



Infopulse
Standards
Compliance
Manager

Infopulse SCM Compliance Digest: Summer Edition, 2020

Content

Digital Transformation of Compliance: Trends for 2021	3
GRC Solutions: Managing Multiple Standards Simultaneously	5
IT Security Assessments Going Online: A Guide to Performing a Virtual Audit	9
Building an Efficient Security Compliance Strategy. Part 1: Challenges and Errors	12
Building an Efficient Security Compliance Strategy. Part 2: Practical Steps	15





Digital Transformation of Compliance: Trends for 2021

Compliance teams face challenging times ahead with increasing regulation, the new normal and an expectation that they will prevent crime without inhibiting the customer experience. The pace of change continues unabated, and 2021 looks like being no exception. For most organizations, throwing more people at the compliance challenges is not an option, so we should expect to continue to see significant increase in digital transformation in terms of AI, automation and simplification of compliance-related processes.

Every year, new directives and regulations are adding complexity to compliance operations across all industries. Navigating the rapidly evolving regulatory landscape is rather challenging for contemporary business owners, which is why advanced alternative approaches to compliance management are becoming essential to retain a competitive advantage.

Modern organizations have to deal with a broad spectrum of issues that hamper the effectiveness of compliance practices. Some of the most pressing issues are – manual and time-consuming

processes, inability to keep pace with regulatory changes, lack of valuable security insights, and siloed approaches to governance and risk management. Companies need to have a profound understanding of why it's important to stay up to date on emerging compliance trends. Leveraging digital transformation initiatives into compliance management can resolve all of the issues mentioned above and help organizations manage and comply with continually shifting regulations proactively. Let's review the most anticipated compliance trends for 2021.

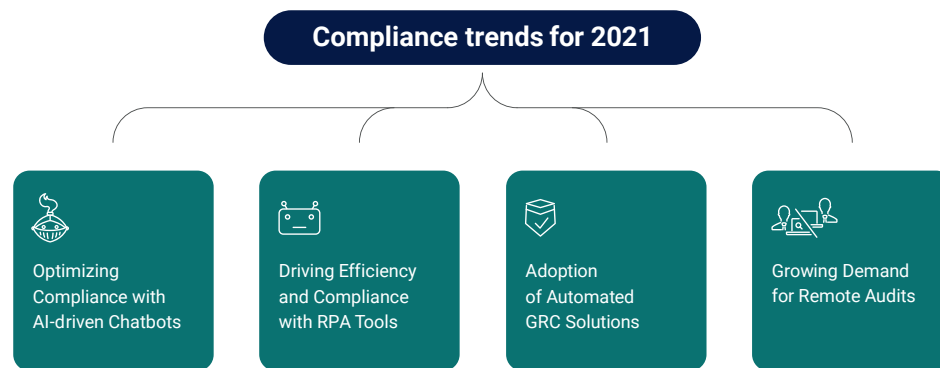
Optimizing Compliance with AI-driven Chatbots

Automated interactions with customers and employees are among the significant digital transformation trends that continue to grow exponentially every year. AI and ML-based chatbots and personal assistants are steadily adopted into workplaces to augment human performance and eliminate time-consuming manual processes. [Gartner](#) predicts that 70% of organizations will integrate AI to assist employees' productivity by 2021.

The adoption of advanced AI-driven solutions is an ascending trend within the digital transformation of compliance. [Chatbots](#) offer compliance assistance that can enhance compliance managers' productivity by providing realtime insights, generating reports, and automating a broad spectrum of other compliance-related activities.

Driving Efficiency & Compliance with RPA Tools

Automated interactions with customers and employees are among the significant digital transformation trends that continue to grow exponentially every year. AI and ML-based chatbots and personal assistants are steadily adopted into workplaces to augment human performance and eliminate time-consuming manual processes. Gartner predicts that 70% of organizations will integrate AI to assist employees' productivity by 2021.



Adoption of Holistic GRC Solutions

As cyber threats evolve and become more sophisticated, effective risk management processes become business-critical. To address this challenge,

organizations are actively adopting innovative governance, risk, and compliance (GRC) tools. Such tools enhance operational efficiency, break down the silos in terms of risk management, and facilitate decision-making. Moreover, holistic GRC solutions enable fast and accurate risk assessment, gap analysis, and incident response. [GRC solutions](#) are becoming indispensable for security compliance, and their adoption will remain a strong trend in the upcoming years.

Growing Demand for Remote Audits

Internal and external audits are essential to ensure full compliance with the changing regulatory landscape. However, usual audit execution with auditors' on-site presence is currently impossible due to the safety constraints and travel restrictions proceeding from the COVID19 pandemic. However, advanced information and communication technologies (ICT) have made [remote audits](#) feasible and practical. In a post-pandemic environment, remote auditing will consolidate its position as a strong trend, as it is flexible, effective, and reduces the time and costs.

Conclusion

By leveraging digital transformation initiatives into compliance, business owners can keep pace and proactively manage and navigate the ever-changing regulatory landscape. The adoption of AI-based solutions, the best RPA tools, and advanced GRC software will remain ascending trends within compliance practices for 2021. This is due to the tangible business benefits they provide, including compliance automation, enhanced efficiency, and integrated approach to compliance management.

