

SEEBURGER

>< Connect >> Automate >>> Innovate

 Webcast Series | Meet the Expert

The EU NIS 2 Cyber Security Regulation is just around the corner!

How can you as a customer easily check SEEBURGER as your service provider?





Disclaimer

This publication contains general information only.

SEEBURGER does not provide any professional service with this publication, in particular no legal or tax consulting service. This publication is not suitable for making business decisions or taking actions. For these purposes, you should seek advice from a qualified advisor (e.g. lawyer and/or tax consultant) with regard to your individual situation.

No statements, warranties or representations (express or implied) are made as to the accuracy or completeness of the information in this publication.

SEEBURGER shall not be liable or responsible for any loss or damage of any kind incurred directly or indirectly in connection with any information contained in the presentation.

Agenda

01 | EU-NIS 2 & EU-RCE at the Gates

02 | Laws in EU Member States (Example NIS2UmsuCG)

03 | Information Security at SEEBURGER

04 | Check your Supply Chain

05 | Next Steps checking SEEBURGER



01

EU-NIS 2 & EU-RCE
at the Gates



Comparison of EU-NIS2, EU-RCE, and EU-DORA

	NIS2	RCE	DORA
Focus	Cyber security	Resilience critical systems	Cyber security and resilience
Scope	Sector definition affects up to 50% of companies	Critical systems (Replacement for KritisV or BSIG §8.1a)	Financial industry (replaces BAIT, VAIT and ZAIT)
Requirements	Governance (§20), cyber hygiene, incident response, business continuity management, supply chain security (§21), reporting chain to BSI (§23)	Physical security, business continuity management & disaster recovery in detail	Operational Resilience, IT Resilience, Incident Management, Business Continuity Management & Disaster Recovery in detail
Relevance for SEEBURGER	Directly as a cloud and managed services provider (CSP & MSP)	No, as we do not (or will not) operate any critical systems	Indirectly as a normal ICT service provider §30.2 but not under §30.3 (important or critical)
Start	18.10.2024	18.10.2024	17.01.2025

New Compliance Requirements 2024 – EU-NIS 2

- NIS 2 = Directive about Security of network and information systems →
“Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)”
- EU-NIS 2 is not a regulation like EU-GDPR, but a EU-Directive. Needs to become law in each respective EU member state by October 2024 or becomes active indirectly
- Difference between „critical” (so far KRITIS §8a / Germany), „very important” and „important”
- *EU IT Implementation Act for NIS 2 (ETA 24.10.2024)* regulates the details



Governance
Article 20



Risk Management & Measures
Article 21



Reporting
Article 23



European Cyber Certifications
Article 24

New Compliance Requirements 2024 – Companies in Scope

Sector 1

- Energy
- Transport
- Banks
- Financial markets
- Healthcare providers
- Drinking water
- Waste water
- Digital infrastructure
- **ICT service management**
 - **Cloud Services providers** **SEEBURGER**
 - **Managed Service providers**
- Managed security service providers
- (Public administration)
- Space

Sector 2

- Postal and courier services
- Waste management
- Chemicals
- Food
- Manufacturing
- Digital services
- Research

Size

EU-NIS 2 uses uniform criteria (2003/361/EC) to identify operators based on business size to harmonize diverging thresholds throughout the EU:

- **Large enterprises: ≥ 250 employees, $> 50\text{m EUR}$ turnover, $> 43\text{m EUR}$ balance** **SEEBURGER**
- **Medium enterprises: < 250 employees, $\leq 50\text{m EUR}$ turnover, $\leq 43\text{m EUR}$ balance**

New Compliance Requirements 2024 – Expect a Kick in Cyber Security Enquiries like with EU-GDPR 2018



Regulation so Far

1. Germany
 1. Legacy KRITIS §8a : 3.000 companies
 2. Legacy KRITIS §8c : another 3.000 companies ?
 3. Finance: BAFIN (BAIT, ZAIT & VAIT)
2. Other EU member states had no or more or less comparable regulation (except in Finance)

Starting 18.10.2024

1. In Germany ~30.000 companies are affected
2. Other parts of the EU add another ~30.000 companies

There is a massive increase of regulated companies due to EU-NIS 2 compliance

We expect a lot Cyber Security Enquiries (like with GDPR since 2018)

Digital Operational Resilience Act (DORA) EU Regulation 2022/2554



DORA is basically like NIS 2 on steroids for companies on financial markets

DORA has been in force since 16.01.2023 and the implementation period of two years ends on 17.01.2025

DORA mandates the European Supervisory Authorities (ESAs = EBA, EIOPA and ESMA) to define technical standards within the framework of legal acts

SEEBURGER is indirectly affected as an ICT provider (management of ICT third party risk Articles 28 to 44)

