JOERG HAMPEL

❑ 25 years of writing SW for a living

❑ Started using LabVIEW in 2007

❑ Founded HSE around 2015/2016

Talk to me about

❑ Working in small teams

❑ Working in fixed-price scenarios

❑ Process & workflow standardisation/automation

❑ Inner Source and Open Source with and in LabVIEW

LabVIEW CHAMPION

ARCHITECT

INSTRUCTOR

Center of Excellence

DQMH® Trusted Advisor

DQMH® Consortium

DSH WORKSHOPS

WUERZBURG bit.ly/WUELUG

North of Britain bit.ly/NOBLUG

CREATE BETTER SOFTWARE!

We work with teams of developers to **increase** the **quality** of their software through **improved** development **processes**.

ARCHITECT

LabVIEW CHAMPION

INSTRUCTOR

WUERZBURG bit.ly/WUELUG

North of Britain bit.ly/NOBLUG

SAM SM SYSTEM FOR AWARD MANAGEMENT

DSH WORKSHOPS

DQMH® Trusted Advisor

ALA

Partner

Center of Excellence

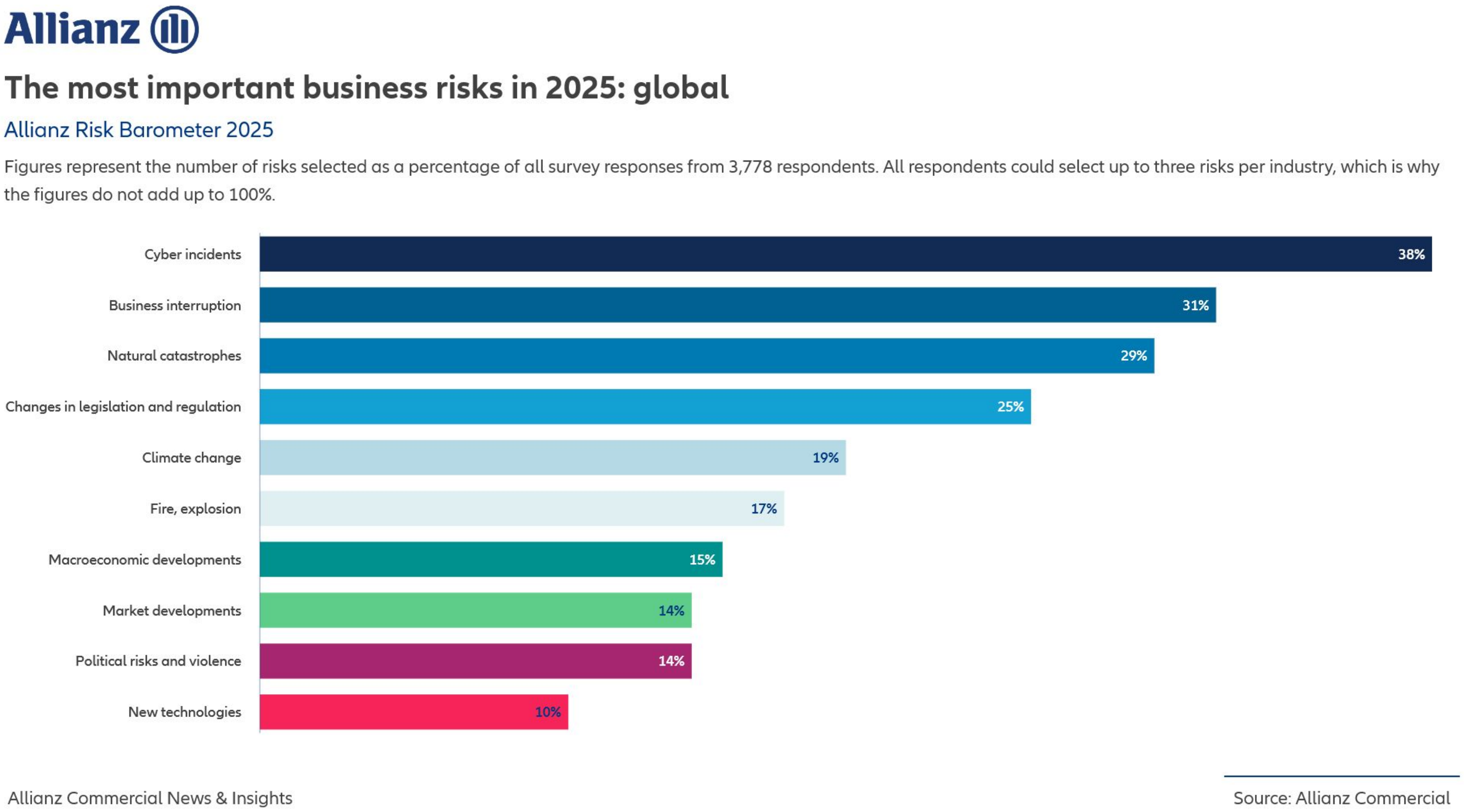