[Infopulse](#) has developed an innovative, all-encompassing GRC tool – [Standard Compliance Manager](#) (SCM) that features advanced automation capabilities. Besides effective risk management processes and a broad spectrum of other advanced features, SCM offers substantial personal assistance to businesses in transforming their compliance management.



GRC Solutions: Managing Multiple Standards Simultaneously

Most organizations benefit from implementing multiple standards to ensure their processes are in line with the business goals and to maintain business models through ever-changing environments. The question is: How to manage multiple standards efficiently without significant time consumption and paperwork?

Over the past several years, the importance of establishing company-wide, adequate quality, security, and business continuity systems has dramatically increased. A continually growing number of companies are striving to enhance their performance by following existing and emerging standards and regulations. Organizations have to comply with them to maintain, e.g., security, privacy, and continuity of their business.

What Are the Key Challenges of Building Multi-Standard Compliance Strategy

When aligning with many standards, the process of gaining compliance often involves too many programs, processes, individual efforts, and may become a mess. Let's point out the significant challenges that compliance officers face when managing several standards for one organization.

Handling Repeated Information

With each new or updated standard or regulation, the responsible manager has to implement it in the system. He needs to upload all company assets, apply requirements to these assets, apply controls to them according to the new or updated version of the regulation or standard. Whether copy-pasting or doing it from scratch, it takes time and effort, not to forget the human error that comes with C&P and repetitive work. The compliance officer has to deal with the continuously growing number of regulations, rules, or updates, filling in information repeatedly. Here is why one system compliance approach is the solution.

An [integrated GRC solution](#) can help you be more productive, as it allows you to overlap specific requirements, put multiple standards into one concept, and leverage it to identify gaps. Thus, you can quickly compare the same requirement/safeguard for a new or updated regulation, so that you can re-use it for another applicable standard.



The Compliance Silo: How to Manage Multiple Standards

Compliance silos are often a significant challenge when dealing with several standards. Handling assets, requirements, and controls for multiple standards often becomes complicated. Some information remains static, while other data is dynamic and changes continuously. Usually, the compliance officer has one standard per concept, but what if details for multiple standards are similar? Every time, you have to switch from one standard to another to check assets, requirements, etc., you spend excessive effort and time.

To successfully apply similar requirements and corresponding controls to assets, it is necessary to use practical tools to meet all your compliance needs. [SCM](#) will ensure seamless operation without needing to process the item from scratch every time there are updates in the regulation or overlap with another standard in use.

Tools That Can Cover All Your Compliance Needs

Using tools that aren't capable of simultaneous management of standards is what often creates silos.

Companies that are starting their compliance journey can choose Excel as a management tool because it is familiar. Yet, it may end up with piles of spreadsheets and lots of extra routines that are more likely to hold up the compliance workflow.

Please [read more](#) to understand why Excel is not the best choice for compliance management. Today, as this topic is peaking, the modern GRC solution for compliance operations can cover inventory analysis, risk management, and compliance checks in a standardized process.

Use Case: Switching Between Standards In One Environment [ISO 27001 and IT-Grundschutz]






Assuming a company has re-considered the business goals and decided to switch from [ISO 27001](#) to [IT-Grundschutz](#).


[IT-Grundschutz](#) is based on ISO 27001, but it is more specific and technically oriented.


The ISO standard is aligned more with business processes, while IT-Grundschutz refers to the equally technical, infrastructural, organizational, and personnel aspects. According to ISO 27001, the risk analysis and the evaluation of the risk objects play a decisive role. Meanwhile, IT-Grundschutz states that risk analysis is only required in individual cases (it is required for Standard and Core but is not obligatory in the Basic level of protection). In ISO 27001, it is necessary to identify the risks for the assets independently; the BSI IT-Grundschutz specifies the typical threats for defined modules and provides in-detail controls to each requirement.

Some requirements in these standards intersect. Why would you need to make the double effort in searching or uploading the new data sets into the compliance tool? If a company has already specified controls for ISO27001, it can re-use these controls for another requirement in IT-Grundschutz.

[Infopulse SCM](#) allows you to effectively manage overlapping environments all in one place and quickly adjust workflows and processes to the compliancy & risk needs.