Like other ICT providers, SEEBURGER is practically regulated twice

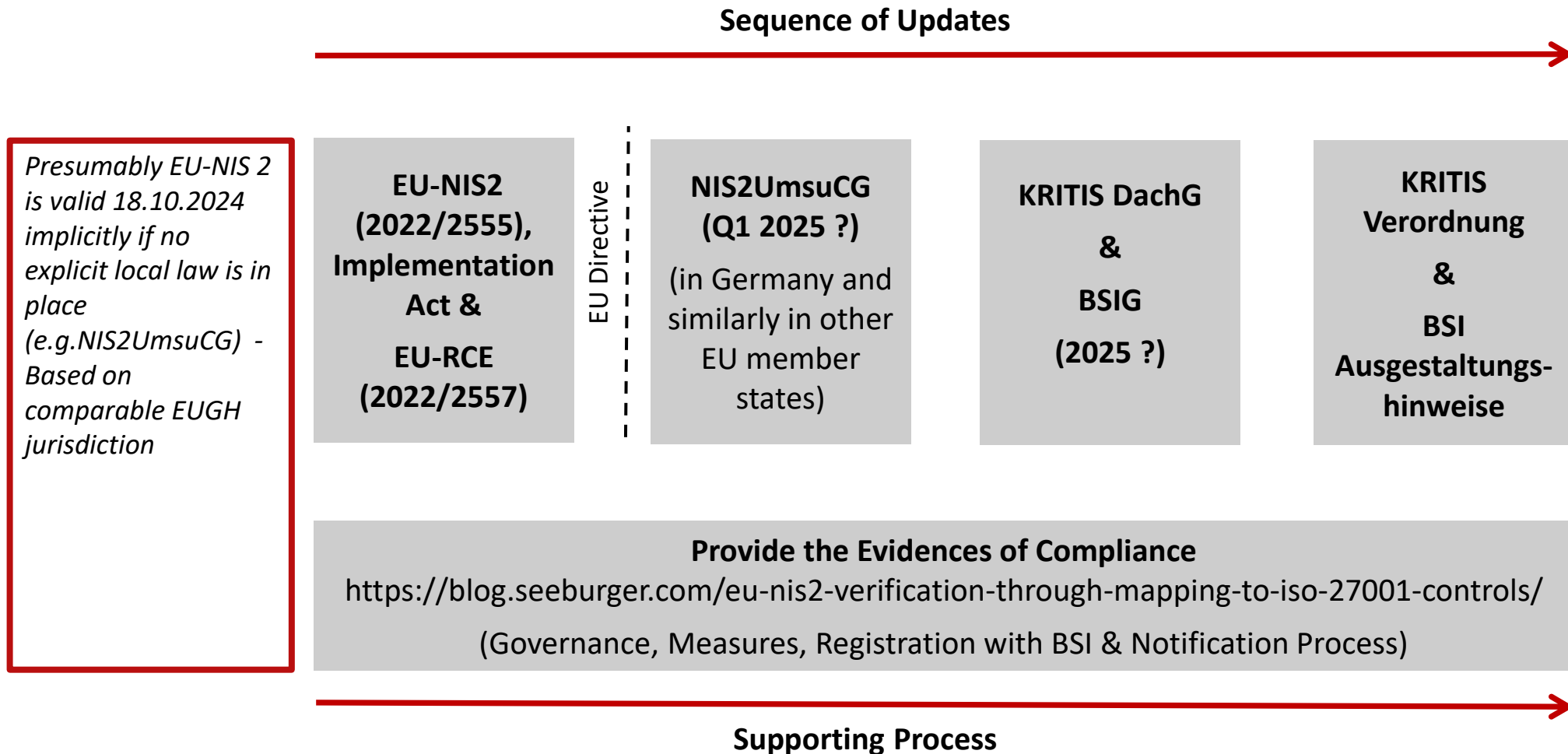
SEEBURGER acts as a „normal“ ICT provider under Article 30.2

02

Laws in EU Member
States (Example
NIS2UmsuCG)