🏆 Global Consultant Impact Award 2025 🏆

SMALL COMPANY, BIG THREATS

Cyber Security for the Rest of Us

⚠️ DISCLAIMER ⚠️

This guy?
Not a lawyer!



Allianz

The most important business risks in 2025: global

Allianz Risk Barometer 2025

Figures represent the number of risks selected as a percentage of all survey responses from 3,778 respondents. All respondents could select up to three risks per industry, which is why the figures do not add up to 100%.

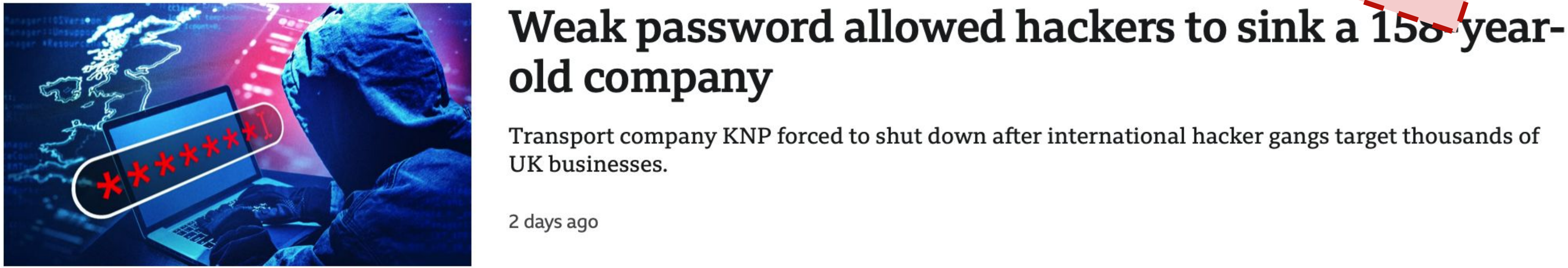
Allianz Commercial News & Insights

Source: Allianz Commercial

[Allianz Risk Barometer 2025 Report]

eve it or not, this works!

GUESSED PASSWORD



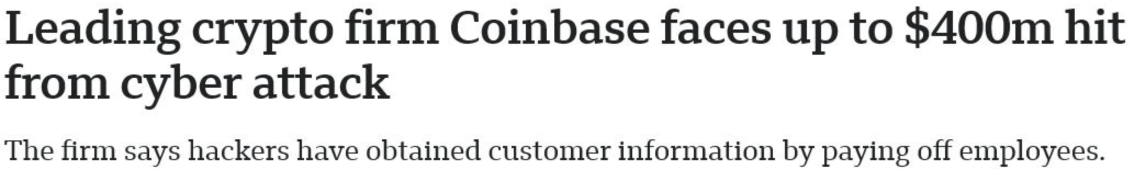
Weak password allowed hackers to sink a 158-year-old company

Transport company KNP forced to shut down after international hacker gangs target thousands of UK businesses.

