Customer Audit Report 2019

Data protection Certification

of SAP by

British Standards Institution (BSI)

BSI Group Deutschland GmbH, Frankfurt am Main, 2019 December 31

...making excellence a habit.™

Content

About SAP 3
Data Protection and Information Security at SAP 4
SAP Policies 5
SAP Security Policy Framework 5
Data Protection Policy 9
Data Protection Management Systems 10
Structure of the SAP Data Protection Management System 10
Goals of SAP's Data Protection Management System 13
Reference to Laws, Standards and SAP Guidelines 13
Development of the Data Protection Management System at SAP 15
Major Changes of the DPMS to comply with the EU GDPR 18
Organizational scope of the DPMS 20
Certification Process 21
Partner BSI 21
Audit Methodology 22
Training 23
Control of Technical and Organizational Measures 24
General Audit structure and types 32
Internal Audits of the DPMS – Compliance 32
Internal Audits of the DPMS – Awareness 33
Internal Audits of the DPMS – Questionnaire 34
Audit Finding Classification SAP 44
Audit Finding classification BSI 45
Audit Structure 2019 46
Internal Audits 2019 46
External Audits 2019 52
Executive Summary 54

About SAP

For more than 45 years, SAP has driven innovation on behalf of its customers to help the world run better and improve people's lives.

Telling our purpose-driven story to the market shows how we grew to become one of the largest technology companies, dedicated to our customers, products, solutions, and people. By promising to help our customers innovate to run at their best, coupled with our Intelligent Enterprise Suite of applications and networks to connect the front office to the back office, they can solve complex problems to address some of the world's biggest challenges.

This story enables employees to tell a consistent message that connects our commitment to helping every company become a best-run business by highlighting who we are, where we've been, and where we're going to produce lifelong customers. Because it's the best-run businesses that make the world run better. And the best run SAP.

Strategy

SAP is committed to supporting every customer to become a best-run business. Together, we help the world run better and improve people's lives. Being a best-run business means being an intelligent enterprise. Our strategy is therefore to deliver The Intelligent Enterprise for our customers, so they can achieve their desired outcomes.

...making excellence a habit.™

Data Protection and Information Security at SAP

Data protection and information security come first at SAP. SAP's aim is to achieve and maintain an effective and appropriate level of data protection and security within SAP and to strengthen the position of SAP as a trusted partner for its customers and partners. Given this matter's importance, a number of departments at SAP are dedicated to data protection and information security.

Data Protection and Privacy (DPP), headed by SAP's data protection officer, defines SAP's strategy in alignment with global, regional, and local data protection legislation.

Thus, Data Protection and Privacy ensures maximum adherence to data protection regulations provided by laws, policies, certificates, work instructions, and contracts across the company. It identifies, handles, monitors, and documents projects and topics related to data protection, and reports on these matters. The DPP operationalizes the strategic conventions given by the SAP security and data protection organizations.

To meet the requirements of the national, European and international data protection legislation, DPP implemented and operates a Data Protection Management System. The Data Protection & Privacy department also works with BSI as certification body on data protection certification, which this customer report describes.

SAP's Corporate Security organization works to protect hardware and software against the loss, deletion, and misuse of data, and liaises with various other security departments, such as those dealing with IT security or facility security. In the global organization, Global Risk and Compliance managers are also the risk and security managers at regional and local level. Data Protection and Privacy, Corporate Security and the Global Risk and Compliance Office are part of the Finance and Administration Board area led by Luka Mucic.

...making excellence a habit.™

SAP Policies

SAP has various policies that ensure a common understanding of security and data protection at the company worldwide. Two policies are of particular relevance here: The Security Policy and the SAP Data Protection Policy.

SAP Security Policy Framework

The Security Policy Framework describes the rules of conduct and processes. The SAP Security Policy Framework consists of several levels of security documents that support the requirements set forth in the SAP Global Security Policy. Lines of Business may also have supporting policies, standards, procedures, and good practices.

Security Policy
A high-level document that defines management intent, expectations, and direction. It establishes the strategic goals and objectives that the organization strives to achieve in order to maintain the highest level of security.

Security Standard
A document that defines the minimum requirements for adherence to a policy. These requirements can be met by executing the corresponding procedure(s).

Security Procedure
Detailed specification of how the standards have to be implemented. The SAP Global Security Procedures are subdivided into instructive (Hardening Procedure) and descriptive (Reference Architecture) documents.

Security Good Practices
A checklist for employees to simplify the Policy implementation process.

...making excellence a habit.™

There are two parts to the Security Policy: the security objectives that are part of strategy and set out in the Security Policy document, and the specific actions required to reach these objectives, which are formulated in the Security standards.

The SAP Security Policy governs fundamental aspects relating to security at SAP for the protection of its employees, information, systems, and assets. It forms the basis for the security measures to be taken in the specific business units and SAP companies. The protection of SAP employees and guests, in particular the protection of life and physical integrity, has priority over all other security measures. The Policy also states that security incidents are to be treated as a matter of highest priority and investigated. According to the Policy, only those persons are authorized to access confidential or sensitive information who require this information to carry out their work. This applies especially to customer and partner data. House rules apply to every SAP building.

Any non-compliance with the Security Policy and the Security standard is reported in a global security report to the Executive Board and could lead to measures or disciplinary actions. The Security Policy and the security standards are monitored continuously for improvement as new threats are discovered.The SAP security policy comprises of many security standards – the ones which are relevant for the Data Protection Management System used at SAP are listed below.

Special security requirements apply to some parts of SAP, and these requirements are set out in separate security standards: Board Security, Physical Security, Crisis Management, Business Continuity, and Product Certification. They are not described in detail here, as they are not expressly mentioned in the Data Protection Management System because they do not apply universally.

All Security standards are subject to a regular review process. Any amendments are documented and communicated to SAP employees. The following topics are data protection relevant aspects of the security policy:

- Mobile Devices
- Laptops and Workstations

- Remote Access
- Human Resources Security
- Security Awareness
- Enforcement
- Asset Management
- Information Classification and Handling
- Return of Assets
- Access Management
- Encryption
- Physical and Environmental Security
- Operations Security
- Electronic Communications Security
- System Acquisition, Development, and Maintenance
- External Party and Supplier Relationships
- Security Incident Management
- Business Continuity
- Compliance with Security Requirements
- Legal and Contractual Requirements
- Protection of Records
- Data Privacy
- Intellectual Property
- Information Security Reviews
- Independent Review
- Compliance with Security Policies and standards
- Technical Review
- Acceptable Use Policy
- Prohibited Activities
- Personal Use
- Laptops and Workstations
- Lock Laptops and Workstations
- Unauthorized Users
- Patch Management
- Removable Storage Devices
- Mobile Devices
- Use of Personal Mobile Devices
- Software and App Installation
- Security Upgrades/Patches

...making excellence a habit.™

- Protection against Theft
- Laptop and Workstation Backup
- Protection Against Malware
- Antivirus Software
- Email
- Virus Scan of External Information
- Suspected Malware Infection
- Monitoring
- Travel Requirements
- Possession of Devices and Information
- Password and Web Browsers
- Return of Assets
- Software Use
- Procurement
- Internet Use
- Social Media
- Voice Communications
- Voice/Telephone
- Voice Mailbox
- Fax Machines
- Email and Electronic Messaging
- Confidential information
- Unacceptable Content
- Passwords
- Recommendations for strong passwords
- Password Protection
- Certificates and Private Keys
- Clean Desk and Clear Screen
- Paper documents
- Screens and Work areas
- Physical Security
- Reporting Security Incidents

...making excellence a habit.™

Data Protection Policy

The SAP Global Personal Data Protection and Privacy Policy defines the basic principles on how SAP handles the collection, processing and use of personal data. It outlines organizational provisions and assigns responsibility and accountability within SAP's organization and thus defines SAP's Data Protection and Privacy Framework. SAP must safeguard the personal data of employees, customers, suppliers, applicants, and other individuals to comply with applicable laws and meet stakeholder expectations.

It is the duty of every SAP employee to comply with this policy when handling personal data in their daily work. SAP is a global company with its headquarters in Germany. Therefore, the SAP Global Personal Data Protection and Privacy Policy is based on the definitions of the European data protection legislation and defines the basic principles that are applicable for every SAP entity. Where the laws that apply in a particular country or other applicable laws are stricter, personal data is treated in accordance with the requirements of these stricter laws. Any further standard or guideline issued under this policy may be supplemented as necessary by such local laws.

The policy establishes the basic principles for any collection, processing, recording, storage, transfer, disclosure, deletion, and any other handling or use of personal data under SAP's legal responsibility by defining requirements for all operations involving personal data and by establishing clear responsibilities and organizational structures.

...making excellence a habit.™

Data Protection Management Systems

A Data Protection Management System (DPMS) gives a company and its organizational items instructions for establishing, implementing, enforcing, monitoring, inspecting, maintaining, and improving data protection guidelines. It defines which instruments and methods the management of the organization uses to comprehensibly direct data protection-oriented tasks and activities. The company's management team is responsible for the strategic role and for the decision to implement and design a Data Protection Management System.