EU-NIS 2 Law in Germany for the EU-NIS 2 and the according Implementation Act

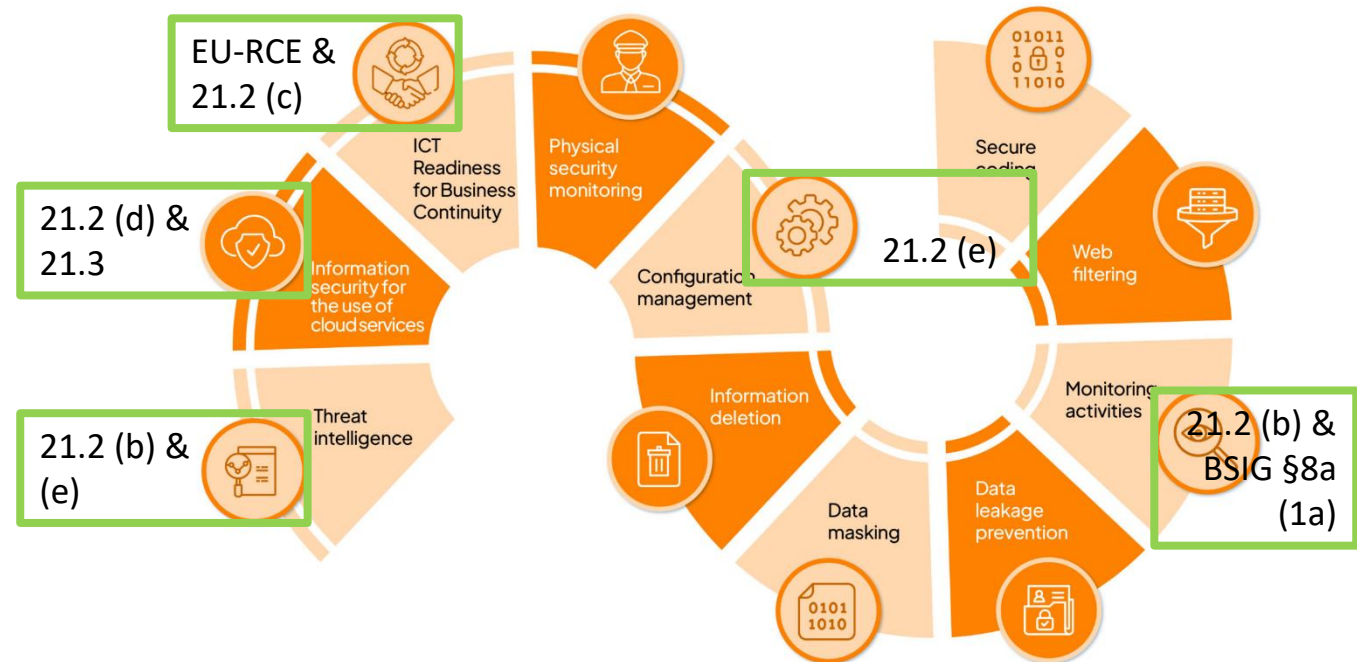


The SEEBURGER Approach

Get ready with Certifications 2024 for EU-NIS 2

- 1) Complete the upgrade to ISO 27001:2022
- 2) Check if your ISO 27001:2022 scope suffices
- 3) Check the NIS 2 EU IT Implementation Act (ETA 24.10.2024)
- 4) Use Control Mappings for Compliance Evidence
ISO 27001 → EU-NIS 2 Article 21 and Implementation Act
- 5) Add Effectiveness Evidence if available
 - ISAE 3402 SOC 1 Type 2
 - TISAX (only every 3 years)
 - BSI C5....
- 6) Local Cyber Agency (e.g. BSI in Germany)
 - Register with Cyber Agency
 - Establish Security Incident reporting process
- 7) Consider
 - Details from the local law (e.g. NIS2UmsuCG)
 - Comprehensive supplier management