2 days ago

[BBC, Reuters, The Guardian]

BRIBED EMPLOYEES

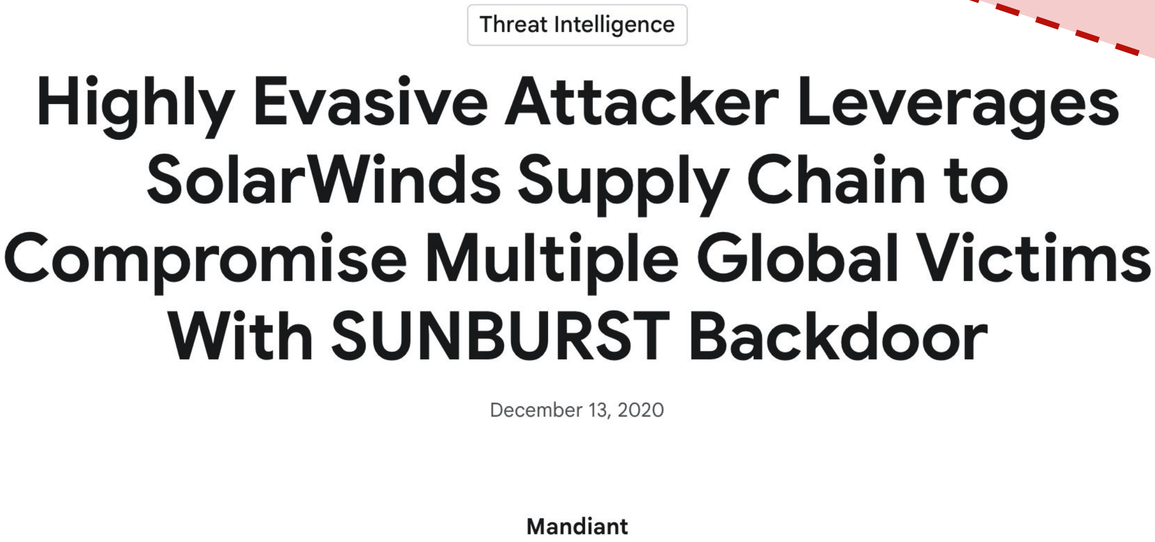


Leading crypto firm Coinbase faces up to $400m hit from cyber attack

The firm says hackers have obtained customer information by paying off employees.

[BBC, Reuters, The Guardian]

INJECT BACKDOOR



Threat Intelligence

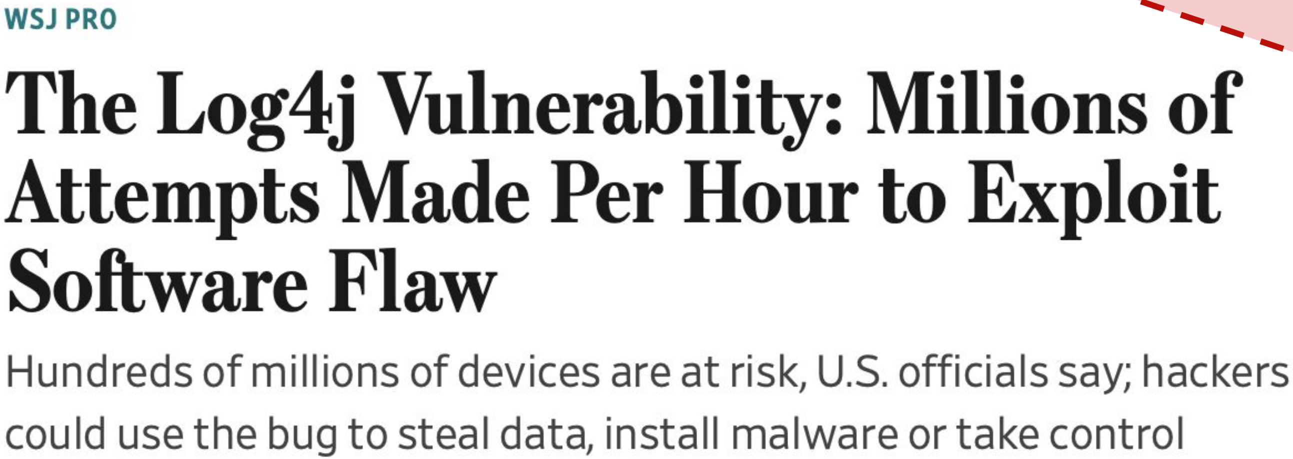
Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

