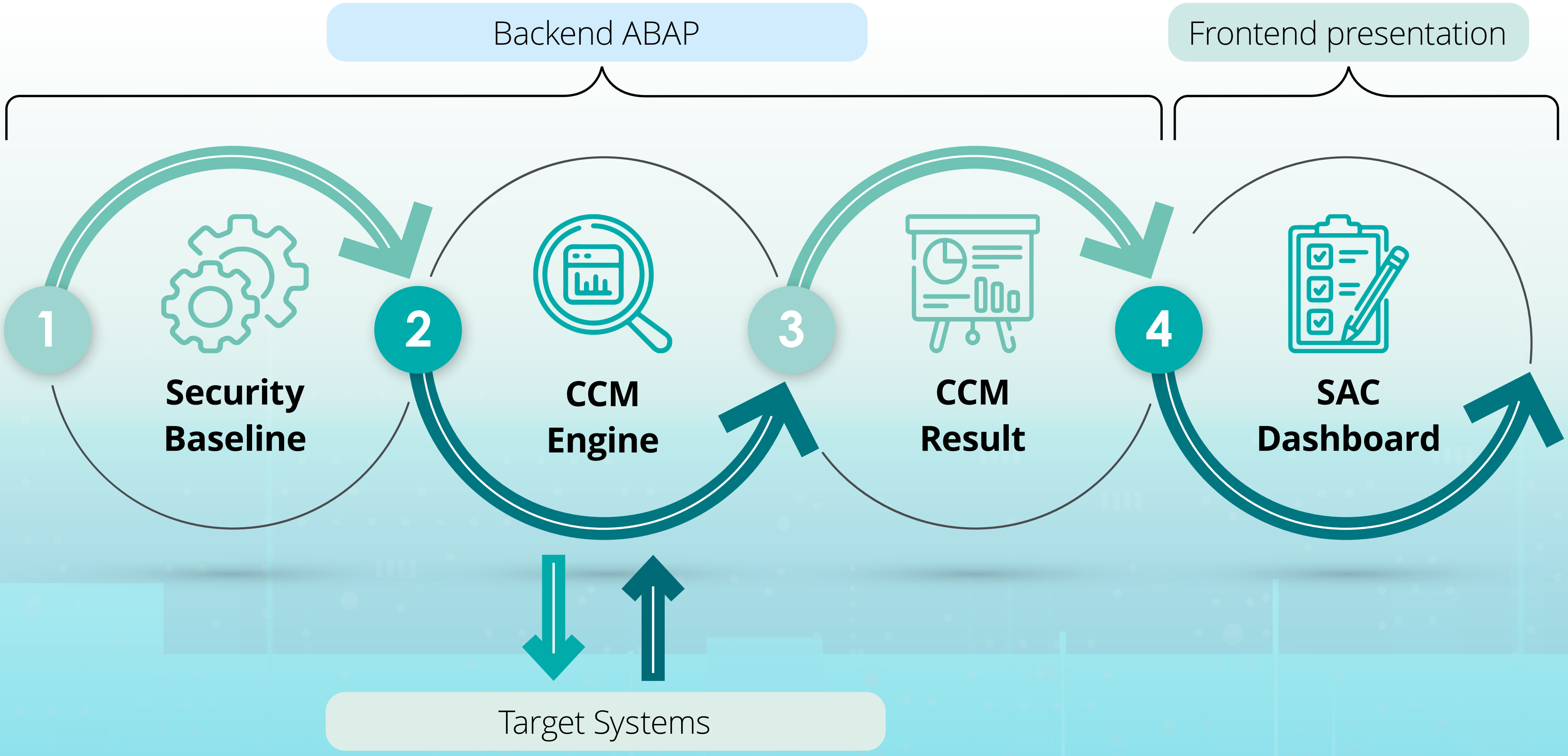


SAP Security Baseline

	Requirement	Recommended Value	Requirement Level	Technology	
System					
Security Hardening					
CHANGE: Protect Production System against changes					
CHANGE-A: Protect Production System against changes – ABAP				ABAP	
	System Change Option "Global Settings"	**Not modifiable**	Critical		
	Client Change Option	- "Client role" = "Live" - "Changes and Transports for Client-Specific Objects" = "No changes allowed" - "Cross-Client Objec: Changes" = "No changes to Repository and Cross-Client Customizing Ojects" - "Client Copy and Comparison Tool Protection" is set eithar to "Protection level1: No overwriting" or to "Protection level2: No overwriting, No external availability".	Critical		
	Activate profile parameter to create customizing table logs	Profile parameter **rec/client <> OFF**	Standard		
	Activate transport parameter to create customizing table logs as part of transports	Transport parameter **RECCLIENT** is defined and not set to **OFF**	Extended		
	Activate transport parameters to create versions of repository objects as part of transports	Transport parameter VERS_AT_EXP. Use **NO_T** respective **TRUE, YES, ON, or 1** for development systems Transport parameter **VERS_AT_IMP**. Decide if value **ALWAYS** should be used for production systems	Extended		see note 2296271 see note 1784300
	Activate transport parameter to validate the content of transportfiles	Transport parameter **TLOGOCHECK = TRUE**	Standard		
	Use at least a specific version of tp/R3trans	Validate the Kernel release or the transport parameters **TP_RELEASE >= 380.44.90** respective **TP_VERSION >= 380**	Extended		See note 2671160
DISCL: Information Disclosure					
DISCL-A: Information Disclosure – ABAP				ABAP	
	Set profile parameter login/show_detailed_errors	0	Standard		
	The rules from chapter DISCL-O: Information Disclosure – Web Dispatcher are relevant for ABAP based systems as well to cover the requirements of the Internet Communication Manager (ICM).		Standard		
	Web methods of sapstartsrv must be protected by setting profile parameter	**service/protectedwebmethods** to **SDEFAULT** (or **ALL**)	Standard		
DISCL-A: Information Disclosure – Java				Java	
	Server Header must be disabled by setting property	**UseServerHeader** to **false**	Standard		