Updated Controls List

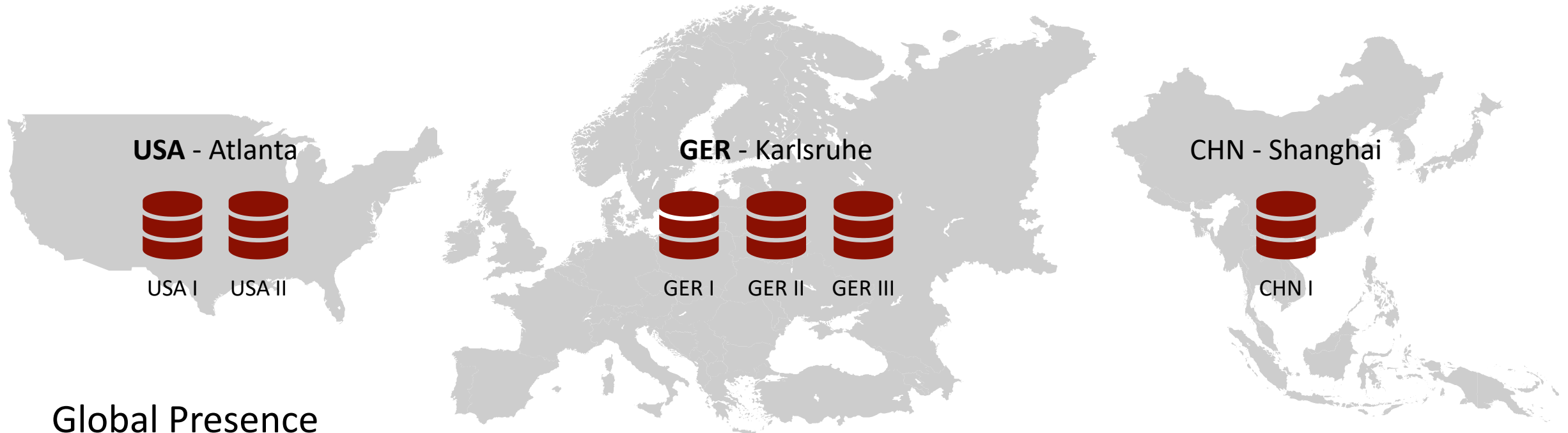


03

Information Security
at SEEBURGER



SEEBURGER Data Centers - Technical and Operational Measures (TOMs) for the Cloud



Global Presence

- + ISO Scope
"SEEBURGER Cloud Services EDI / B2B, GTS and iPaaS Operations including the process components Go-Live, Incident Management, Event Management & Monitoring, Change Management as well as the supporting IT processes"
- + Tier 3+ data centers in Germany, China and USA
- + International data protection agreements (IGDTA)
- + ISO/IEC 27001 Certification, annually since 2012
 - + The migration from ISO/IEC 27001:2017 to 27001:2022 is done from SEEBURGER's side
 - + Due to the 3 year certification our ISO 27001 certificate will fully reflect this Q3 2025
- + ISAE 3402 SOC 1 Type 2, annually since 2017
- + TISAX certification
 - + effectiveness audit & attestation of ISO 27001
 - + since 2020 in a 3-year cycle

SEEBURGER Information Security Certifications 2024 at a glance

ISO 27001

- + Proof that the organization has implemented an effective Information Security Management System (ISMS)
- + Internationally recognized standard
- + De facto standard that all our customers demand
- + Specified control mechanisms from ISO 27002
- + Verified annually by audit (KPMG) since 2012

ISAE 3402 SOC1 Type 2

- + Proof that installed controls are effectively implemented
- + Auditing on the basis of retrospective sampling in the period under review (12 months)
- + Provides very specific information on the quality and effectiveness of the implemented controls
- + Detailed audit report, which is also made available to the customer
- + Verified annually by audit (KPMG) since 2017
- + Telemaxx meanwhile has their own SOC 1 report

TISAX

- + Effectiveness control in the automotive industry
- + Industry-specific proof of information security based on ISO 27001 with predefined scope
- + Classification according to assessment levels and maturity levels
- + Verified by external audit (KPMG) every 3 years since 2020

Operations



On Premises



iPaaS



Fully-Managed-Service

	On Premises	iPaaS	Fully-Managed-Service
Trading Partner Management	Customer	Customer	SEEBURGER
Change Management	Customer	Customer	SEEBURGER
Mapping Development	Customer	Customer	SEEBURGER
Incident Management	Customer	Customer	SEEBURGER
Monitoring and Detection of Incidents	Customer	Customer	SEEBURGER
BIS Release Management	Customer	SEEBURGER	SEEBURGER
Operate and maintain Database	Customer	SEEBURGER	SEEBURGER
Operate and maintain OS	Customer	SEEBURGER	SEEBURGER
Network	Customer	SEEBURGER	SEEBURGER
Hardware & Infrastructure	Customer	SEEBURGER	SEEBURGER
Support for On Premises	SEEBURGER	Not required	Not required
Consulting	SEEBURGER	Optional	Optional
BIS Development	SEEBURGER	SEEBURGER	SEEBURGER

ISO 27001 (TISAX & ISAE 3402 SOC 1)

ISO 27001, TISAX & ISAE 3402 SOC 1

The processes for BIS Development, Support for On Premises and Consulting customers are a subset and follow adapted but in principle similar specifications, however they are not an explicit part of the certification scope.

Customer
SEEBURGER

ISO27001:2022 A.5 Security Incident Management

Cloud Customers Threat Intelligence & PEN Testing Example


- Trigger for Security Incident Process

- Notification/Incident
- Major Findings
 - PEN Testing
 - Vulnerability Scans
- Audits
- Major CVEs