The objective of the Data Protection Management System is to define the data protection level in the organization, to ensure that the necessary legal, regulatory, contractual, and internal data protection requirements are met and that an effective monitoring system is in place to ensure regular checks on whether data protection requirements are being met. The functions of the Data Protection Management System are:

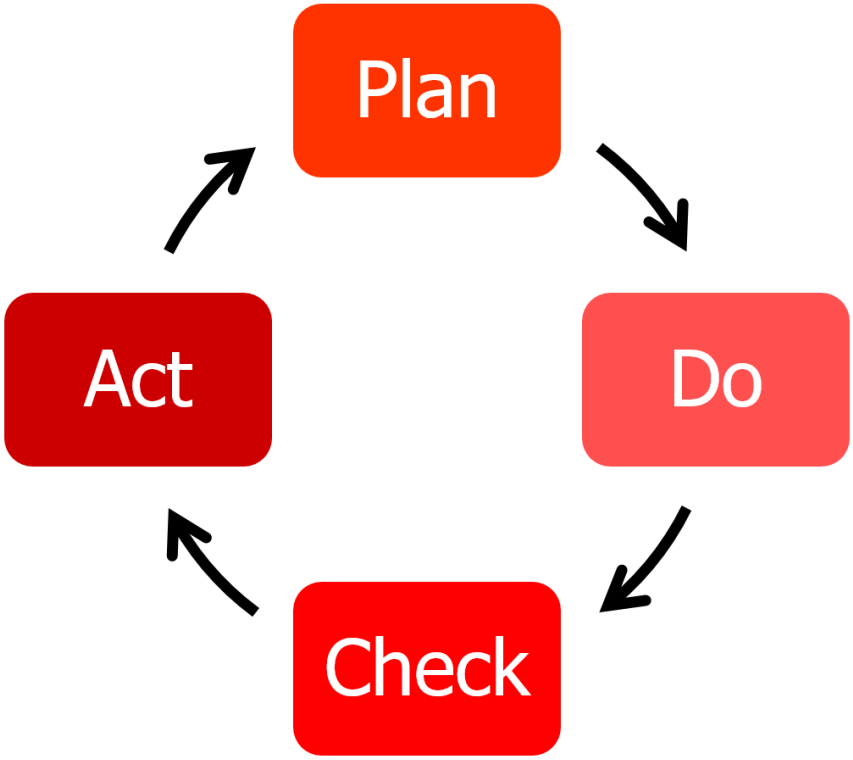
- To plan, develop, apply, monitor, and improve measures that are necessary to meet statutory and contractual data protection requirements.
- To take account of the statutory and contractual data protection requirements, the instructions in the data protection policy issued by the responsible body, and the requirements specified in this document.
- To determine and describe the current level of data protection in a clear and transparent way.
- To maintain, continuously review, and improve the level of data protection achieved.

Structure of the SAP Data Protection Management System

SAP's Data Protection Management System, like all other management systems, is based on a structured model known as the PDCA (plan-do-check-act) cycle. This is an iterative, four-step management method that is typically used to control and continuously improve business processes. It ensures that the Data Protection Management System process is improved continuously. Data Protection and Privacy is responsible for setting up, executing, monitoring,

...making excellence a habit.™

and continuously improving the Data Protection Management System. To improve the effectiveness and functionality of the Data Protection Management System, it is subjected to mandatory inspections at intervals of one year, in cooperation with the SAP data protection officer.



PDCA cycle

The PDCA cycle can be applied to the Security Management Framework as follows:

In the first step, the "plan" step, objectives and processes are established that are intended to deliver the desired result. This means that, during the initial implementation of the PDCA cycle, plans are made for the first time about how the management system will be introduced into the organization. The "plan" step also consists of establishing the organizational structure in the form of internal and external audits and defining the security risks for each line of business. This involves conducting a risk analysis on the individual business

...making excellence a habit.™

processes that are included in the scope of the Data Protection Management System in cooperation with Global Risk Management. Following the analysis, risk owners are defined who are responsible for mitigating and regularly checking the identified risks. Appropriate security measures are defined for each of the security risk areas in collaboration with the responsible organizations. The security and data protection requirements are also set out in the SAP Security Policy and the associated in-house standards.

As set out during the "plan" cycle, the "do" cycle involves executing the process steps that are needed to carry out the implementation as planned using the available resources, operational processes, and measures.

This means that the security requirements defined in the "plan" cycle are implemented in the "do" cycle with the help of the DPMS representatives from the individual lines of business and locations and from the operational organizational units. Mandatory training courses and campaigns are provided to help implement and enact the measures.

The third step in the cycle, the "check" step, consists of several stages. Potential weak points that may have negative implications for data protection are checked and mitigated on an ongoing basis. The organizational units are continuously assessed by means of external and internal audits. The external audits are carried out by the BSI and the internal audits by SAP's Data Protection and Privacy.

In the fourth and final phase, the "act" phase, the established security and data protection strategy is continuously adapted to fit new requirements and, thus, continuously improved. The security and data protection guidelines, controls, and measures are modified if necessary. Discussions are also held with management team in this phase that serve to confirm the implementation of the Data Protection Management System, to report on the audit results, and to devise ways of improving the system. Modifications are carried out in close consultation between the data protection officer, Data Protection and Privacy, and the DPMS representatives from the individual lines of business.

When the fourth phase of the Data Protection Management System is complete, the continuous improvement cycle starts again from the beginning.

Goals of SAP's Data Protection Management System

The objective of the SAP Data Protection Management System (SAP DPMS) is to achieve and maintain an effective and high standard of data protection and data security in all lines of business and among all employees. With such a system in place, SAP proves itself to be a trusted partner to its customers. The Data Protection Management System contains instructions for all SAP employees on how to integrate data protection into their daily work.

To ensure that the content of the Data Protection Management System and its appendixes stays up to date, it is reviewed once a year by the process owner in each line of business in cooperation with the Data Protection & Privacy team.

In the data protection steering meeting, which takes place annually, the participants sign-off the strategic DPMS planning for the upcoming years. Participants of the steering meeting are Luka Mucic (member of the Executive board), SAP`s data protection officer and members of the global DPP, who are responsible for the DPMS.

Reference to Laws, Standards and SAP Guidelines

The Data Protection Management System is based on the British Standard BS 10012:2017 and on the requirements of global data protection laws and regulations and ensures adherence to these regulations. The new release of the German Federal Data Protection Act (BDSG), released on 30. June 2017, and the European Global Data Protection Regulation (GDPR) form the basis for the Data Protection Management System.

The DPMS follows also the requirements of the ISO 29100:2011 which describes the set-up of a data protection management system.

The provisions of the SAP DPMS should not contradict national laws. However, the SAP DPMS may contain regulations that are stricter than those that apply in a particular country. In this case, the SAP DPMS is valid and applicable.

...making excellence a habit.™

BS 10012:2017

British Standard "BS 10012:2017 Personal Information Management System[1]" is a specification for a personal information management system and mandates the implementation of such a system within corporate security programs. Consequently, it is subject to and ensures compliance with the regulations that make up the data protection management system. The combined certificate was developed as a British national standard by the British Standards Institution (BSI).

In its latest release, British Standard BS 10012:2017 combines British data protection regulations with the European General Data Protection Regulation (GDPR) in a management-style system. This European regulation is also the foundation for the German Federal Data Protection Act. The British standard is used because a uniform ISO standard that deals with the topic of data protection has not yet been developed. The BS 10012 standard was originally developed in 2009 to provide combined certification for a management system. It has largely revised in 2017 to cover the European GDPR.

The procedure based on BS 10012:2017 offers a variety of advantages. First, the data protection requirements are mapped in the company's processes. Second, by virtue of its alignment to a valid management system, the standard increases acceptance of data protection regulations among managers and employees. And lastly, the standard complies with the current European General Data Protection Regulation.

ISO 19011:2011

ISO 19011 is a guideline for the auditing of management systems. The standard is applicable for all organizations performing internal or external audits of management systems or which are responsible for the management of an audit program.

To this end, external audits are understood as those audits performed by the certification body as substantial part of the DPMS as well as the auditing of SAP's sub-processors performed by SAP. All audits of the DPMS are being performed according to the regulations of the ISO 19011 standard and are certified by the certification body.

[1] In SAPs context named „Data Protection Management System"

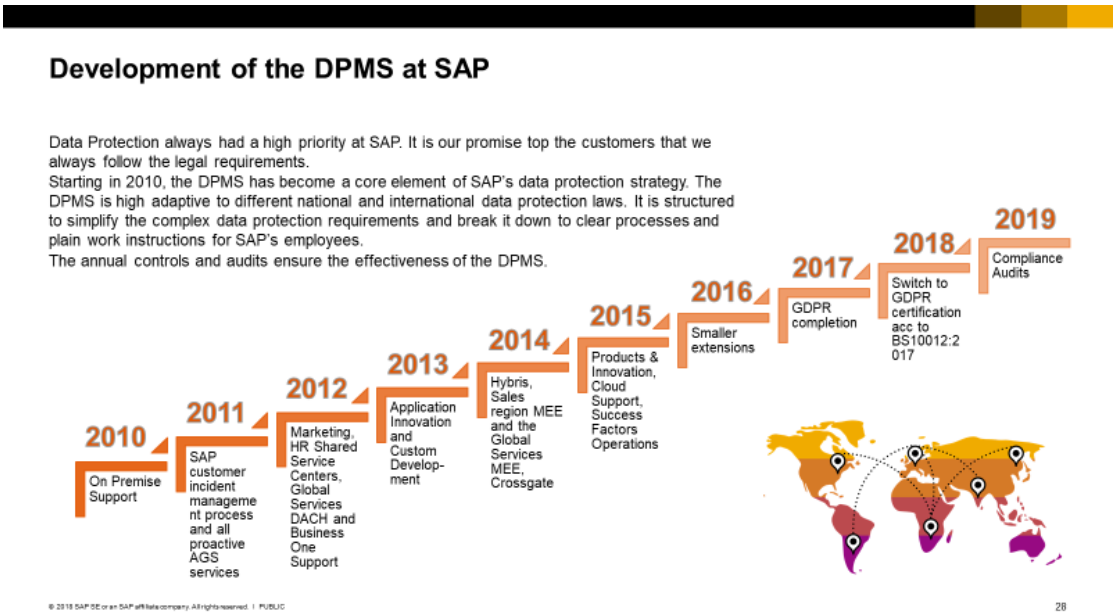
...making excellence a habit.™

ISO/IEC 27001:2017

The international standard ISO/IEC 27001:2017 specifies the requirements for creating, introducing, operating, monitoring, maintaining, and improving an information security management system, taking account of the information security risks within the entire organization. The standard is also defined as a DIN (German Institute for Standardization) standard. ISO/IEC 27001:2017 defines the requirements for implementing appropriate security mechanisms that suit an organization's needs.