	Web methods must be protected by setting profile parameter	**service/protectedwebmethods** to **SDEFAULT** (or **ALL**)	Standard		
DISCL-A: Information Disclosure – Web Dispatcher				Web Dispatcher	
	Information disclosure for Web Dispatcher and Internet Communication Manager (ICM) must be prohibited by setting profile parameters	to value **false, FALSE** or **0**	Standard		
	The following Web Dispatcher URL filter entries shall be included into a file which you address via profile parameter **wdisp/permission_table (which therefore should not be empty):**	/sap/public/icman/* /sap/public/ping /sap/public/icf_info/* /sap/wdisp/info	Standard		
	Profile parameter icm/HTTP/admin_<num> should contain sub-parameters CLIENTHOST (any value) to restrict administrative access to specific clients and ALLOWPUB=FALSE to require authentication for certain administration pages		Standard		see note 2260323
	Profile parameter **icm/HTTP/error_templ_path** should contain **/usr/sap/<SID>/<Instance>/data/icmerror**		Standard		see notes 1616535 respective 2260323
	Profile parameter rdisp/TRACE_HIDE_SEC_DATA = 1 should be activated	**rdisp/TRACE_HIDE_SEC_DATA = 1 / Valid values are on, ON**	Standard		see note 2012562
	Profile parameter icm/trace_secured_data = 0 should not be activated	**icm/trace_secured_data = 0 / Valid values are false, FALSE or 0**	Standard		see note 634262
	Profile parameter icm/accept_forwarded_cert_via_http should not be activated	**icm/accept_forwarded_cert_via_http / Valid values are false, FALSE or 0**	Standard		see note 2656596
	Profile parameter **icm/trusted_reverse_proxy_<num>** should not contain wildcards for **SUBJECT** or **ISSUER**		Standard		see note 2052399
FILE: Directory Traversal Protection					
FILE-A: Directory Traversal Protection – ABAP				ABAP	
	Profile parameter abap/path_normalization <> off should not be deactivated	**abap/path_normalization <> off**	Standard		see notes 1497003,
	Control critical authorization for authorization object **S_PATH** based on customizing table SPTH.	Control critical authorization for authorization object **S_PATH** based on customizing table SPTH.	Extended		
	Control critical authorization for authorization object **S_DATASET.**	Control critical authorization for authorization object **S_DATASET.**	Extended		

Solution details

Deloitte SAP Cybersecurity Dashboard consists of 4 key components to enable continuous control monitoring (CCM).