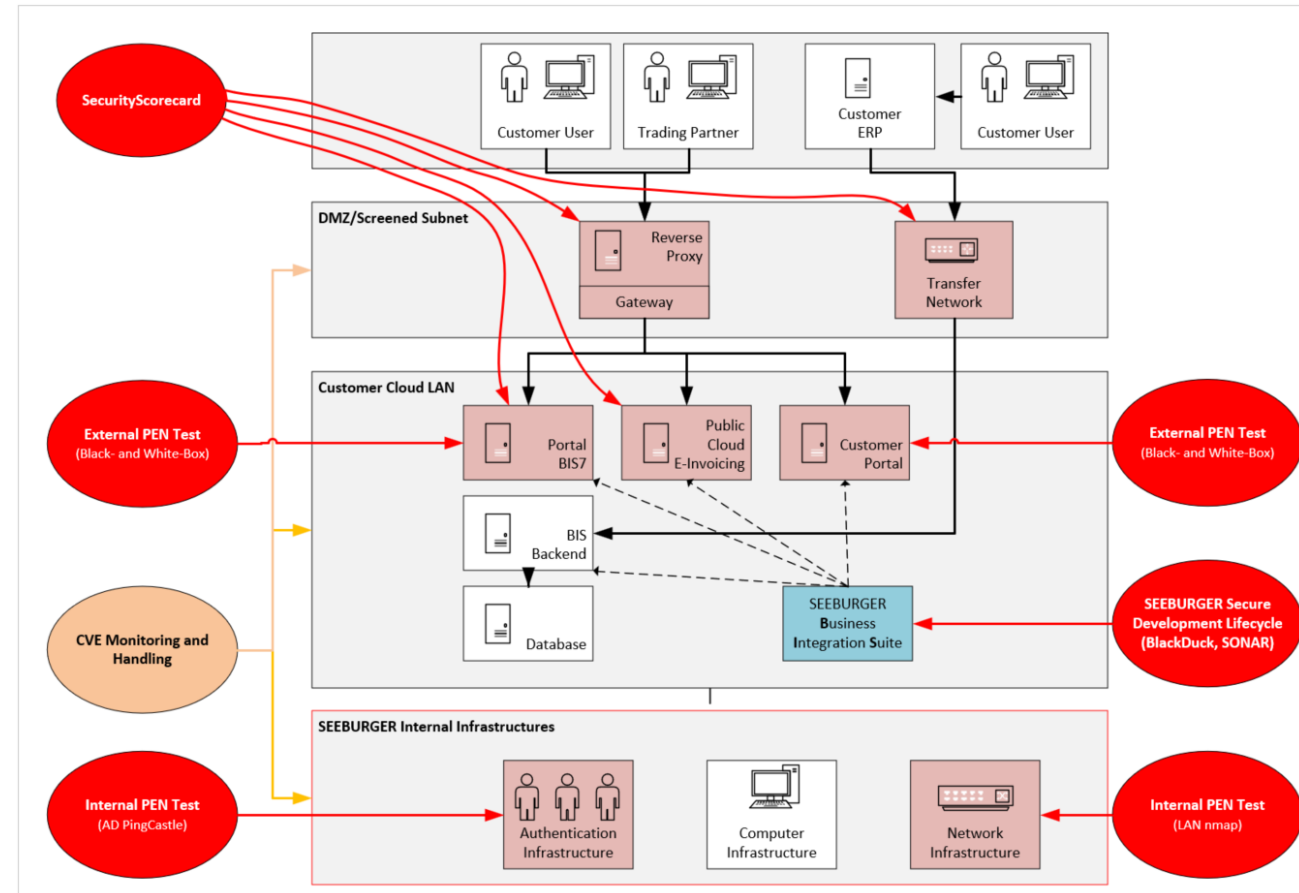
- Tools and Ressources

- Pink Castle
- KALI Linux
- NTFS Permissions Reporter
- Security Scorecard: 96 / 100 (23.09.2024)

 **SEEBURGER AG Security Rating**
seeburger.com

 **A** 96 / 100

- CVE Monitoring



ISO27001:2022 A.5 Security Incident Management

On Premises Customers Threat Intelligence & PEN Testing

- SEEBURGER supports on premises customers with security-related aspects of SEEBURGER software and solutions based on vulnerability handling and according disclosure
- Errors can be rectified by providing instructions, patches, hotfixes or new releases of the software. Details can be found in user documentation and release notes via SEEBURGER Service Desk which the customer screens.
- If SEEBURGER offers the customer a patch, hotfix or a new release to rectify errors, the customer is obliged to accept it and is responsible for installing them as provided by SEEBURGER as part of software maintenance

PEN Tests combined in 2024 (last update 23.09.2024):

- Information Security
 - Planned Tests: 7
 - Tests in progress: 2
 - Tests done: 2
- Corporate IT
 - Planned Tests: 1
 - Tests in progress: 1
 - Tests done: 0
- Cloud IT
 - Planned Tests: 5
 - Tests in progress: 1
 - Tests done: 1
- Development
 - Planned Tests: 2
 - Tests in progress: 1
 - Tests done: 1
- **Summary 2024 so far**
 - Overall planned Tests: 15
 - Tests in progress: 5
 - Tests done: 4