The ISO standard was designed to ensure that suitable security mechanisms are selected to protect all assets in the value chain. SAP maintains various ISO 27001 management systems and - wherever possible - applies the procedures defined in ISO/IEC 27001:2017 to the relevant processes in its Data Protection Management System. If an organizational unit does not have a management system based on ISO/IEC 27001:2017, then BS 10012:2017 applies as the management system standard.

Development of the Data Protection Management System at SAP



In 2009 increasing data protection regulations in Europe, in Germany and in many other countries companies were more and more challenged to comply

...making excellence a habit.™

with the complexity of the different legislation requirements. Structured approaches became ever more important and shaped a need for an actively driven management of data protection. In addition, SAP customers started progressively verifying compliance of data-protection requirements with their respective suppliers, as well as with SAP. Until today, this is done using many different types of auditing – from questionnaires and self-assessments through on-site audits.

To make auditing as straightforward as possible for its customers and to obtain confirmation of the high standard of data protection at SAP from an independent source, a Data Protection Management System was introduced at SAP for the first time in 2010, in the SAP Primary Support department. This area was already certified according to ISO 9001 and ISO/IEC 27001 before the Data Protection Management System was introduced. In order to address its customers' accountability obligations more effectively, SAP not only implemented the new management system, but also had it tested and certified by an independent body, the BSI (British Standards Institution).

In 2011, the Data Protection Management System was extended. Adding to the certification already awarded to Primary Support, the Installed Base Maintenance department and Development Support were also certified. As a result, the entire on-premise delivery message-handling process is included in the Data Protection Management System.

In 2012, four more lines of business were subjected to the data protection certification process: Global Services (with processes in the near-shore and off-shore centers); the HR Shared Services Center; the Global Marketing department; and Business One Support.

The scope of the data protection certificate was extended also in 2013. For some of the covered units new locations were added. Initial implementation was done in Custom Development and Products & Innovation the development unit of SAP.

In 2014, Global Services in the region MEE and the Sales organization were initially certified by the DPMS. In addition, it was the first time to implement the DPMS in parts of acquired companies like SAP Customer Experience and Crossgate.

The development of the DPMS focused in the year 2015 on the cloud services and was extended to Cloud Support, Managed Cloud Delivery and SAP Success-Factors Cloud Operations. Current areas have been extended like Global Consulting Delivery (11 new locations) and Products & Innovation (16 new locations).

In 2016 the last missing departments were brought under the operation of the DPMS making it the first certificate of SAP covering all board areas with one standard.

2017 and 2018 were focused on the adaption of the DPMS to the new released European data protection legislation, the General Data Protection Regulation (GDPR). All processes have been reviewed, adapted were needed or new processes were implemented. The company guidelines for data protection – as manifested in SAP's General Book of Data Protection (GB) – were changed to the new legislation. In addition, the GB has been changed to the new version of the BS10012:2017 standard. In order to comply with the higher risks caused by the new penalties of the GDPR, a new type of audits was developed (compliance audits) and executed on board level for the first time in 2018. Starting in 2019, DPSM will focus on risk-based audit structures, mainly to check on compliance. Awareness audits will also be continued but in a reduced sample.

In 2019 the focus of the DPMS was further pointed towards general process compliance. Therefore, only questionnaire audits were conducted to check on the data protection awareness of the employees. In parallel a global training was set up, rolled out and mandatorily provided to all SAP employees. The training comes with a data protection skill assessment which will replace the awareness audits for the future. Consequently, the role of the data protection representative is not mandatorily required by the DPMS anymore. However, it is recommended that the LOB's keep the network to strengthen the data protection awareness in a sustainable way.

...making excellence a habit.™

For the first time, the audit plan was not based on employee numbers, but created with the help of LOB specific data protection risk assessments.

Width of the annual risk assessment – content layer

Question	Unit A	Unit A	Unit A	Unit A
Is personal data being processed in the L1 unit?	Yes	Yes	Yes	Yes
From the unit point of view, is a Data Protection Compliance Audit required?	yes	yes	yes	yes
If you think that no Data Protection Compliance Audit is required, please explain why.				
How many people in the unit are processing personal data? (rudimentary number)	66	1200	700	2600
Are special categories of personal data processed?	no	yes	no	no
Whose personal data is processed?	only internal data subjects	internal & external data subjects	only internal data subjects	only internal data subjects
Is personal data transferred outside SAP?	no	no	no	no
Are external service providers used by the unit?	yes	yes	yes	yes
Does the unit itself collect personal data?	yes	yes	yes	yes
Are externally accessible webpages operated by the unit?	no	no	no	no
Is the unit responsible for own developments?	no	no	no	no
How would you rate the overall Data Protection risks?	low	low	low	low
Calculated risk level:	medium	high	medium	medium
How is the risk estimated by DPP?	High	High	medium	High
Audits required (to be specified by DPP)	C and A	C and A	C only	C only

© 2018 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC

C = Compliance Audit
A = Awareness Audit 22

Major Changes of the DPMS to comply with the EU GDPR

Integration of GDPR requirements into the DPMS

With the introduction and implementation of the GDPR, the DPMS structure needed to be changed accordingly. As a first step the "General Book of Data Protection" was changed and extended to cover all GDPR aspects.
Significant changes have been made to

- Audit structure, types and methodology
- Management review
- Data Protection governance (roles and responsibilities)

Further, the chapters seven new chapters have been added:

- 15 Records of processing activities
- 16 Data Protection Impact Assessment (DPIA)
- 17 Privacy by Design and Default
- 18 Privacy Statements
- 19 Consent Management
- 20 Management of Personal Data Breaches
- 21 Data Subject Rights

...making excellence a habit.™

All changes and extensions have been supplied with new controls.

Adaption of the new BS 10012:2017 standard

In order to embrace the enforcement of the GDPR, the British Standard Institution has decided to publish a new version of the BS 10012 Standard. The version BS 10012:2017 comprises all new requirements which came with the new European regulation. The new standard needed to be implemented into SAP's DPMS as well, which led to additional changes of the General Book. In particular, a reference table of the new standard and SAP's General Book was added and reflected in chapter 22.2.

Transition to and certification of the new BS10012:2017 standard

After all changes were completed, BSI conducted a transition audit of SAP's changed DPMS. The transition audit was successful, and SAP won one of the first BS 10012:2017 certificates ever in March 2018. The new certificate was announced in a joint press release of BSI and SAP and announced at SAPPHIRE in Orlando as well.

Adaption of the audit structure

Since the DPMS was established in 2010, the focus was always on the data protection awareness of SAP's employees. The GDPR requires a higher control of all data protection relevant processes and how the legal requirements have been integrated into business processes. To satisfy this aspect on one hand and to perform a GDPR readiness check as well, DPP introduced the "DPMS Compliance Audits" as a new audit type. The compliance audits have been designed to address and control the major DPMS requirements on board level. Based on a specific questionnaire DPP performed the first 13 compliance audits – one for each board area and five for the board area of CBG.

The audit results have been reported to the corresponding GDPR project leads and the resolution of the findings have been regularly monitored by DPP. The new audits type was very successful by creating good transparency on the implementation status for all GDPR requirements.

...making excellence a habit.™

Based on the positive reception, it was decided to not only continue with the new audits type, but to extend it and make it the focus of all DPMS control activities for the future. Thus, a board areas specific data protection risk assessment will be used for each L1 areas of each board LoB. Based on the risk assessments, the audit landscape and the level of details, audits have to be conducted for the L1 area, will be determined. Awareness audits will be planned with a reduced scope and with an increased usage of questionnaire-based controls.

Adaption of the governance model

The effectiveness of the DPMS is mainly based on the support of the LoB, which is driven by the DPMS governance model comprising of the DPMS Accountable and the DPMS Coordinator. For the GDPR implementation project each board area has nominated a project lead in addition to the existing DPMS roles. In order to ensure that the DPMS governance model covers all GDPR aspects in the future, the scope for all DPMS roles have been extended to the GDPR tasks, combining the fading out GDPR project and switching the GDPR project into an operational mode for the future. The changes have been introduced to and accepted by the Management Accountable and to the Coordinators of each board area during the annual DPMS management review calls.

Organizational scope of the DPMS

The requirements of the Data Protection Management System and the corresponding guidelines are geared to the processes in the individual board area that handle personal data. The following SAP board areas are in scope in 2019:

- Digital Business Services
- Technology & Innovation
- Human Resources
- Global Customer Operations
- Office of the CEO
- Cloud Business Group
- Intelligent Enterprise Group
- Global Finance & Administration
- Product Engineering

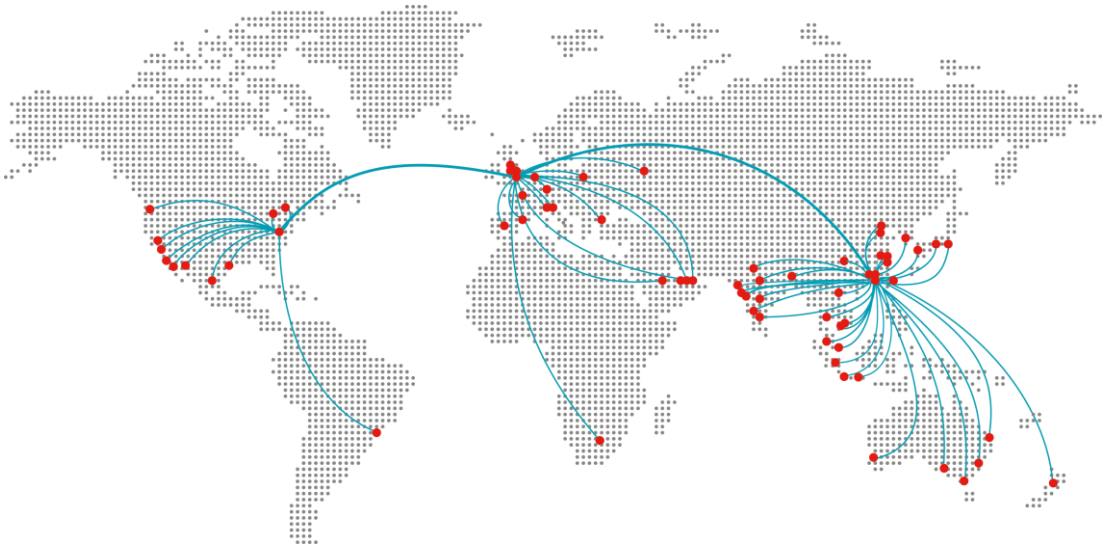
...making excellence a habit.™

Certification Process

Partner BSI

The British Standards Institution (BSI) is a global business improvement company that develops standards and provides training, auditing and certification amongst others on risk, quality management systems and sustainability standards. In accordance with its motto "making excellence a habit", BSI helps its customers all over the world to achieve success by enabling excellent performance through the implementation of standards.