Compliance Check Standards Compliance Manager admin     

Demo > Version 2 (Working) TABLE VIEW 

UPDATE UPDATED 10:34 AM Controls 

X CLEAR FILTER X CLEAR SORTING X CLEAR GROUPING 16 1 EXPORT

Standard	Requirement	Status of Req.	Control	Status of Con.	Asset No.	Status of Asset
Standard: IT-Grundschutz						
IT-Grundschutz	BMS.1.K1 Assumption of overall responsibility for information security by the ...	Yes	BMS.1.C1 Assumption of overall responsibility for information sec...	Yes	Reglist	Untreated
IT-Grundschutz	BMS.1.K2 Determination of security objectives and strategy [Institutional mana...	Dispensable	BMS.1.C3 Determination of security objectives and strategy [Instit...	Untreated	Reglist	Untreated
IT-Grundschutz	BMS.1.K3 Creation of a guideline for information security [Institutional manage...	Untreated	BMS.1.C3 Creation of a guideline for information security [Institut...	Untreated	Reglist	Untreated
IT-Grundschutz	COB.2.H1 Implementation standard privacy model	Partial	COB.1.C1 Survey of the influencing factors of data backup (special...	Partial	Reglist	Untreated
Standard: ISO 27001						
ISO 27001	A.17.1.B1 Planning information security continuity	Untreated	A.17.1.C1 Requirement realization	Untreated	Reglist	Untreated
ISO 27001	A.17.1.B2 Implementing information security continuity	Untreated	A.17.1.C2 Requirement realization	Untreated	Reglist	Untreated
ISO 27001	A.17.1.B3 Verify, review and evaluate information security continuity	Untreated	A.17.1.C2 Requirement realization	Untreated	Reglist	Untreated
Standard: ISO 22301						
ISO 22301	CN.7.3.B1 Awareness	No	CN.7.3.C1 Requirement realization	No	Reglist	No
ISO 22301	CN.4.2.B2 Legal and regulatory requirements	Partial	CN.4.2.C2 Requirement realization	Partial	Reglist	No
ISO 22301	CN.10.K2 Continual improvement	Yes	CN.10.C2 Requirement realization	Dispensable	Reglist	No
Standard: GDPR						
GDPR	CHAPTER 1.3.P1 Subject-matter and objectives	No	INFOPU.SE.3.C5 Lawful grounds to process should be ensured	No	Reglist	Untreated
GDPR	CHAPTER 1.3.B3 Territorial scope	Yes	INFOPU.SE.3.C2 Define territorial applicability	Dispensable	Reglist	Untreated
GDPR	CHAPTER 1.3.K4 Definitions	Yes	INFOPU.SE.3.C3 Define personal data and their type	Yes	Reglist	Untreated
GDPR	CHAPTER 1.3.R2 Principles relating to processing of personal data	Partial	INFOPU.SE.3.C4 Ensure processing of personal data is compliant w...	Partial	Reglist	Untreated
GDPR	CHAPTER 1.3.R0 Lawfulness of processing	No	INFOPU.SE.3.C5 Lawful grounds to process should be ensured	No	Reglist	Untreated
GDPR	CHAPTER 1.3.R6 Processing of special categories of personal data	Untreated	INFOPU.SE.3.C6 Ensure lawful processing of special categories of p...	Untreated	Reglist	Untreated

Compliance check in Infopulse SCM



Benefits of Using GRC Solutions that Support Multiple Standards



Harmonizing management of all standards in one place – you get a consolidated view of all applicable standards in one concept.



Implementing custom standards into SCM.



All existing relevant data can be re-used with every new or updated regulation.



Linking new requirements to the existing assets.



Cross-implementing the existing controls for more than one standard.



Simplicity in the management of multiple threats from common threat catalogs if they intersect for multiple standards.



Well-structured compliance management framework consisting of regulations, clear user roles, processes, operations, assessments, and procedures.



Effective gap analysis allowing you to find overlaps and gaps between regulations and eliminate redundant controls.

The benefits of aligning multiple standards in one GRC solution are clear. However, developing an efficient compliance framework with many standards might require significant time and effort. Enforce your digital advantage with up-to-date GRC solutions for building effective compliance strategies.



IT Security Assessments Going Online: A Guide to Performing a Virtual Audit

Cyber security audits provide the basic cyber security foundation for building and improving your ISMS. In the new reality, virtual audits are becoming in-demand. What is the difference between a regular audit and a virtual assessment? What happens during the virtual IT audit and how to perform it?

When the whole world has been put to a lockdown, things started to change: companies shifted to the [work-from-home mode](#) and significant scope of work has gone remote. The new normal has challenged companies in many ways, namely the inability to adapt and maintain business continuity in uncertain times. Things have changed and this has also affected the compliance world. Companies started to pay more attention to security and data privacy, while the compliance obligations didn't go anywhere – you still need to align with the requirements and conduct regular audits to keep your sensitive data safe.