Security Scorecard: 96 / 100

ISO27001:2022 Annex 5.29, 5.30 & 8.14 Business Continuity Management

There are BCP and DR plans in place for a potential disruption while delivering services, support and consulting

SEEBURGER prepares for emergencies, crises and disasters based on ISO 27001

We also pick best practices provided by the German government institution BSI (Bundesamt für Informationssicherheit - IT Grundschutzkompendium 200-4) with a focus on current cyber security scenarios

Cyber-Krisenmanagement EDIT LINKS

Taskforce_BCM_RP_Plans · English_2024

[+ new document](#) or drag files here

All Documents

✓	Name	Modified	Version
	Supplemental_Procedures	... August 1, 2023	1.0
	1_ISO_27001_Policy_A5-29etal_BCM_2025_EN	... August 23	1.0
	2a_KS-Cyber-Crisis_Managementplan_2024	... August 15	17.0
	3a_KS_Team_Roles_2024	... August 23	20.0
	3b_KS_Role_Cards_2024	... August 15	9.0
	3c_KS_Communication_FAQ_Crisis_Management_plan_2024	... August 6	4.0
	3d_KS_Protocol_Template_2024	... August 6	8.0
	3e_KS_Simple_Protocol_Template_Meeting_2024	... August 6	8.0
	3f_KS_Vizualisation_Template_2024	... August 6	10.0
	4_BCM_Administration_Marketing_2024	... August 13	9.0
	4_BCM_AdministrationPayment-HR_2024	... August 13	10.0
	4_BCM_Cloud_IT_2024	... 4 days ago	8.0
	4_BCM_Consulting_2024	... August 9	12.0
	4_BCM_Development_2024	... August 13	11.0
	4_BCM_Sales_2024	... August 13	13.0
	4_BCM_SEEBURGER_Informatik_EOOD_BG_2024	... August 13	4.0
	4_BCM_SEEBURGER_US_2024	... August 13	5.0
	4_BCM_Support_2024	... August 13	9.0

3rd Party Platforms for Appraisal of Information Security

Cyber Risk Rating Platforms

- CRRs scan from the outside for vulnerabilities and provide a generic score
- SEEBURGER only uses and maintains one CRR:
<https://securityscorecard.com/security-rating/seeburger.com>
- SEEBURGER can't maintain all the others:
 1. Bitsight
 2. Black Kite
 3. BlueVoyant
 4. ISS Corporate Solutions
 5. Locate Risk
 6. Panorays
 7. Prevalent
 8. Recorded Future
 9. Risk Recon
 10. UpGuard.....

Third Party Risk Management Platforms

- TPRMs are Meta-Platforms to score provided information (certifications etc.)
- TPRMs may contain CRR functionality
- We can't maintain meta-certifications scores:
 1. Aravo
 2. Archer
 3. Cybervadis
 4. Diligent TPM
 5. Exiger
 6. IBM OpenPages
 7. LogicGate
 8. MetricStream TPM
 9. Navex
 10. Onetrust TPM
 11. Prevalent
 12. ProcessUnity
 13. ServiceNow TPM
 14. Venminder.....

04

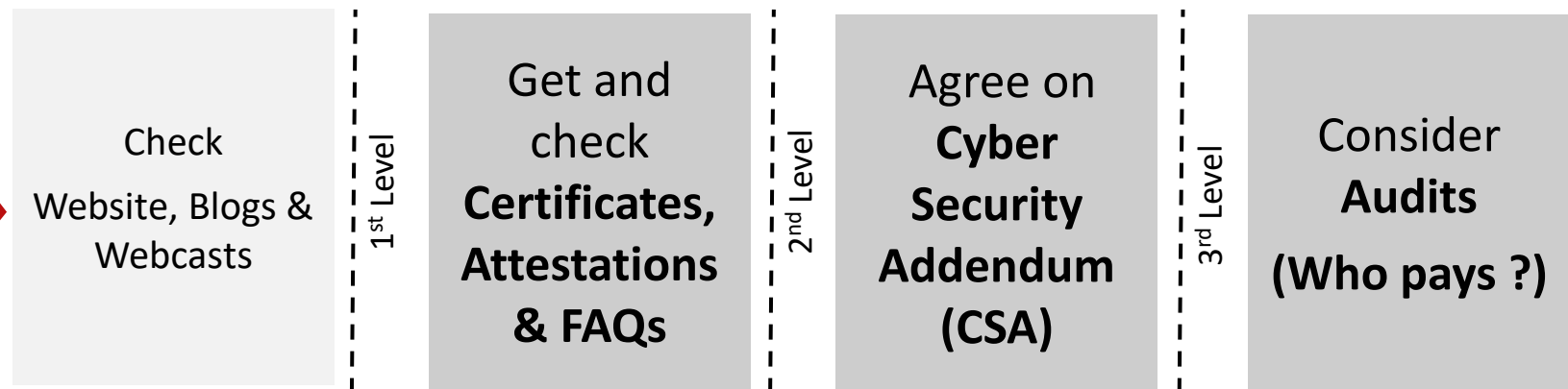
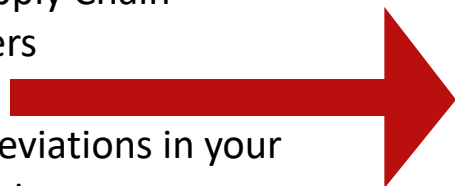
Check your
Supply Chain