December 13, 2020

Mandiant

[FireEye Google Bloc]

EXPLOIT VULNERABILITY



WSJ PRO

The Log4j Vulnerability: Millions of Attempts Made Per Hour to Exploit Software Flaw

Hundreds of millions of devices are at risk, U.S. officials say; hackers could use the bug to steal data, install malware or take control

[The Wall Street Journal]

Test your knowledge:
Secret Service or CyberSec jargon?

CRA

EU Cyber Resilience Act

NIK

Nemzeti Információs Központ

(Hungarian National Information Center)

NCSC

National Cyber Security Centre (UK)

BSI

Bundesamt für Sicherheit in der Informationstechnik

(Federal Office for Information Security)

ZTNA

Zero Trust Network Architecture

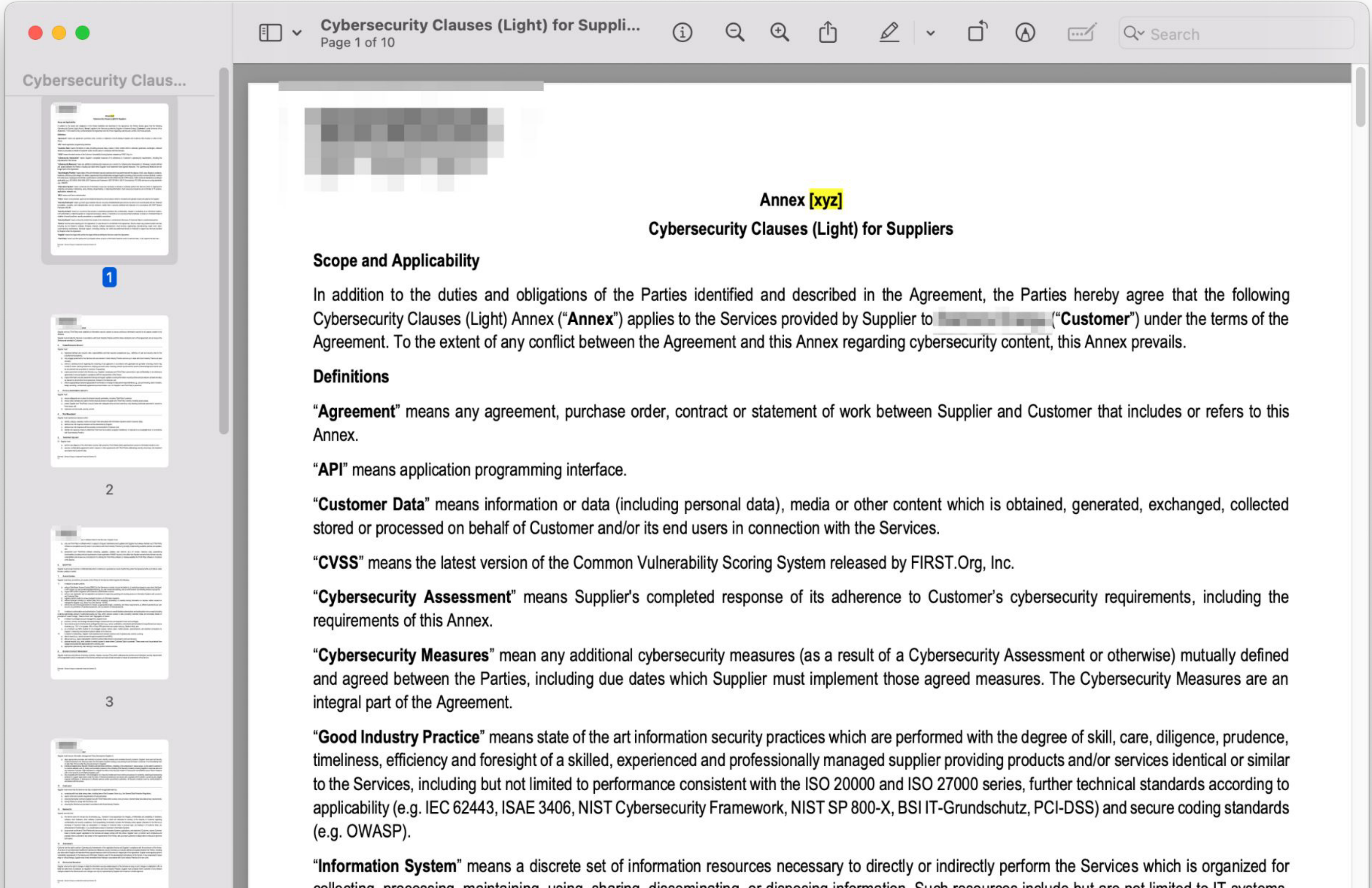
ASIS

Australian Secret Intelligence Service

ISMS

Information Security Management System

How our CS journey started



[redacted]

Annex [xyz]

Cybersecurity Clauses (Light) for Suppliers

Scope and Applicability