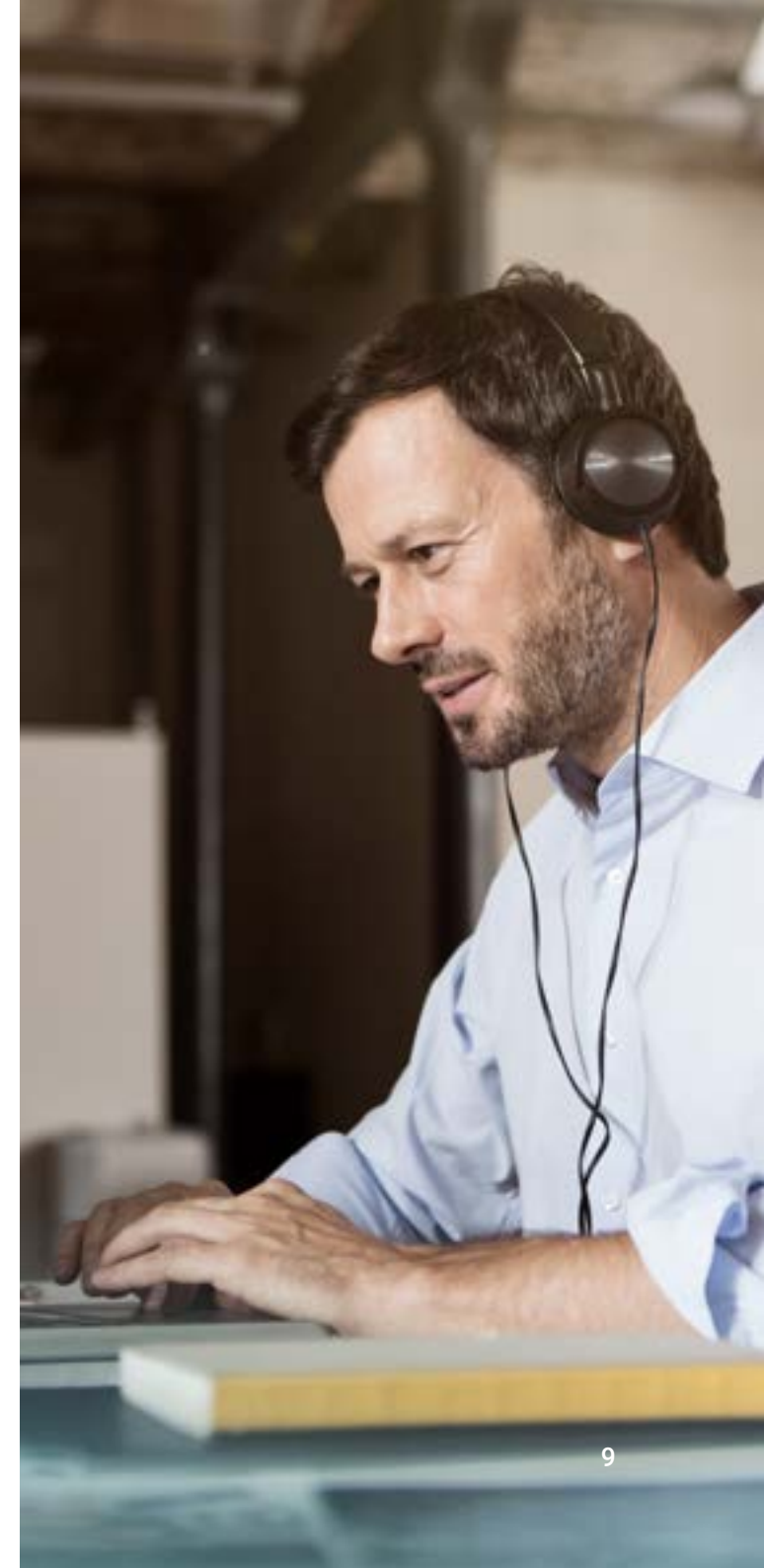
Why Are Cybersecurity Assessments Critical Today?

Cybersecurity audit is a technical assessment of an organization's IT infrastructure, i.e., their operating

systems, applications, and more. They provide invaluable information about the organization's security controls and are particularly beneficial to companies for documenting and addressing their risks, vulnerabilities, and threat exposure. Internal and external security evaluations allow security managers to evaluate the potential disruptions, discover gaps and leaks, and get ready for future certifications. In the post-pandemic world, remote audits are an option that more and more organizations start to consider and implement in their compliance processes. Regular assessments help to discover new vulnerabilities, besides, they are required by regulations and standards. For example, an internal audit is mandatory for [ISO27001](#), as well as for [IT-Grundschutz](#) on the check phase.

What Is a Remote Audit?

A virtual IT audit is conducted partially or completely off-site. It covers all the points and steps as an onsite audit, but the auditor uses communication technology when a site visit is not possible.





How Is a Virtual Audit Conducted?

The remote audit will typically last as long as the regular onsite audit. The assessor will dial you into the conference call via the previously agreed platform. You will need to be available all the time and share your screen. The assessor may ask you to send documents for review via any of the secure communication channels available.

Security Audit Workflow

A security audit should follow such basic format:

Definition of the Assessment Criteria

At first, it is necessary to determine the general goals of the company, what exactly you need to address in the assessment, and then define the priorities of these objectives. Whether you need to check your security system for further improvements or you're heading for certification – it should be clearly stated. According to Gartner, a company should agree on how the performance and tracking of the audit will be carried out, as well as on gathering and addressing the assessment results.

Preparation for the Remote Security Audit

Since remote auditing relies on technology, you may follow these points to arrange your virtual audit:

- Define which tools you will use for your virtual audit. Check the benefits the right software can provide you with.
- Decide which online conferencing system you would use for interaction with the assessor, such as Microsoft Teams, Skype, Zoom, GoToMeeting, Google Hangouts, etc.
- Ensure online connection. If it's not possible, the auditor may ask you to email the necessary information and follow up with a telephone call.

Three Essential Aspects of the Virtual Audit

You will also need to make sure the following aspects to be available for a virtual IT audit:



1. Personnel

People that have to be present during the audit:

- CISO or IT security manager;
- Key personnel involved;
- Representative(s) of the management board if planned for the opening and final meetings, or the leadership part if planned.