BSI was established in 1901 as the Engineering Standards Committee and was the first national standards body. It now has over 4,600 employees in 90 offices and is the British member of the International Organization for Standardization (ISO). BSI has around 84,000 customers in more than 190 countries, is headquartered in London, with Howard Kerr as its chief executive.



In addition, the company's range of services also includes innovative software solutions for management systems, cyber security and product certification where BSI is famous for its marks of excellence, including the Kitemark® and CE quality marks. As a developer of standards on highest quality level for national and international clients, BSI publishes about 3000 standards each year.

BSI worked with SAP to devise SAP's Data Protection Management System.

...making excellence a habit.™

BSI helped produce the international standard ISO/IEC 27001. In 1992 the United Kingdom's Department of Trade and Industry (DTI) set up a commission to identify accepted best practices in information security. The findings were published as a Code of Practice in 1993, which was amended and republished by the British Standards Institute in 1995 as BS7799:1995. Since 1999 there has been a standard against which practices can be measured. In 2000, the International Organization for Standardization (ISO) adapted part 1 of ISO/IEC 17799:2000. ISO/IEC 27001:2005 was first published as an international standard on October 15, 2005.

BSI Group:

- Devises national and international standards
- Audits and certifies second- and third-party management systems
- Verifies and certifies products and services
- Provides software solutions for management systems
- Provides training courses on all standards relevant worldwide
- Provides the British Standards Online service, a bibliographical online database of over 50,000 national and international standards

BSI is known and recognized internationally for its independence, integrity, and innovation in creating standards that ensure best practice and excellence. BSI is the world's third-largest certification company.

Audit Methodology

All processes and Board Areas of SAP are subject of being audited using the given criteria of the BS 10012:2017 and the DPMS. In accordance with the generally accepted audit criteria ISO 9001 and ISO/IEC 27001, samples are determined from the departments and locations, from the employees surveyed, from the documentation and records, and from the implemented measures. All audits are conducted according to auditing principles, with management involvement, and in compliance with ISO 19011 and ISO/IEC 17021. ISO/IEC 17021 sets out requirements for certification bodies providing management system certification and involved auditors.

...making excellence a habit.™

BS 10012:2017 certification is currently acknowledged by the United Kingdom Accreditation Service (UKAS) and the Information Commissioners Office (ICO). A final accreditation for BS 10012:2017 is in preparation but depending of agreements regarding Article 43 of GDPR.

Training

SAP has announced 2 mandatory trainings for the entire group of employees covering the topic of data protection and privacy. The "Human Firewall" training covers the security aspect of processing of personal data. It was initially released in 2012 and everybody had to take a short test upon completing the course. As the title suggests, the course highlights what employees can do to protect the company through their own conduct and by being security-aware. In 2015, a revised Human Firewall Campaign was released in the entire organization. With an additional anonymous quiz each employee can test the data protection knowledge.

Beginning of 2018, the "Compliance Baseline Training" has been rolled out. This mandatory training is about legal compliance, intellectual property compliance, communication, data protection and privacy and security. As well, every participant has to take a short test for completing the course.

In order to drive data protection awareness on a broader scope, a mandatory data protection training has been created and mandatorily rolled out to all SAP employees in 2019. This training comprised of data protection principles, which are relevant to all employees. The training always ends with a data protection skill assessment, which will be in the main control instrument for data protection awareness at SAP in the future.

It is the responsibility of the business unit to ensure that employees are informed about data protection guidelines regularly. This must happen independently of the internal and external audit program. All new hires have to pass the mandatory and business unit specific data protection related trainings as well. Should processes involving personal data change, employees' knowledge must be refreshed accordingly.

Control of Technical and Organizational Measures

One part of the Data Protection Management System covers the control of the technical and organizational measures (TOM), which are designed to protect personal data when it is stored, processed, and destroyed. The audits examined these TOM's by looking at the required controls and whether they have been implemented effectively and appropriately.

Physical Access Control Mechanisms

The external audit found that the buildings, facilities, and rooms at SAP are effectively protected against unauthorized access. The internal security department determines the appropriate controls based on the security level of the building. Here, door-locking systems (chip card access system) have been deployed together with active key management.

Every SAP location has its own house rules that set out additional measures to prevent access by unauthorized persons. When the company optimized access controls, it issued different language versions of the house rules, which also contain instructions on handling visitor passes.

Depending on the security level, additional controls protect buildings and parts of buildings, such as special access profiles, video surveillance, intruder alarms, security revolving doors, and biometric access control systems.

Access rights for authorized persons are granted individually in accordance with the criteria specified. Only authorized SAP personnel and contractors receive passes to access buildings. SAP employees and external staff are required to wear their identification while on SAP premises. Guest and visitor access to SAP buildings is documented, and they are only permitted access when accompanied by SAP employees.

System Access Control Mechanisms

All the audited IT systems are secured against unauthorized access through personalized login procedures. Authorization is enforced at all levels of the relevant system. There are authorization rules in which the processes for approval, deletion, and modification are described. Each user has a separate ID with which he or she accesses SAP's systems. If a user leaves the company or his or her role changes, access rights are revoked.

The security guideline on passwords forces users to handle system login securely. The domain password must be changed at least every six months, and this is technically enforced. Default passwords must be changed before users start working with a system. Every computer has a password-protected screen-saver that is activated automatically when the computer has been inactive for a short interval. This means that when the employee returns to his or her desk, he or she must enter a password to continue working on the computer. This prevents unauthorized access.

Remote access to data is regulated using two-factor authentication. Here, encryption technology is used when data is transferred. The SAP firewall protects the company network from the public network. To keep the firewall up to date, Global IT regularly installs system updates on all company computers. To optimize system access standards across the company worldwide, SAP raised employee awareness of system security. The company ran a number of campaigns in which employees received feedback on how they work and how their conduct might enable unauthorized persons to access company systems.

Data Access Control Mechanisms

Both in the operating systems audited (Windows and so on) and in the specific SAP support systems, access to customer data and other personal data is regulated by a dedicated role and authorization concept and a stringent authorization process in which access is granted for a short period only.

Access to data and systems belonging to customers and partners is provided on a strictly need-to-know basis. Employees may view confidential data only if there is a specific business need to do so. Data belonging to business partners and customers to whom SAP employees have access during their employment is treated as confidential.

Access to data processing systems is subject to strict requirements for personnel and is governed by a global authorization system. Authorizations are not assigned automatically; they have to be specifically requested and approved by all relevant persons.

Once an authorization has been granted, it is usually valid for not more than three years. Critical authorizations have a more restricted term of 18 months. If authorizations are not extended before this term elapses, they are automatically revoked. This control mechanism prevents critical authorizations from being extended without being checked.

In-house, SAP uses a single-sign-on system (SSO), which is service that provides secure system login. With Single Sign-On, employees are granted access to all systems relevant to them in accordance with their role and the associated authorizations following a single logon in the SSO system using their user ID and password. After a specified number of failed attempts, logon to the SAP systems is blocked. If the password is entered incorrectly too many times on smartphones, the data is deleted from the smartphone.

So that employees can log in to SAP systems securely outside of SAP premises and SAP networks, SAP uses a two-factor authorization system valid worldwide involving SecurID cards or a soft token. These allow secure access to internal and external networks, VPNs and WLANs, e-mail, Microsoft Windows desktops, Web servers, and other networks. The SecurID card and soft token remain the property of SAP. They can only be used by the person to whom the card was issued and must be returned to SAP or deactivated when that person's employment contract ends.

The user management process concerns all activities related to setting up, assigning, and terminating roles, including the associated rights and authorizations. This process is largely automated and is based on the SAP Identity Management System and Access Request Management (ARM). Data classification, access procedures, profile administration, and user management together ensure a secure authorization lifecycle.

- Regular deletion: The user data of employees who are leaving the company is largely deleted automatically.

- Special deletion: A separate procedure applies if managers need to block user rights for internal or external users immediately. User management blocks user access to the appropriate systems. This procedure ensures SAP can lock users immediately, and these users lose all rights in SAP systems.
- Control mechanisms for restricting critical authorizations: Authorizations and roles assigned to users in the SAP financial system are checked at least once a year for critical authorizations.
- SAP security guidelines for the use of external systems: External systems are connected to the SAP network only in exceptional circumstances and providing that this is urgently required for business reasons. All external systems that are connected to the SAP network are registered accordingly. The external system must never relate to other non-SAP systems.

In the SAP Security Policy, the minimum classification for customer information is "confidential." Access to customer's IT systems generally takes place using remote support, and the following security guidelines apply:

- The Internet remote connection is usually set up using Secure Network Communication (SNC) or virtual private networks (VPN). Both options use various security measures to protect customer systems and data from unauthorized access: strong encryption, user authentication, and access control technology.
- The Secure Area of SAP Support Portal enables customers to transfer access data and passwords. The Secure Area has extra access protection and all access to it is logged.
- SAP customers always have control over the connections they set up to SAP for remote support. SAP employees cannot access a customer system without the knowledge and active support of the customer.

All SAP personnel and contractors are bound in contract to treat all sensitive information, including trade secrets of SAP and partners, as confidential.

Data Disclosure Control Mechanisms

SAP uses encryption as the main method of protecting systems and data when it transmits protected and sensitive customer data. SAP rolls out encryption software worldwide to protect e-mail communications with customers. Any

exceptional unencrypted communications identified in the audit were in accordance with the express wishes of the customer concerned.