Information Security & EU-NIS 2

Check Supplier with a structured Appraisal Process

1. Central Supplier Register
2. Internal counterparts
3. Use Case and setup of your solution
4. Add Contract value
5. Add Confidentiality, Integrity, Availability, Authenticity & Criticality for Supply Chain
6. Prioritize suppliers
7. **Check supplier**
8. Document the deviations in your Risk Management



Information Security & EU-NIS 2

EU IT Implementation Act

EU IT Implementation Act for NIS 2 regulates the details of NIS 2 Article 20 & 21 as well as the significant incidents of article 23

ISO 27001:2022 Mappings are available

- <https://blog.seeburger.com/eu-nis2-verification-through-mapping-to-iso-27001-controls/>
- <https://www.openkritis.de/massnahmen/implementing-acts-it-nis2-mapping.html>

Download the DRAFT

- https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en
→ Draft implementing regulation and the Annex - Ares(2024)4640447
- ETA 24.10.2024

EU IT Implementation Act 5.1.4. may lead to Cyber Security Addendums (CSAs) efforts similar to the 2018 GDPR §28 (Data Protection Agreements – DPAs) efforts

- ICT suppliers have their own Cyber Security Standards
- Work with reasonable approach which ICT suppliers can accept and can argue with their own suppliers
- Reduce effort for yourself and ICT suppliers looking for relevant certifications
- Get reasonable response rates and answers swiftly

EU-NIS 2 Article 21.2 (d) & 21.3 Supplier Management – EU IT Implementation Act Article 5.1.4

Cyber Security Addendum

EU IT Implementation Act 5.1.4.

Based on the supply chain security policy and taking into account the results of the risk assessment carried out in accordance with point 2.1. of this Annex, the relevant entities **shall ensure that their contracts with the suppliers and service providers specify**, where appropriate through service level agreements, specify the following, **where appropriate**:

- (a) cybersecurity requirements for the suppliers or service providers, including requirements as regards the security in acquisition of ICT services or ICT products set out in point 6.1.;
- (b) requirements regarding skills and training, and where appropriate certifications, required from the suppliers' or service providers' employees;
- (c) requirements regarding background checks of the suppliers' and service providers' employees pursuant to point 10.2.;
- (d) an obligation on suppliers and service providers to notify, **without undue delay**, the relevant entities of incidents that present a risk to the security of the network and information systems of those entities;
- (e) provisions on repair times;
- (f) **the right to audit or right to receive audit reports**;
- (g) an obligation on suppliers and service providers to handle vulnerabilities that present a risk to the security of the network and information systems of the relevant entities;
- (h) requirements regarding subcontracting and, where the relevant entities allow subcontracting, cybersecurity requirements for subcontractors in accordance with the cybersecurity requirements referred to in point (a);
- (i) obligations on the suppliers and service providers at the termination of the contract, such as retrieval and disposal of the information obtained by the suppliers and service providers in the exercise of their tasks.....



Brussels, XXX
[...] (2024) XXX draft

ANNEX

ANNEX

to the

Commission Implementing Regulation

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

05

Next Steps checking
SEEBURGER



Information Security & EU-NIS 2

Individual Customer Enquiries

SEEBURGER will use Priority Boarding mainly based on incoming date and complexity of enquiry

SEEBURGER doesn't consider suitable

1. Large Excel Spreadsheets in customer freestyle
2. Portal Questionnaires, because these are high risk due to the lack of legal evidence
3. TPRM-Portals
 - <https://www.processunity.com/> etc.
 - Outside EU GDPR and EU AI Act
 - TPRM require that SEEBURGER accepts the respective TPRM T&Cs. Typically they use our intellectual properties and content to train their own AI
 - TPRM require SEEBURGER annual payment and maintenance