2. Documentation

The assessor will review your ISMS remotely via screen share or by sending the files via a secured communication channel. Documents that are usually to be submitted for the auditor are as following:

- Internal audit records
- Internal audit plan
- Management review minutes and actions
- Complaints log
- Corrective actions
- Improvement documentation
- Risk register
- Documentation supporting core business processes (if possible) and final meetings, or the leadership part if planned.



3. Site tours

A remote audit may require a site tour, so you should show the auditor around via a webcam or a video call. If the location is closed, or a virtual site tour is not possible due to technology, safety, or health issues, then this procedure will be carried out on-site during the next audit. The assessor will determine it based on your circumstances.

Timeframes for remote audit preparation	
Min. 2 weeks before the audit	Make a prior call with an Auditor Agree on the logistics of your assessment, audit plan, timeframes, records, necessary documents, and personnel.
Before the audit	Prepare documents, inform the personnel, and submit any information requested by the Auditor if agreed.
Audit day one	Start the conference call at the time and via the channels agreed.

Remote Audit Results

You should monitor the progress of the audit and prioritize certain points that may require further examination. After the audit is completed, discuss the results with all of the stakeholders. Create a list of action points based on the audit and decide which steps to take first to fix the security issues discovered.

How a GRC Solution Can Make Your Virtual Audit a Blast

During the remote assessment, the auditor will require you to send documents via email. With Infopulse SCM you can [generate reports](#) with just a few clicks, make all the necessary snapshots upon the auditor's request, and provide clear and consolidated information regarding your compliance operations when necessary. [Infopulse SCM](#) enables you to maintain a holistic view of your ISMS and manage multiple standards in one system.





Building an Efficient Security Compliance Strategy. Part 1: Challenges and Errors

As the world is going digital, businesses face more stress while protecting their assets from cyber threats. Not only building a reliable and robust IT security compliance strategy is a challenge - companies need to align with the constantly evolving regulations and standards as well.

Today organizations face an evolving array of security threats and continually changing compliance requirements. As the business grows, privacy and security concerns only multiply and add to a dynamic set of priorities.

In IT security, organizations seek compliance not only because of the need to have security certifications formally but also to reduce security liabilities and protect digital assets from a continuously growing number of cyber threats. Let's take a look at common challenges and mistakes companies may face when enforcing and maintaining their security compliance strategies.