The data transferred from SAP's network to other, outside networks is encrypted as described in SAP's technical and organizational measures. When data has to be physically transported, adequate means (such as encryption, sealed containers, and others) are available to ensure agreed requirements are met.

Protected information stored on hard disk is encrypted using Pretty Good Privacy (PGP) at SAP. SAP personnel can protect confidential information in Microsoft Office files using Microsoft Rights Management Services (RMS). Only specified teams can use the RMS file decryption capabilities.

Input Data Control Mechanisms

SAP permits only authorized persons to access personal data in their work. Entry, modification, and deletion of data is recorded using log files. This applies also when customer systems are accessed.

To check whether data protection and data security regulations have been observed in SAP systems, access to the log files is required. Access to these files is kept to an absolute minimum and granted only to a restricted number of employees.

Outsourced Data Processing

Sub-processors regarding the DPMS are 3rd party vendors (supplier, partner) processing personal data on behalf of SAP. SAP has set up a system to centrally assess all sub-processors worldwide, checking and auditing them according to the agreed Technical and Organizational Measures (TOM) and the requirements of the German Federal Data Protection Act section 11.

SAP's own quality standards and international regulations demand the greatest care in the selection and monitoring of sub-processors. To ensure all sub-processors meet protection and security requirements for personal data, SAP implemented the Sub-processor verification process.

All of SAP's sub-processors (suppliers, vendors partners, etc.) – dealing with personal data - must be audited. They are referred to as sub-processors below.

The process comprises three main steps:

- Contractual compliance with sub-processor
- Sub-processor self-assessments
- Sub-processor onsite audits

As described above, SAP has introduced an audit process to check that all sub-processors meet the legal requirements and standards. The determination of the data protection relevance for each sub-processor is part of the contract management work. This task is done for each new purchase, for each new contract and for each new sub-processor. The ordering parties who manage the contracts, determine whether the sub-processor processes any personal data, or delivers maintenance on behalf of SAP to SAP or any SAP clients. If so, SAP must verify the compliance of the sub-processor with the German Federal Data Protection Act. The SAP organizations verify the contractor using the three-step process:

Step 1: Contractual compliance
The responsible organization sends the Data Protection Agreement (DPA) in its current version, released by Global Legal and DPP to each sub-processor identified in the preparatory step. The DPA comprises of two major documents, the Master Data Protection Agreement (MDPA) and the order specific appendix and is usually provided in the form of an addendum to the sub-processors' contract. Sub-processors are only allowed to process personal data or to provide maintenance, if they have signed the data protection agreement (see Step 1). The DPA specifies the data subjects and the type of data (Data subjects, categories of data and special categories of data sections) accessed by the sub-processor. It also obligates the sub-processor to SAP's global TOM's. The agreement has to be signed before any goods are delivered or services provided.

If the sub-processor does not sign the data protection agreement or does not sign it in time, the ordering organization has to find a substitute vendor or to commence the escalation process.

Step 2: Sub-processor self-assessment
As well as having to sign the agreement, the sub-processor has to undergo an initial check proving that sufficient technical and organizational measures have

been implemented. This check is done as a self-assessment provided as an online survey to the sub-processor.
Once the survey is completed and returned to SAP, the DPP organization analyses the responses to the questions and sends the evaluation report to the responsible organization. A successful rated self-assessment is the prerequisite for doing business with the subcontractor in question.

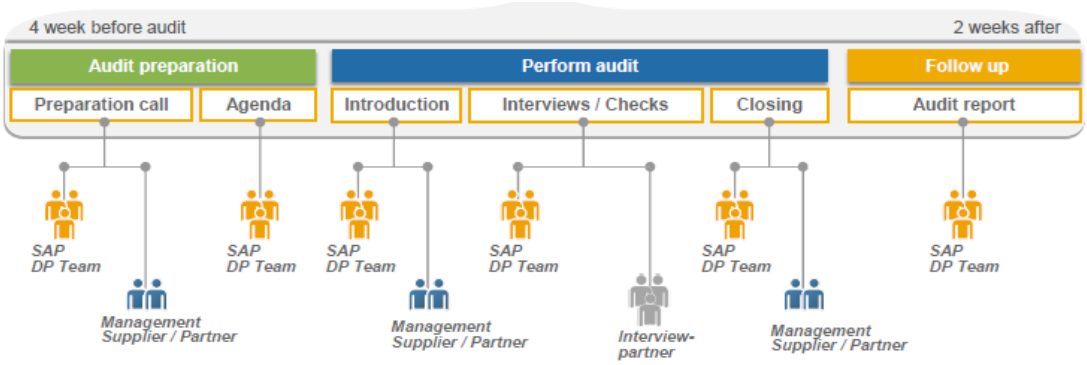
If the sub-processors' survey result is rated insufficient (red), the ordering organization must find another sub-processor or to commence the escalation sub process. A self-assessment is valid for two years. SAP automatically commences a new check at or before the end of that period. If there are reasons to suspect a sub-processor is in breach of the data protection requirements, a new check can be initiated earlier.

Step 3: Sub-processor onsite audits
As an additional step, all sub-processors can be subject to onsite audits. The decision for executing an onsite audit depends on various criterions like business footprint, the sensitivity of the accessed data, the self-assessment results and so on. DPP receives a list of candidate subcontractors, and with other departments in SAP, such as GPO and Global IT, decides what sub-processors will be audited onsite in addition to the self-assessment.

Every audit must be arranged, planned, and scheduled in consultation with the sub-processor. The audit regularly takes one to three days and includes discussions with management, the data protection officer, and personnel. It also comprises of an examination of documents, a site-check and a physical inspection of the technical and organizational measures the subcontractor has in place to ensure proper data security and protection.

In general, this type of audits is conducted onsite, additionally one or more of a sub-processor's locations may be audited remotely. All audit documents, such as agendas, reports, and the findings of checks and inspections, are retained.

SAP's generic sub-processor audit process:



SAP's Generic Supplier Audit Plan

Availability Controls

The systems operated by SAP's support organizations have multilevel backup systems and redundant system components to be able to ensure business continuity when needed. For example, the data centers have an uninterruptable power supply.

Segregation of Data Processing

All support systems have appropriate client separation, supported by the authorization rules used in the audited systems.

When support services are provided, personal data from different customers is separated physically or logically. It is also ensured that data collected for different purposes can be processed separately.

SAP does this by using the technical capabilities of the deployed software (multitenancy, separate system landscapes for production, quality, test, and development systems) to bring about data separation.

If a customer's data is required to process a message from that customer, the data is assigned to that message and used to process that message only; such data is not used to process any other message.

This data is stored in dedicated support systems.

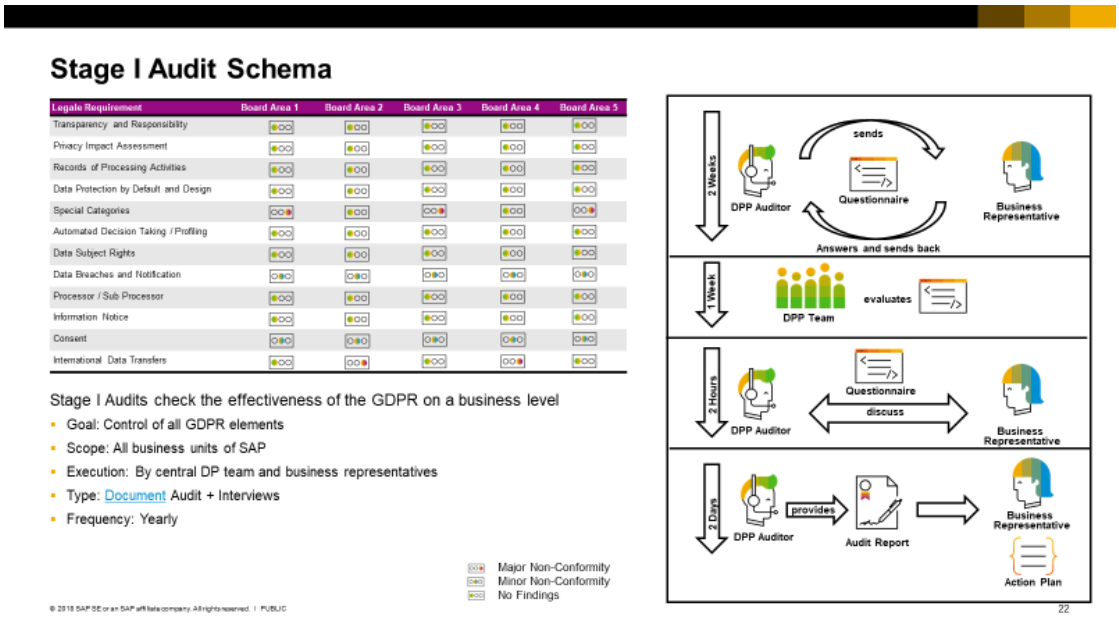
...making excellence a habit.™

General Audit structure and types

This chapter describes the different audit types and the finding classifications used by the SAP DPMS.

Internal Audits of the DPMS – Compliance

To ensure that a business unit is compliant with all data protection requirements, DPP executes compliance audits for every L1 unit that has been selected according to the result of the data protection risk assessment. During the preparation phase, DPP sends a detailed agenda and questionnaire to the Data



Protection Coordinator and/or Unit Coordinator. They are in charge to provide the required documents and information. Within a 2 weeks period, the questionnaire has to be completed. The DPP auditor team evaluates the given information and prepares the questions for the interview audit. During the interview open topics or questions are clarified so that the DPP auditor can judge every data protection topic that is relevant for the business unit. A few days later the DPP auditor provides the final audit report to the Data Protection Coordinator and/or Unit Coordinator.

Goal of the compliance audits is to ensure the adherence to all data protection requirements for each L1 business unit.