SEEBURGER Information Security delivers towards the SEEBURGER standard and CSA

SEEBURGER Information Security doesn't consider suitable

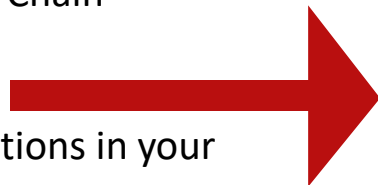
1. External Cyber Security Contracts with
 - Unclear TOMs
 - Additional guarantees like
 - "Immediately" instead of "undue delay"
 - SLAs....
 - Burden of proof moves to SEEBURGER
 - Increased liability
 - Audit Rights without limits and payment
 - Evidences required beyond the SEEBURGER Standard
2. Cost for external legal council or requirements for negotiations

Instead we prefer to focus on Information Security itself and extending certifications to increase the safety of our entire installed base

Information Security & EU-NIS 2

Check SEEBURGER in line with your structured Appraisal Approach

1. Find your own internal counterparts
2. Document Use Case and setup of your SEEBURGER solution
3. Add Contract value
4. Add Confidentiality, Integrity, Availability, Authenticity & Criticality for Supply Chain
5. Prioritize suppliers
6. **Check SEEBURGER**
7. Document the deviations in your Risk Management



Check
Website, Blogs &
Webcasts

SSD
Knowledgebase
#20240708-0362

1st Level

Get and
check
**Certificates,
Attestations
& FAQs**

2nd Level

Get and sign
**SEEBURGER
CSA**

3rd Level

Participate in
SEEBURGER
**Audit
Convention
2025**

Evidences of necessary due diligence



Contact your SEEBURGER Sales contact for our Cyber Security Addendum (EU IT Implementation Act for NIS 2 Article 5.1.4)

SEEBURGER will deliver along the lines of the SEEBURGER CSA, even if the customer hasn't signed it. This is our standard based on the law and ISO 27001.





2024 SEEBURGER AG. All rights reserved.

The information in this document is proprietary to SEEBURGER. Neither any part of this document, nor the whole of it may be reproduced, copied, or transmitted in any form or purpose without the express prior written permission of SEEBURGER AG. Please note that this document is subject to change and may be changed by SEEBURGER at any time without notice. SEEBURGER's Software product, the ones of its business partners may contain software components from third parties.

As far as reference to other brands is concerned, we refer to the following:

SAP®, SAP® R/3®, SAP NetWeaver®, SAP Cloud Platform & Cloud Platform Integrator®, SAP Archive Link®, SAP S/4HANA®, SAP® GLOBAL TRADE Service® (SAP GTS), SAP Fiori®, ABAP™ and SAP ARIBA® are registered trade marks of the SAP SE or the SAP Deutschland SE & Co. KG (Germany). Microsoft, Windows, Windows Phone, Excel, Outlook, PowerPoint, Silverlight, and Visual Studio are registered trademarks of Microsoft Corporation in the United States and other countries. Linux is a registered trade mark of Linus Torvalds in the United States and other countries. UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group. Adobe, the Adobe logo, Acrobat, Flash, PostScript, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and / or other countries. HTML, ML, XHTML, and W3C are trademarks, registered trademarks, or claimed as generic terms by the Massachusetts Institute of Technology (MIT), European Research Consortium for Informatics and Mathematics (ERCIM), or Keio University. Oracle and Java are registered trademarks of Oracle and its affiliates.

All other company and software names mentioned are registered trademarks or unregistered trademarks of their respective companies and are, as such, subject to the statutory provisions and legal regulations. 4invoice®, iMartOne®, SEEBURGER®, SEEBURGER Business-Integration Server®, SEEBURGER Logistic Solution Professional®, SEEBURGER Web Supplier Hub®, WinELKE®, SEEBURGER File Exchange®, SEEBURGER Link®, SMART E-Invoice® and other products or services of SEEBURGER which appear in this document as well as the according logos are marks or registered marks of the SEEBURGER AG in Germany and of other countries worldwide. All other products and services names are marks of the mentioned companies.

All contents of the present document are noncommittal and have a mere information intention. Products and services may be country-specific designed. All other mentioned company and software designations are trade marks or unregistered trade marks of the respective organizations and are liable to the corresponding legal regulations.

- The information in this document is proprietary to SEEBURGER. No part of this document may be reproduced, copied, or transmitted in any form or purpose without the express prior written permission of SEEBURGER AG.
- This document is a preliminary version and not subject to your license agreement or any other agreement with SEEBURGER. This document contains only intended strategies, developments, and functionalities of the SEEBURGER product and is not intended to be binding upon SEEBURGER to any particular course of business, product strategy, and/or development. Please note that this document is subject to change and may be changed by SEEBURGER at any time without notice.
- SEEBURGER assumes no responsibility for errors or omissions in this document. SEEBURGER does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.
- SEEBURGER shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intent or gross negligence.
- The statutory liability for personal injury and defective products is not affected. SEEBURGER has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party web pages nor provide any warranty whatsoever relating to third-party web pages.