The TOP-5 Challenges of Creating a Cybersecurity Strategy

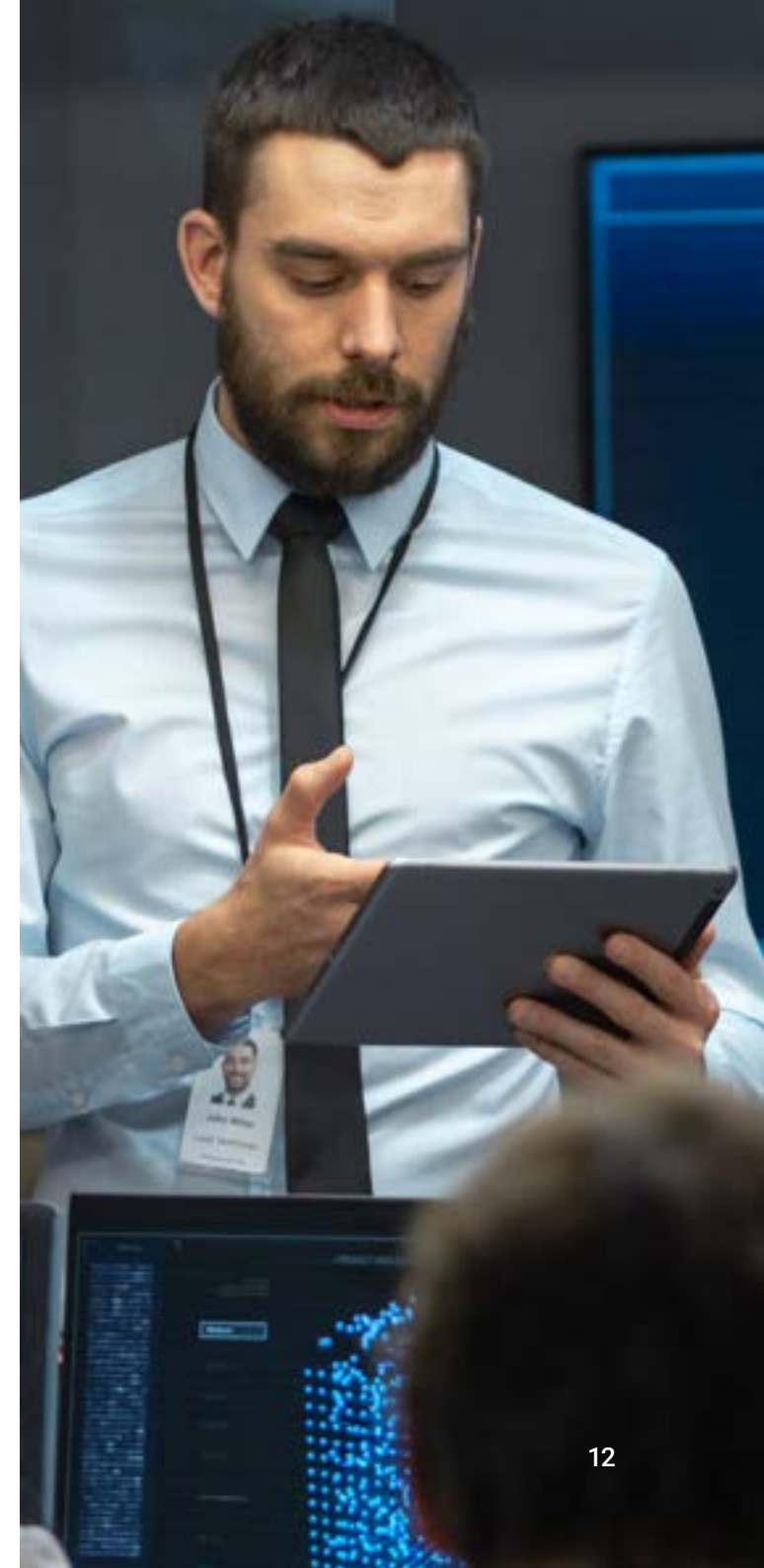
1. Geopolitical & local regulations

The focus has shifted from globalization back to

nationalism and affected the policy and regulations aspects, too. Today companies should align with regulations taking into account industries and locations where they are doing business. Some certifications are a must if you're doing business in certain countries (e.g., [IT-Grundschutz](#) for Germany), while others may require you to align with entirely different standards. For example, in terms of data protection and privacy, [GDPR](#) is a must for organizations located in Europe and those working with the European companies. If you target the U.S. market, you need to get CCPA certified.

2. Crisis and force-majeure

As the current crisis has demonstrated, not all businesses were ready to face the pandemics and take proper actions to mitigate its influence in terms of security, data privacy, and business continuity. Shifting to the work-from-home mode has posed severe obstacles for many organizations to ensure secure connections and networking for their employees, avoiding data breaches.





3. Governance and involvement

Compliance requires full company engagement into the process, so that everybody, from top management to trainees, put efforts together to maintain and follow reliable and robust security policies. While company decision-makers should support and enforce regulations, they need to be involved in security decisions, understand risks, and allocate the proper budget for adequate resources and tools in support of safeguard implementation efforts.

4. Quick adaptation to changing patterns

Regulators expect businesses to have a highly broad view of operational resilience by both controlling the operational risks and managing the disruptions. Therefore, they need to have a comprehensive approach, including inventory, risk analysis, and continuity planning.

5. Growing frequency of cybercrimes

As the beneficial side of technology is undeniable for the companies to deliver better service and value to their customers, it is also giving way to cybercrimes and fraud.

In 2020, personal data was twice as much involved in security breaches (58% of total), while 86% of breaches were financially motivated ([Verizon 2020 Data Breach Investigation Report](#)). Three leading causes of data breaches are credential theft, social attacks (i.e., phishing and business email compromise), and software defects. So, for most organizations, these three areas should be the focus of the bulk of security efforts.

Three Common Mistakes in Building a Security Compliance Strategy

Here are the most common mistakes when striving to align with regulations and international standards.

Mistake: Failing to scale a global compliance strategy

While every global company has a compliance strategy, very few think about integrating these strategies to support operational efficiency and profitability.

Solution: Take a proactive and holistic approach to build an Information Security Management System (ISMS) in the organization by including not only technological aspects of security but also accounting for the people and the working environment. This approach will enforce companies to make their security system more comprehensive.

Mistake: Poor Due Diligence on Vendors

Proper diligence of your business partners, third-party vendors, and service providers is another critical part of maintaining your security compliance strategy.

Solution: Ensure proper third-party risk management with your vendors and outsourcers by creating an adequate TPRM (third-party risk management framework).

Mistake: Siloed Data, Siloed Teams and Old Technologies

One of the most common mistakes is keeping compliance efforts siloed across different workgroups and using outdated software.

Solution: Consider compliance platforms and cloud-based solutions for quick data access and analysis. Proper software can help minimize costs, reduce redundancies, and streamline data. An integrated platform is the best option for you to avoid siloed teamwork and quickly retrieve the data relating to a company's compliance program.



Critical Components of the IT Security Compliance Strategy

Cybersecurity standards are a robust basis for companies to build, maintain, and continuously improve their ISMS. Considering all possible challenges and an array of common errors, it becomes clear that creating an effective ISMS is not a one-day-operation for any company, no matter its size or operational field.

Regulatory compliance strategies should include answers to the following questions:

- how your organization will address relevant security standards from an operational perspective;
- how you will establish security-related processes and modify them if needed;
- how you will measure effective risk mitigation and compliance success;
- which tools and proven techniques you will use for this.

Taking a comprehensive, holistic approach to creating your ISMS is crucial for being efficient and smartly scaled in terms of effort-, time- and cost-effectiveness. [Infopulse SCM](#) is one of the progressive GRC solutions allowing you to enforce your ISMS according to your business needs.

Check for the step-by-step guide and checklist for creating an ISMS in the next article of the series.





Building an Efficient Security Compliance Strategy. Part 2: Practical Steps

Today companies are paying more attention to the processes of planning, implementing, maintaining, and monitoring their ISMSs. IT-Grundschutz is one of the most comprehensive and holistic methodologies to be considered when establishing your ISMS.