In addition to the duties and obligations of the Parties identified and described in the Agreement, the Parties hereby agree that the following Cybersecurity Clauses (Light) Annex ("**Annex**") applies to the Services provided by Supplier to [redacted] ("**Customer**") under the terms of the Agreement. To the extent of any conflict between the Agreement and this Annex regarding cybersecurity content, this Annex prevails.

Definitions

"**Agreement**" means any agreement, purchase order, contract or statement of work between Supplier and Customer that includes or refers to this Annex.

"**API**" means application programming interface.

"**Customer Data**" means information or data (including personal data), media or other content which is obtained, generated, exchanged, collected stored or processed on behalf of Customer and/or its end users in connection with the Services.

"**CVSS**" means the latest version of the Common Vulnerability Scoring System released by FIRST.Org, Inc.

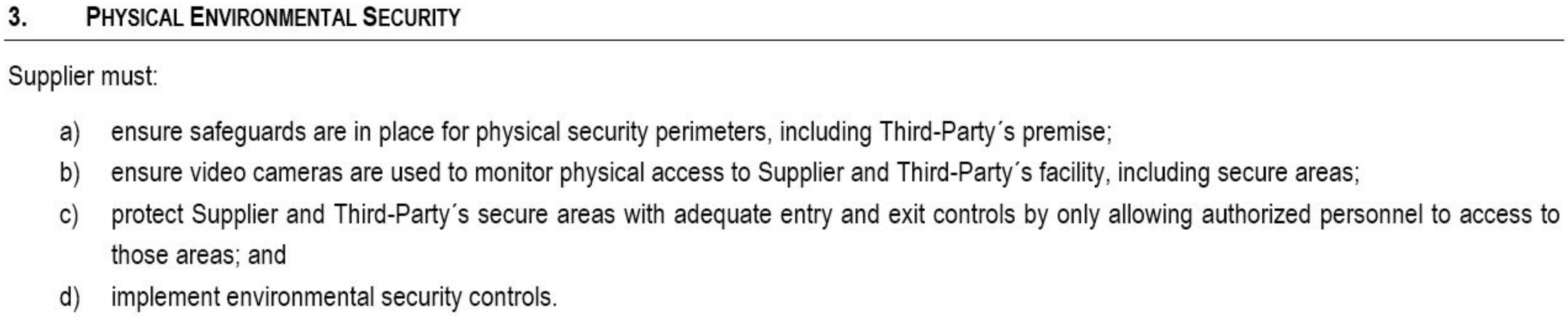
"**Cybersecurity Assessment**" means Supplier's completed response of its adherence to Customer's cybersecurity requirements, including the requirements of this Annex.