...making excellence a habit.™

Internal Audits of the DPMS – Awareness

The following diagram shows the generic internal audit schema for awareness audits in accordance with the PDCA cycle. The audit schema has three phases: audit preparation, conduct of the audit, and audit follow-up. The local DPMS representative works with Data Protection and Privacy to prepare the audit. Besides the organizational aspects, they identify and prepare the employees who are to be audited. These parties are closely involved in the audit itself. Local management is also audited. All parties attend the opening and closing meetings. As for the audit preparation phase, Data Protection and Privacy has overall responsibility, as it writes the audit report and monitors the corrective actions. Data Protection and Privacy is available for consultation.

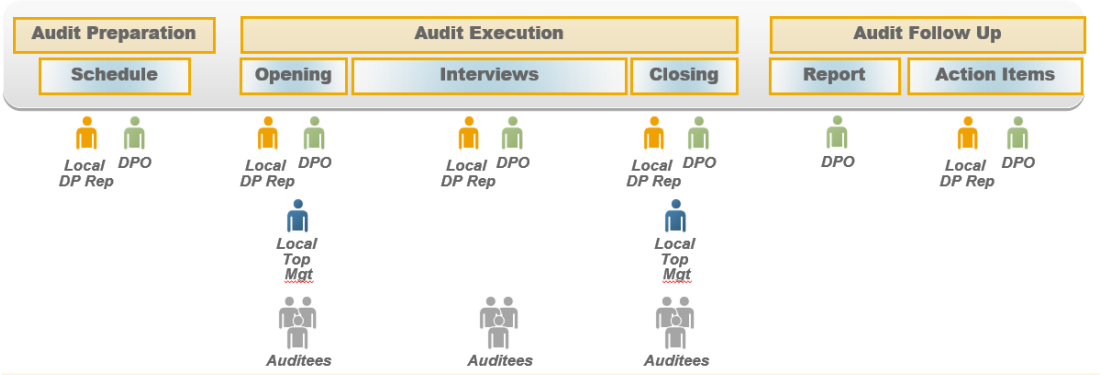
Offices were inspected in all on-site audits. All other items on the agenda were covered in both on-site and remote audits.

The aim of the sample is to audit all relevant locations at least once every three years. An initial certification audit is conducted in the first year in which a business unit is audited. This is a larger audit in terms of locations and the number of people involved. Surveillance audits start from the second year of certification. Under the general certification rules of ISO/IEC 17021 recertification takes place in the third year in the appropriate area. As for the initial certification, recertification involves more audit days and covers more locations.

The findings of the documentation audits, office inspections, and interviews were recorded appropriately. Data Protection and Privacy retains and archives the findings. The same applies for all supporting documentation provided to the external auditors during or after the audit.

The respective facilities were inspected, notably building entrances, offices, printer rooms, and the equipment in these rooms for disposing of records, meeting and conference rooms, server rooms and data centers.

...making excellence a habit.™



Generic Internal Audit Plan Following the PDCA Cycle

Sample agenda for the internal audit; each agenda covers one working day:

Auditees / Participants	**Standard / Process**	**Lead Auditor of DPP**	**Co Auditor of DPP**
All	***Opening***	Lead Auditor	Co Auditor
Manager	Interview with local management	Lead Auditor	Co Auditor
DPMS Representative	Interview with DPMS repre-sentative	Lead Auditor	Co Auditor
	Onsite inspection / Work-space inspection	Lead Auditor	Co Auditor
Employee 1	Interview with employee	Lead Auditor	Co Auditor
Employee 2	Interview with employee	Lead Auditor	Co Auditor
Employee 3	Interview with employee	Lead Auditor	Co Auditor
All	***Closing***	Lead Auditor	Co Auditor

Sample General Internal Audit Plan

Internal Audits of the DPMS – Questionnaire

Internal audits can be performed as questionnaire audits as a substitute for an internal audit. These questionnaire audits are executed as DPMS questionnaire audits.

...making excellence a habit.™

Specifics of the DPMS questionnaire audits

This audit type is used as a substitute for the regular annual internal audits. It will only be offered to locations which demonstrated flawless audits and good cooperation in past audits. A questionnaire audit can be actively requested via email by the local representative, the request will be evaluated and decided by DPP. A questionnaire audit cannot be requested for two consecutive years.

General rules for the DPMS questionnaire audits

The number of DPMS questionnaire audits counts towards the number of remote audits (max 50%) and is limited to a maximum of 20% of all remote audits conducted in a given audit cycle. At least 8 participants per location are required (as only anonymous results are evaluated). For each participating location DPP evaluates the anonymous results of the underlying questionnaire audit, creates an audit report and provides it to the responsible DPMS Representative. Passing the questionnaire audit successfully, no further onsite/remote audit is necessary at the participating LoB in the current audit cycle.

Setup of the questionnaire audits

For each Lob a set of questions and answers is developed by DPP as basis for the questionnaire audit. All questions are derived from content/work instructions given in the DPMS General Book/LoB specific DPMS Appendix of the concerning LoB. The questionnaire audit is based on these questions and answers and is implemented by the SAP Online-Survey Management Team.

The LoB together with the responsible DPR nominate the participants for each location and the DPMS Representative forwards the list of participants to the SAP Online-Survey Management Team. To start the questionnaire audit, the SAP Online-Survey Management Team sends out invitation e-mails to the nominated participants containing individual links.

The typical duration of a questionnaire audit is 2 weeks. DPP aligns the exact start and end date with the DPMS Representative in advance.

...making excellence a habit.™

After the questionnaire audit ended the SAP Online-Survey Management Team provides the anonymous results for each location to DPP if a minimum of 8 persons participated in the questionnaire audit per location. If the number of participants is less than 8 per location, it would be necessary to conduct an onsite/remote internal audit at the given location.

DPP evaluates the anonymous results and creates the audit reports according to the current evaluation guidelines. DPP provides the audit report to the responsible DPR of the participating unit. In case of major non-conformities, a follow-up internal DPMS audit has to be performed either onsite or remotely.

The current evaluation metrics of questionnaire audit results (per location) is described in a separate document. In accordance with the BSI classification for audit findings, the findings are based on thresholds:

Threshold for observations (per question): if 50 % <= calculated % < 75 %
Threshold for minor non-conformity (per question): if calculated % < 50 %
Threshold for major non-conformity: to be evaluated by DPP (several aspects can be taken into account, no automated evaluation possible)

...making excellence a habit.™

Audit Question Catalog

The following question catalog is used as a guide for internal and external audits. Questions are taken from the catalog, but auditors are free to focus on certain topics and ask questions that are not in the catalog, or to focus on topics not covered by the catalog.

- General Information
  - Please introduce yourself briefly (name, position, org chart etc.)
  - Please describe what your organization does...
  - What do you understand by data protection?
  - Where do data protection and confidentiality come in to your everyday work?

- Data Protection and Data Security
  - In your organization, who is responsible for data protection and security?
  - How do you liaise with your local DPMS representative, global DPMS coordinator, and with DPP?
  - How do you raise awareness of data protection and security in your organization?
  - When and how often are courses held on data protection and security? (Records of team's course attendance)
  - How do you ensure that changes in data protection and security practices are communicated to everyone?
  - Where can employees find DPMS documents and security policies?
  - How do you check whether employees follow data protection and security policies?

- Questions on Technology and Organization
  - How are data protection incidents dealt with? How should employees respond to a data protection incident?
  - How do you ensure that your employees are able to classify information (such as documents and emails) correctly in terms of confidentiality?
  - How often are employees permitted to work remotely?
  - Which security policies apply to employees when they work remotely?

  - What is the "clean desk policy"?
  - How are printed confidential documents disposed of securely?
  - How are computers secured on which personal data is stored?

- User Management
  - How are access rights granted to the IT systems of SAP?
  - How often access rights are reviewed?
  - What procedures are in place for reviewing and changing access rights when employees change departments or roles?
  - How are data protection and security covered in employee onboarding?

Auditee: DPMS Representative

- General Information
  - Please introduce yourself briefly (name, position, org chart etc.)
  - Please describe what your organization does.
  - How did you become the DPMS coordinator or representative?
  - How do you liaise with local management, DPP, and your global DPMS coordinator?
  - As a percentage, how much of your time is taken up by DPMS coordinator or representative tasks?
  - Are your tasks as DPMS coordinator or representative jointly agreed objectives in the PRM tool?

- Data Protection Management System
  - When DPMS was officially rolled out in your organization?
  - How do you ensure the DPMS appendix is kept up to date?
  - Where are the DPMS documents (general book and appendix) stored?

- Training and Awareness
  - Are training courses on data security held for SAP employees? If so, please state how often and for whom?
  - Do you keep records on who has attended DPMS training courses?
  - What have you done in the past year to maintain or improve data protection awareness?

- How do you roll out changes to the DPMS documents to SAP employees?
- What procedures are in place to ensure local training course material is updated as necessary?

- Risk Assessment
  - Do you conduct data protection risk assessments regularly? If so, please state how often and the scope of these assessments.
  - How do you document identified risks and the plans to mitigate them?

- Incident Management
  - Please describe the process for responding to data security incidents.
  - Please demonstrate the Security Incident Management tool.

Auditee: Employee

- General Information
  - Please introduce yourself briefly (name, position, org chart etc.)
  - Please describe your duties (in relation to DPMS processes).
  - What do you understand by data protection, confidentiality, and security?
  - Where do data protection and confidentiality come in to your everyday work?

- Security and Data Protection
  - Have you heard about the current Data Protection Management System? Please show me how to find it.
  - When did you last complete a training session on security and data protection?
  - Are you able to classify information such as documents and emails by its sensitivity? What information and procedures have you received?
  - How is personal data classified?
  - How do you share personal data with others? (by email, by saving the data as a print-out)

  - How do you dispose of or destroy confidential documents that you no longer require?
  - What do you do with confidential documents when you leave your work station?
  - Who is your local contact for data protection matters?
  - How was it announced in your organization that this particular person was your DPMS representative or coordinator?
  - Have you been aware of or involved in a security or data protection incident?
  - What would you do in the event of a data protection incident in your organization?
  - Please demonstrate the Security Incident Management tool.