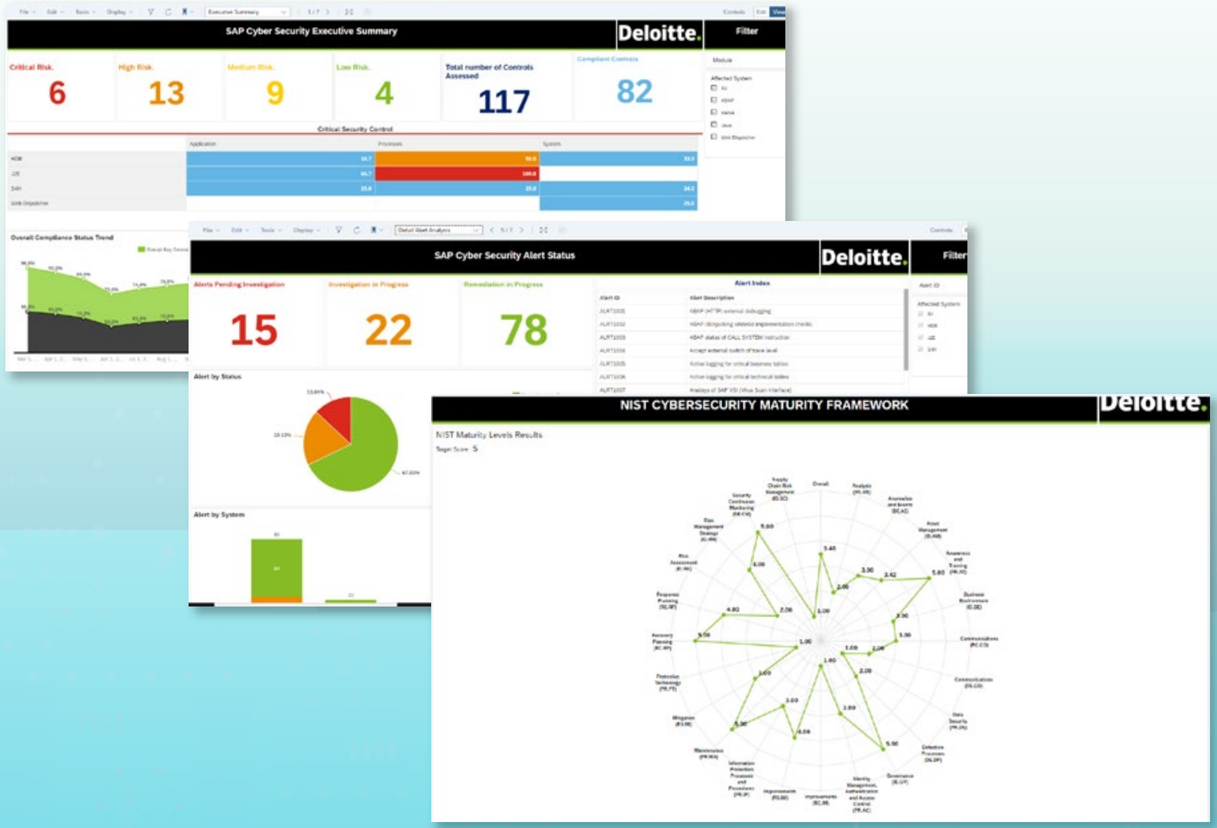
SAP S/4 HANA
SAP HANA

ECC	CRM
EP	BW
SRM	And others

SAC dashboard

Overall compliance status of all controls are fully integrated into pre-built SAC dashboard.
For clients who do not have SAC, the same dashboard can be built in Power BI / Tableau / Qlik.

SAP® Analytics Cloud



SAP Cyber Security Executive Summary

Deloitte.

Filter

Critical Risk.	High Risk.	Medium Risk.	Low Risk.	Total number of Controls Assessed	Compliant Controls
6	13	9	4	117	82

Critical Security Control

Overall Compliance Status Trend

SAP Cyber Security Alert Status

Deloitte.

Filter

Alerts Pending Investigation	Investigation in Progress	Remediation in Progress
15	22	78

Alert Index

Alert by Status

Alert by System

NIST CYBERSECURITY MATURITY FRAMEWORK

Deloitte.

NIST Maturity Levels Results

Target Score 5

Also available in

Power BI

tableau

Qlik® Sense

Want to know more? Let’s talk

Tang Ke	Vishal Chandrahas	Eugene Loh
Executive Director	Senior Manager	Senior Manager
tke@deloitte.com	vichandrahas@deloitte.com	juloh@deloitte.com
+65 6216 3231	+65 6800 2124	+65 6800 2172

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/aboutto learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

About Deloitte Singapore

In Singapore, risk advisory services are provided by Deloitte & Touche Enterprise Risk Services Pte. Ltd. and other services (where applicable) may be carried out by its subsidiaries and/or affiliates.

Deloitte & Touche Enterprise Risk Services Pte. Ltd. (Unique entity number: 197800820D) is a company registered with the Accounting and Corporate Regulatory Authority of Singapore.

© 2023 Deloitte & Touche Enterprise Risk Services Pte. Ltd

Designed by CoRe Creative Services. RITM1313863