Proper maintenance of an organization's information security management system (ISMS) is the key to the protection of your sensitive information and valuable assets.

As we have described in [Building an Efficient Security Compliance Strategy. Part 1](#), companies face many challenges when establishing and maintaining security compliance strategies.

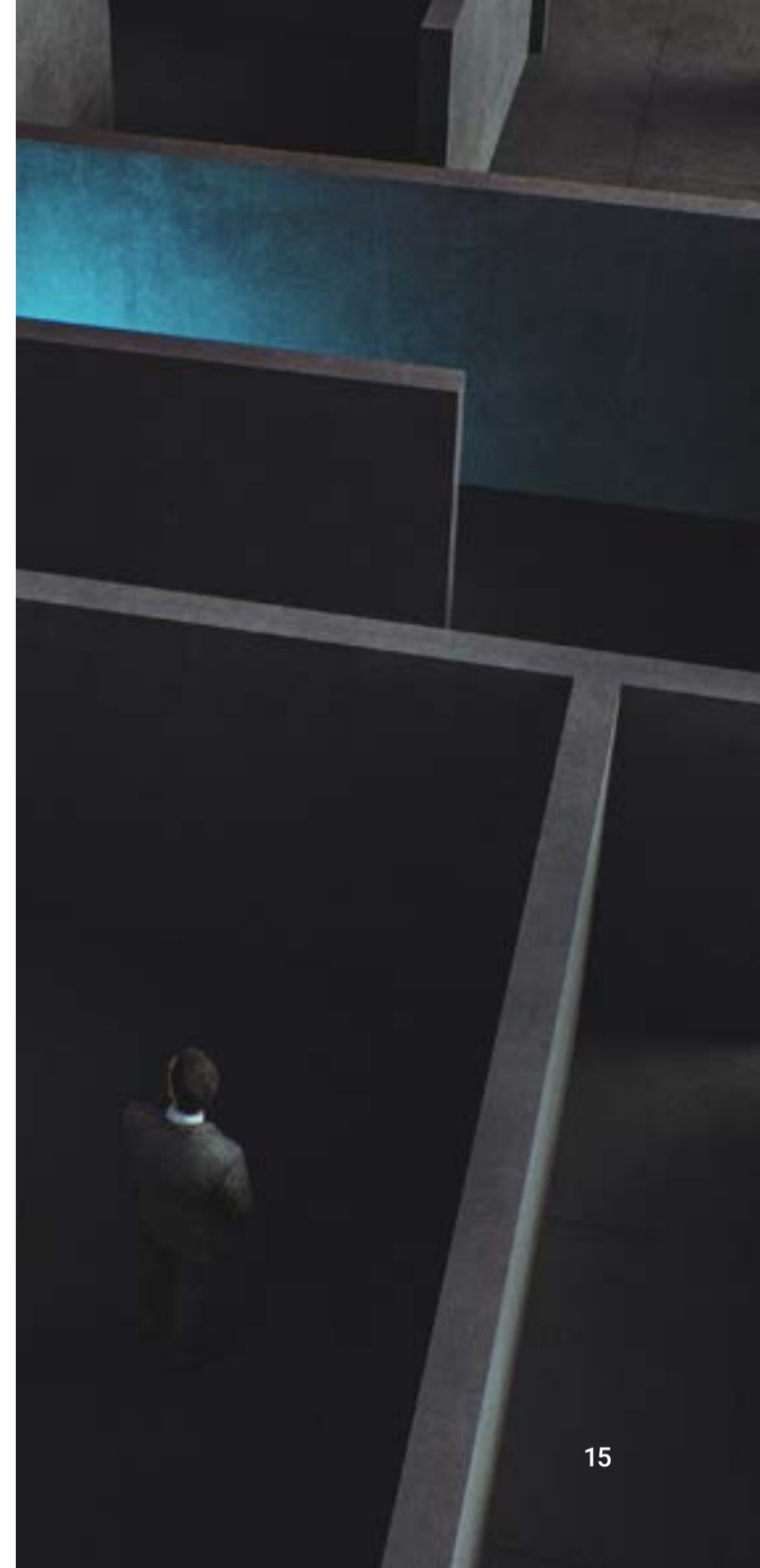
We continue our information security journey and will guide you through a step-by-step ISMS implementation on the basis of [IT-Grundschutz](#).

ISMS via IT-Grundschutz

Following IT-Grundschutz, you will be able to appropriately build an ISMS and protect your organization. This regulation provides users with standardized security recommendations and clearly outlined implementation steps collected in the [Compendium](#).

IT-Grundschutz Compendium in combination with modern governance, risk, and compliance solution make it easier for security and data protection officers to maintain information security (IS) in their day-to-day work.

It is essential not only to focus on the security of IT systems, but also pay attention to the technical, organizational, infrastructural, and personnel aspects. The security of the operating environment, the reliability of services, proper handling of the information, and many other important things should also be taken into account.