- Training and Awareness
  - Which training courses on data protection and security have you attended recently? Please state how often you attended such courses and what they covered.
  - Where these courses are formally documented?
  - What have you done in the past year to maintain or improve data protection awareness?
  - How were you informed about changes to the DPMS documents?

- Password-Security
  - Under what circumstances may you share passwords with others?
  - What are SAP's policies on passwords?

- Physical Access and Logical Access Controls
  - When you are in SAP buildings, where do you have your employee ID card?
  - How do you protect your computer from unauthorized access?
  - What additional measures do you have to take when you are working at a non-SAP location?
  - How do you protect personal data stored on your computer?
  - Do you save personal data on an SAP server? Are there authorization rules for this server?
  - How do you protect your notebook from theft and loss? (at the office, when traveling on business)?

  - Are you permitted to install any software on your computer?
  - What do you do if you have invited a visitor to SAP's facilities?

- Secure Disposal of Material and Data
  - How do you ensure that records (paper or electronic) containing personal data that is no longer required are destroyed securely and permanently?
  - How do you prevent employees from leaving documents containing personal data on company printers?
  - Does your location have secure methods of disposing of paper records?

- DPMS Work Instructions
  - Which DMPS work instructions did you learn about in training sessions or from reading the document?
  - How do you classify personal data in your daily work How do you classify personal data in your daily work?
  - Why does the policy state that personal data should be saved in SAP systems, and on servers, and so on (SAP environment)?
  - When you are working in SAP systems, how do you obtain the authorization you need?
  - Do you regularly have to have your authorization in SAP systems renewed, or do you have authorization permanently?
  - When you have to share personal data with other SAP employees how do you make sure the person you are sharing this data with is authorized to have this data?
  - How do you encrypt personal data when you communicating with customers or contractors?

Auditee: HR representative (optional)

- General Information
  - Please introduce yourself briefly (name, position, org chart etc.)
  - Please describe what your organization does.

- HR's Role in Hiring, Internal Transfers, and Dismissals
  - How are data protection and security covered in employee onboarding?

- Do all employees have a duty of confidentiality (section 5 of the German Data Protection Act) clause in their employment contracts?
- What procedures are in place to ensure that an employee's authorizations and profiles are changed or removed if he or she transfers internally or leaves the company?
- What does HR do when an employee leaves the company?

If required, the auditor could always follow audit-trails arising in the audit.

Inspection

- Building Use
  - Is the building used only by SAP/The building or shared with other tenants?

- Entrance
  - How is the entrance secured (access controlled by employee ID cards at security revolving doors, turnstiles, doors, and so on)?
  - Are video surveillance cameras or alarms, or both, installed at the entrances to buildings?
  - Are there warning signs informing people that an area is under video surveillance?
  - What is the procedure if an employee has forgotten or has lost his or her ID card?
  - If visitors are permitted to access buildings, do they have to report to the front desk and sign in there, and sign out when they leave the building?
  - If visitors are permitted to access buildings, do they have to wear a visitor's badge so that they can easily be identified as visitors?
- In the Office
  - Are laptops secured against theft?
  - How are documents containing personal data protected from prying eyes when desks are unattended?
  - Are there lockable office cupboards and cabinets?
  - Has the secure printing function been activated and do employees use this function?

- Printer Room and Disposal of Documents and Data Carriers
    - Does the document shredder meet the security guideline?
    - Are any documents containing personal data left on or near printers?

- Meeting and Conference Rooms
    - Are any documents containing personal data left in these rooms?
    - Are the whiteboards wiped clean after meetings, and used flip-chart paper removed?
    - Can SAP's internal network be accessed in customer conference rooms?

- Server Room and Data Center
    - Is there is a separate access system and are there separate authorization rules? Are these actually used?
    - Is there a fire suppression system, and is it maintained properly?
    - Are there any flammable materials in the room?

...making excellence a habit.™

Audit Finding Classification SAP

Data Protection and Privacy performs the internal audits as an independent organization. The definitions of the possible audit findings are in accordance with the British Standards Institution and international accreditation schemes.

A *Major Nonconformity* is defined when there is an absence or a total breakdown of a system or control to meet a requirement. Several minor non-conformities against one requirement can represent a total breakdown of the system and thus be considered a major non-conformity. The organization is asked to implement a corrective-action within an agreed timeframe of a maximum of 90 days. The auditor needs to verify evidence of the effective implementation whether on-site or by document review.

A *Minor Non-conformity* is defined as a failure to comply with the requirements which based on judgement and experience is not likely to result in the failure of the management system or reduce its ability to assure controlled processes and services. Like a failure in some part of the organizations documented management system or a single observed lapse in following one item of the company`s management system. The organization must analyse the non-conformity and to plan corrective action within a maximum timeframe of 10 working days. The auditor needs to verify evidence for the effective planning by document review.

Then the auditor could define an *opportunity for improvement*. The organization is asked to review this kind of finding and decide whether to start an implementation or not. The decision must be documented.

If the auditor wants to document a topic which should be picked up in more detail in the next internal or external audit, then an *observation* will be created.

Data Protection and Privacy records the following corrective actions, which are listed in the appendix of this document, in the Corrective Action and Preventive Action overview (CAPA). The local DPMS Representatives are responsible for the collection and ongoing updates of their local CAPA list. DPP monitors the global CAPA lists.

...making excellence a habit.™

Audit Finding classification BSI

BSI categorizes the finding according the following definition:

A *Major Nonconformity* is defined when there is an absence or a total breakdown of a system or control to meet a requirement. A number of minor nonconformities against one requirement can represent a total breakdown of the system and thus be considered a major non-conformity. The organization is asked to implement a corrective-action within an agreed timeframe of a maximum of 90 days. The auditor needs to verify evidence of the effective implementation whether on-site or by document review.

A *Minor Nonconformity* is defined as a failure to comply with the requirements which based on judgement and experience is not likely to result in the failure of the management system or reduce its ability to assure controlled processes and services. Like a failure in some part of the organizations documented management system or a single observed lapse in following one item of the company`s management system. The organization has to analyse the non-conformity and to plan corrective action within a maximum timeframe of 10 working days. The auditor needs to verify evidence for the effective planning by document review.

Then the auditor could define an *opportunity for improvement*. The organization is asked to review this kind of finding and decide whether to start an implementation or not. The decision has to be documented.

If the auditor wants to document a topic which should be picked up in more detail in the next internal or external audit, then an *observation* will be created.

...making excellence a habit.™

Audit Structure 2019

In 2019, SAP conducted the two audit programs: Compliance audits and Awareness audits.

Internal Audits 2019

The internal audits are conducted between February and August 2019. All internal audits are planned, executed and evaluated by the central DPP team.

Compliance Audits

For each of the following L1 units a compliance audit has been performed by the DPP team:

- Digital Business Services
  - Global Support Delivery
  - Digital Interconnect
  - Global Customer Success
  - Global Service Delivery
  - DBS Region MEE
  - Innovative Business Solutions

- Technology & Innovation
  - SAP Cloud Platform
  - DDM & Analytics
  - Big Data

- Office of the CEO
  - Marketing and Communications

- Global Finance & Administration
  - Corporate Financial Reporting
  - Global Finance Infrastructure
  - Global Governance, Risk & Compliance
  - Global Legal
  - Global Tax
  - Legal Compliance and Integrity Office
  - Global Security

...making excellence a habit.™

- Global Customer Operations

- Human Resources
  - Global HR Service Delivery

- Intelligent Enterprise Group
  - IT Services
  - Intelligent Data & Analytics

- Product Engineering
  - Enterprise Cloud Services
  - Industries & Intelligent Enterprise

- Cloud Business Group
  - SAP Concur
  - SAP SuccessFactors
  - SAP Ariba
  - SAP Fieldglass
  - SAP Customer Experience (limited to ex hybris organization)

Awareness Audits

DPP executed in the following locations onsite awareness audits:

- Bangalore
  - Innovative Business Solutions
  - SAP SuccessFactors
  - Global Support Delivery
  - Global Service Delivery
  - Enterprise Cloud Services

- London
  - SAP Fieldglass

- New York
  - Marketing and Communications

Additionally, DPP performed awareness audits remotely:

...making excellence a habit.™

- Newtown Square
  - Innovative Business Solutions
  - Service Delivery
  - Marketing and Communications
  - IT Services
  - Global Finance Infrastructure

In 2019, the following questionnaire audits have been executed:

- Digital Business Services
  - Brno, Czech Republic
  - Vienna, Austria
  - Paris, France
  - Palo Alto, United States
  - London and Maidenhead, United Kingdom
  - Budapest, Hungary
  - Sao Leopoldo and Sao Paulo, Brazil
  - Rome, Italy
  - Lisbon, Portugal
  - Johannesburg, South Africa
  - Mexico City, Mexico
  - Buenos Aires, Argentina

- Technology & Innovation
  - Istanbul, Turkey
  - Shanghai, China
  - La Crosse, United States

- Office of the CEO
  - Mexico City, Mexico
  - Sao Paulo, Brazil
  - Beijing, China
  - Paris, France

- Global Finance & Administration
  - Buenos Aires, Argentina

...making excellence a habit.™

- Global Customer Operations
  - London, United Kingdom

- Human Resources
  - Dublin, Ireland

- Product Engineering
  - Toronto, Canada
  - Sao Leopoldo, Brazil

- Cloud Business Group
  - Chicago, United States
  - Manila, Philippines
  - Pittsburgh, Unites States
  - Prague, Czech Republic
  - Montreal, Canada
  - Gliwice, Poland

Results of the internal audits

DPP has performed 90 audits distributed to 41 Compliance audits and 49 Awareness audits. The DPP audit team has observed 82 findings in total.

The 41 compliance audits result to 32 observations, 12 minor non-conformities and 1 major non-conformity. Looking to the observations the main topics that lead to an observation are Records of processing activities (28%), sub-processor topic (15%) and Data Protection Impact Assessment (12%). The 12 minor non-conformities are distributed across all data protection requirements. For all of them a detailed action plan exists for mitigation. The one identified major non-conformity was closed within the binding due date and was evaluated in an external audit in addition.

49 Awareness audits result to 34 observations and 3 minor non-conformities. Especially for the non-conformities a detailed action plan exists for mitigation. The observation will be reviewed in the next internal audit cycle.

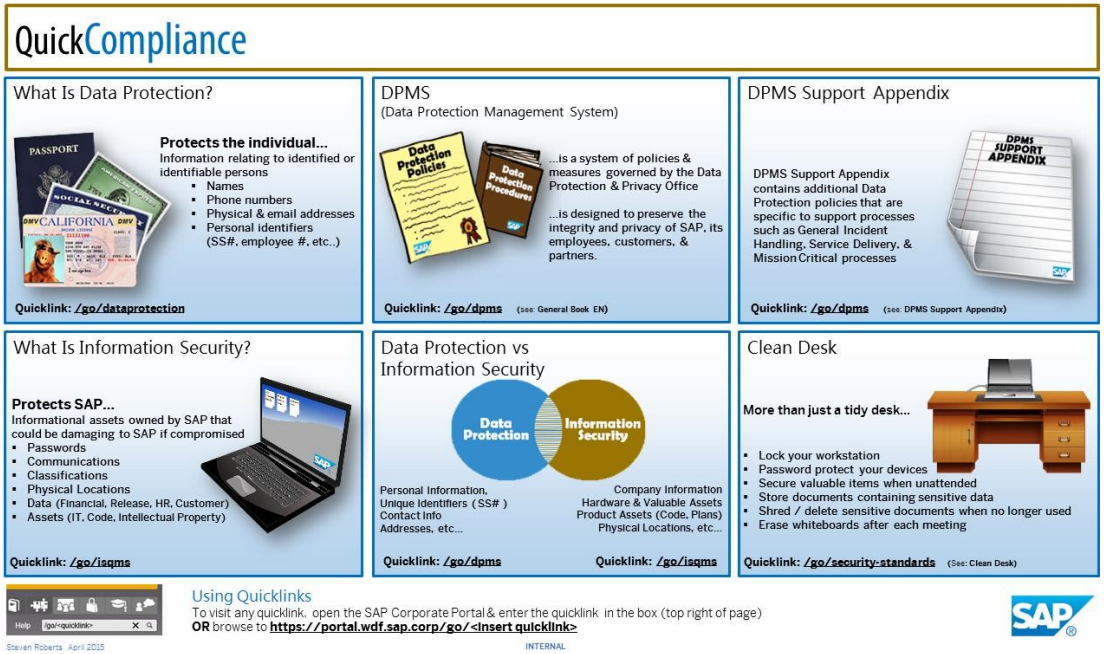
...making excellence a habit.™

Positive findings

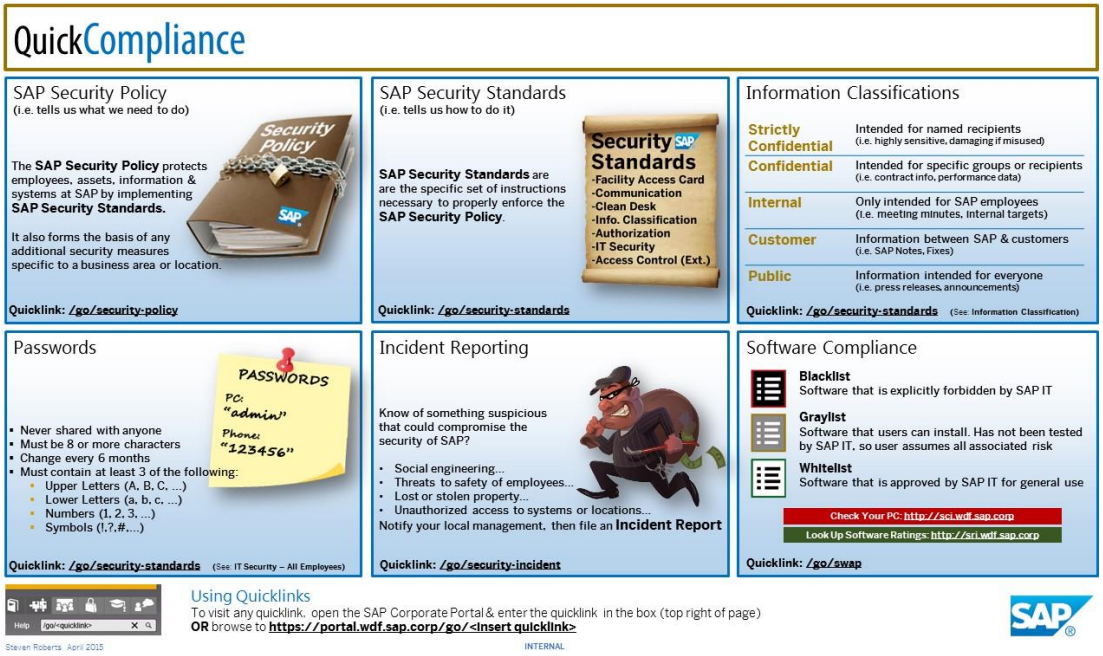
The Data Protection Management System at SAP has reached its 9th year of existence and has influenced the data protection culture at SAP significantly. It has been observed that many areas started own awareness campaigns producing a big portion of creativity, demonstrating strong commitment and unshaken tenacity for the DPMS. During the interviews the auditors have collected some of the best practices and shared them with the DPMS community.

Quick compliance guide:

Laminated version distributed to the work spaces of all employees as a quick reference.



...making excellence a habit.™



...making excellence a habit.™

External Audits 2019

The external Awareness audits and Compliance audits are conducted in a combined way in the months of September till December.

The audits of the locations listed below were conducted on site or as a video or telephone conference (in accordance with the IAF[2] requirements on advanced auditing methods). The appropriate DP Coordinator / Unit Coordinator organized the audit in advance. DPP assisted as and when required.

Business Units selected for the external audits cycle 2019:

- Digital Business Services
  - Global Support Delivery
  - Global Service Delivery
  - DBS Region MEE
  - Innovative Business Solutions
- Technology & Innovation
  - SAP Cloud Platform
- Global Finance & Administration
  - Global Governance, Risk & Compliance
  - Global Tax
- Human Resources
  - Global HR Service Delivery
- Intelligent Enterprise Group
  - IT Services
  - Enterprise Cloud Services
- Product Engineering
  - User Experience

[2] International Accreditation Forum

...making excellence a habit.™

- Cloud Business Group
  - SAP Concur
  - SAP Fieldglass
  - SAP Customer Experience (limited to ex hybris organization)

Results of the external audits

BSI has performed 33 audit days to verify that SAP runs the DPMS actively in every SAP organization in scope. The auditors reported 2 opportunities for improvements and 2 minor nonconformities.

Observations and Opportunities for improvements

For the opportunities of improvements DPP will follow up with the business units in the next internal data protection compliance audit cycle monitoring the decision of the business unit. Independent from that, BSI will request a status update when performing an external audit for the corresponding business unit.

Minor non-conformities

2 minor no-conformities were observed regarding the monitoring process of corrective and preventive actions. In both cases a detailed going forward plan was presented to the auditor team so that the minor con-conformities could be closed during the audit program 2019. Nevertheless, for both business units BSI will follow up the status in the audit cycle in 2020.

...making excellence a habit.™

Executive Summary

The 2019 data protection re-certification audit checked conformity and compliance towards company procedures, including legal and contractual requirements, and the company's supervisory organizations. This consists of training courses, awareness-raising activities, and the technical and organizational mechanisms for data protection considering the current internal and external context of the organization.

During the re-certification process a review of improvements over the past 3-year cycle of certification was an important part of audit activities.

An enhanced focus was paid to the managerial aspects of the DPMS as per Line of Business, and here especially the roles of Data Privacy Coordinators. This ensures a more relevant sampling rate to better understand how specific aspects of i.e. Marketing, HR or development are integrated with protecting personal identifiable information. This approach was supported by site samples to understand the local management support and awareness of member of staff.

As an additional factor the integration with management systems as ISO 9001 or ISO/IEC 27001 can be better evaluated per line of business.

The organization adopted a state-of-the-art approach to a global operating management system and presented evidence of its continuous improvement.

A global risk assessment process is established to identify the need for specific maturity levels of the Data Protection Management System.

- Tier 1 – full BS 10012:2017 certification in activities relevant for contracted data processing.
- Tier 2 – roll-out and implementation of SAP`s data protection measures in the entire organization.

...making excellence a habit.™

Considering GDPR[3], SAP presented its ability to effectively manage changes in data protection regulation on a global scale and to ensure its on-going conformity with requirements. Architectural changes in relevant supporting information systems ensure the capability to minimize data collection, ensure appropriate retention schedule management, enable Data Subject Right requests to be followed up on and supports SAP's Binding Corporate Rules (BCRs) under GDPR.

SAP's customers can be confident that for the processes audited, SAP fulfills the legal requirements for handling confidential and personal data as evidenced based on the samples taken. Beyond that a full-covering risk assessment with respect to data protection is enabled.

The certification assures SAP's customers that SAP meets the standards for collecting, processing, and using personal data for them, under GDPR requirements and requirements of non-EU jurisdictions. The effort and expense customers would incur if they conducted their own audits and supplier-assessments, and had to make contractual arrangements, are reduced considerably or avoided altogether.

The following focus areas were identified in the 2019 audit:

- Network of Data Privacy Coordinators and strong liaison with Data Privacy and Protection organization of SAP
- Overall improvement and maintenance of the Data Protection Management System over the 3-year cycle

[3] GDPR – General Data Protection Regulation

...making excellence a habit.™

Contact:
Milo Tauber
BSI Group Deutschland GmbH
Tel: +49 (0) 69 22 22 89 - 299
Email: milo.tauber@bsigroup.com

Contact:
Gordon Stier
SAP SE
Tel: +49 (0) 6227 7 - 63588
Email: gordon.stier@sap.com

Marketing:
Claudia Rheingans
BSI Group Deutschland GmbH
Tel: +49 (0) 69 22 22 89 - 217
Email: claudia.rheingans@bsigroup.com

...making excellence a habit.™