Three Steps of Establishing an effective ISMS based on IT Grundschutz

1. Initiating the security process

- Functions and responsibilities
- Scope of application: Information system
- Security objectives and guideline

2. Organization of the security process

- Development of an organization for Information Security
- Integration in procedures and processes
- Design and planning

3. Implementing the security process

- Modeling according to IT-Grundschutz
- IT-Grundschutz check
- Implementing the security concept

1. Starting the Security Process

- **Governance.** Ensure that the company's management board understands the necessity and importance of the ISMS and offers assistance at all levels.
- **Responsible Person.** Company management should consider an appointment of a chief information officer (CISO) who will be responsible for guiding and working with the ISMS. Data Protection Officer (DPO) can be assigned to accompany all aspects of data protection within an organization and introduce appropriate control mechanisms. Without someone capable of performing the IT security compliance program, the whole plan will be hard to implement.
- **Integration of All Employees into the Security Process.** Conducting practical training and education of the CISO, DPO, IT security managers, and all people involved in the security compliance process is a must. It will ensure better workflow and cooperation between all the parties involved.





- **Planning the Security Process: Define the Scope.** Establishing a continuous information security process and defining an appropriate strategy. The company management should set basic security objectives and the level of IS to align with the business goals. During this phase, analyze stakeholders (i.e., the relevant internal and external parties), business objectives, tasks, and security requirements.

It is vital to determine the IS goals at the very beginning of each security process so that the security strategies and concepts match the actual requirements of the company.

2. Organization of the Security Process

- **Establish the Organization for Information Security.** The structure of the company should promote and implement the information security process. The organization of IS depends on the size, nature, and structure of the particular business.
- **Integrate Information Security in All Organization Processes.** Information security must be integrated into the processes within the overall organization, and contact persons must be specified. Take into account all the necessary security aspects in all strategic decisions at an early stage.
- **Design the Security Process.** Identify all the conditions for your IS to be implemented and the level of information security required for your company. IT-Grundschatz offers three approaches to IT protection to follow: basic, standard, and core.

3. Implementation of the Security Process

- **Create a Concept.** Draw up a concept according to any type of protection approaches based on IT Grundschatz. Define the security concept, decide which data must be protected and prioritize.





- **Inventory Analysis.** Define all your existing assets that must be protected. IT-Grundschatz provides you with detailed requirements and controls for your valuable objects.
- **Compliance Check.** After you have all your assets defined, you will check your project's current compliance status. Go through each requirement for every asset and access the implementation details and threats provided by IT-Grundschatz Compendium.
- **Risk Analysis.** During this phase, you will use the modeling in line with IT-Grundschatz to assess risks in a structured manner and take corresponding security measures. According to IT-Grundschatz, there are three ways you can respond to the risk: 1) Treat the risk by applying controls; 2) Terminate the risk by avoiding it; 3) Transfer the risk to third parties.
- **Documentation of Results: Reporting.** Document the results of the risk analysis, as you will be able to use them as the basis to address the requirements and measures where the gaps still exist.
- **Audit.** The audit is an integral part of any security implementation process. You can conduct internal and external audits within the company to see all the potential ISMS gaps. It is the final stage of preparation for certification.
- **Certification.** The last step is, obviously, to have your ISMS examined and certified by the Federal Office for Information Security. You can be certified according to ISO 27001 on the basis of IT-Grundschatz.

Continual Improvement

For your ISMS to be effective, it is not enough just to implement appropriate security safeguards and update documents. You should take an approach to the continuous improvement of the information security process. The information security audit is an essential part of your ISMS and is integrated into the "Check" phase of the PDCA model. It is essential to trace success, make appropriate evaluations, and hold meetings after serious security incidents happen or if there are serious changes to the framework conditions. Document all results and decisions.

We at Infopulse follow the Plan-Do-Check-Act cycle predefined by [ISO 27001](#) to achieve the continual improvement model that starts right after the audit. First, you plan your ISMS and then implement it. Next, you check the performance of your new arrangements and decide if they are achieving what you had intended or can be further enhanced. Finally, you act upon those decisions, beginning another PDCA cycle as you implement the improvements.

Managing Your Security Management System with the GRC Solution

To make your information security procedures more holistic, you may use a relevant GRC solution that will enforce automation and make your compliance routine easier, more reliable, and faster.

Key Beneficial Features of SCM for IS

Implementing BSI IT-Grundschatz you will be able to:

- Create concepts, perform inventory and compliance checks as well as risk analysis, consider all the gaps, risks, and safeguards available.
- Use the IT-Grundschatz and Compendium integrated into the system and access all the relevant updates with the newly issued version.
- Migrate from the old version of IT-Grundschatz to the new one with one click.
- Easily manipulate, arrange, bulk-edit, sort, and filter the data during inventory and compliance checks, risk management analysis;
- Generate standard GS reports;
- Fully automate the report generation process thanks to the SCM Bot and then send them at a specific time via email to the defined persons involved.

With [Infopulse SCM](#), you will be able to achieve the most efficient implementation of the intended security measures.

Bring your compliance to the next level with Infopulse SCM!



Infopulse
Standards
Compliance
Manager

Contact us for a demo:

 infopulse-scm.com

 scm@infopulse.com

 +49 7971 919 01 70

 **Cyber-Security Council**
Germany

 Licensed
IT-Grundschutz Content
Federal Office for Information Security

Alliance for
Cybersecurity
Member 

Ready for 
KRITIS