"**Cybersecurity Measures**" mean any additional cybersecurity measures (as a result of a Cybersecurity Assessment or otherwise) mutually defined and agreed between the Parties, including due dates which Supplier must implement those agreed measures. The Cybersecurity Measures are an integral part of the Agreement.

"**Good Industry Practice**" means state of the art information security practices which are performed with the degree of skill, care, diligence, prudence, timeliness, efficiency and foresight of a skilled, experienced and professionally managed supplier providing products and/or services identical or similar to the Services, including but not limited to performance consistent with the ISO 20000 and ISO 27000 series, further technical standards according to applicability (e.g. IEC 62443, ISAE 3406, NIST Cybersecurity Framework, NIST SP 800-X, BSI IT-Grundschutz, PCI-DSS) and secure coding standards (e.g. OWASP).

"**Information System**" means a discrete set of information resources necessary to directly or indirectly perform the Services which is organized for collecting, processing, maintaining, using, sharing, disseminating, or disposing information. Such resources include but are not limited to IT systems

Are these really applicable to us?



3. PHYSICAL ENVIRONMENTAL SECURITY

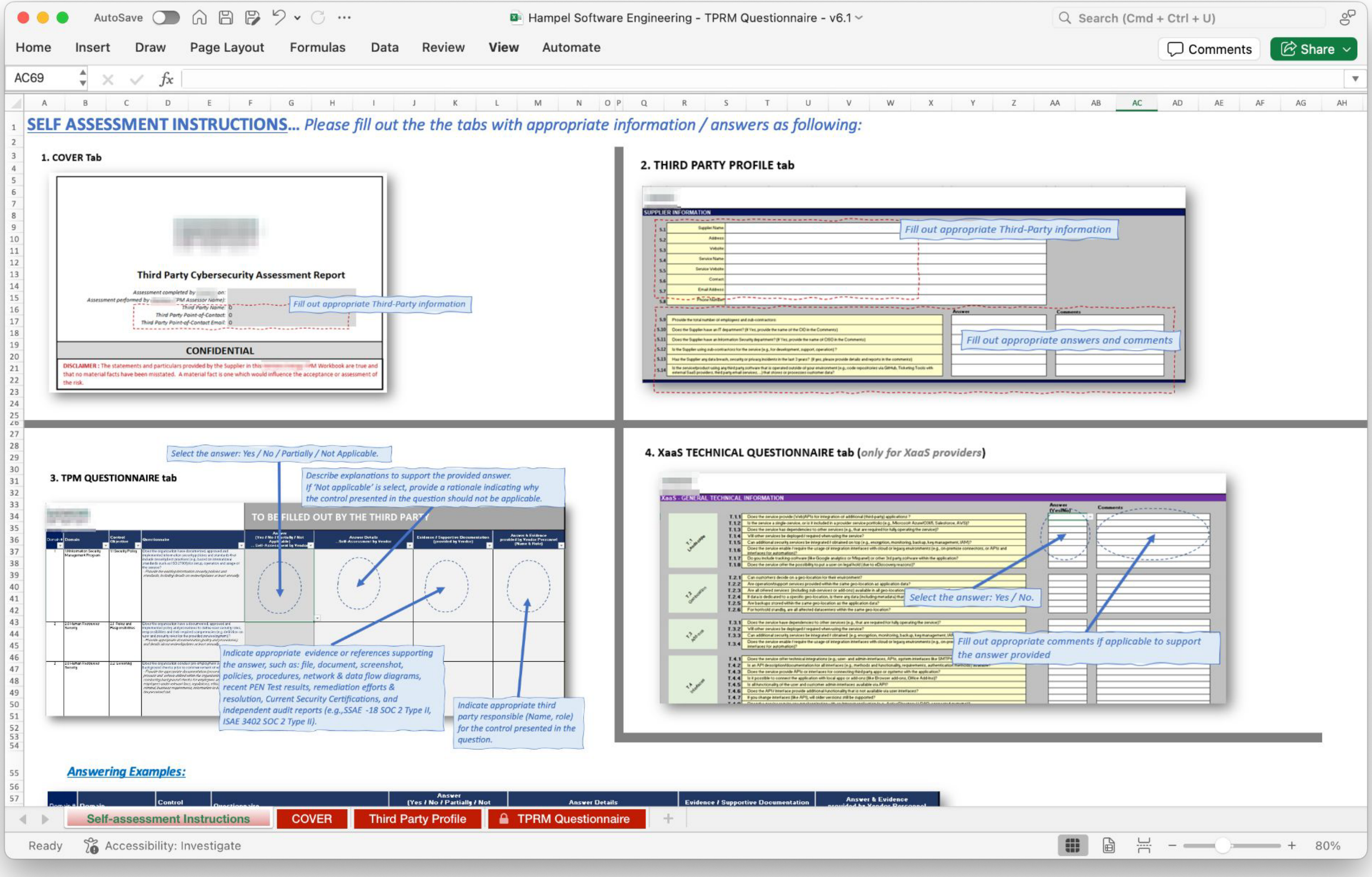
Supplier must:

a) ensure safeguards are in place for physical security perimeters, including Third-Party´s premise;

b) ensure video cameras are used to monitor physical access to Supplier and Third-Party´s facility, including secure areas;

c) protect Supplier and Third-Party´s secure areas with adequate entry and exit controls by only allowing authorized personnel to access to those areas; and

d) implement environmental security controls.



SELF ASSESSMENT INSTRUCTIONS… *Please fill out the the tabs with appropriate information / answers as following:*

1. COVER Tab

Third Party Cybersecurity Assessment Report

Assessment completed by [redacted] on:
Assessment performed by [redacted] PM Assessor Name):
Third Party Name: 0
Third Party Point-of-Contact: 0
Third Party Point-of-Contact Email: 0

Fill out appropriate Third-Party information

CONFIDENTIAL

DISCLAIMER : The statements and particulars provided by the Supplier in this [redacted] PM Workbook are true and that no material facts have been misstated. A material fact is one which would influence the acceptance or assessment of the risk.

2. THIRD PARTY PROFILE tab

SUPPLIER INFORMATION

S.1	Supplier Name	
S.2	Address	
S.3	Website	
S.4	Service Name	
S.5	Service Website	
S.6	Contact	
S.7	Email Address	
S.8	Phone Number	

Fill out appropriate Third-Party information

		Answer	Comments
S.9	Provide the total number of employees and sub-contractors		
S.10	Does the Supplier have an IT department? (If Yes, provide the name of the CIO in the Comments)		
S.11	Does the Supplier have an Information Security department? (If Yes, provide the name of CISO in the Comments)		
S.12	Is the Supplier using sub-contractors for the service (e.g., for development, support, operation)?		
S.13	Has the Supplier any data breach, security or privacy incidents in the last 3 years? (If yes, please provide details and reports in the comments)		
S.14	Is the service/product using any third party software that is operated outside of your environment (e.g., code repositories via GitHub, Ticketing Tools with external SaaS providers, third party email services, ...) that stores or processes customer data?		

Fill out appropriate answers and comments

3. TPM QUESTIONNAIRE tab

Select the answer: Yes / No / Partially / Not Applicable.

Describe explanations to support the provided answer.
If 'Not applicable' is select, provide a rationale indicating why the control presented in the question should not be applicable.

TO BE FILLED OUT BY THE THIRD PARTY

Domain #	Domain	Control Objective	Questionnaire	Answer (Yes / No / Partially / Not Applicable) ... Self-Assessment by Vendor	Answer Details ... Self-Assessment by Vendor	Evidence / Supportive Documentation (provided by Vendor)	Answer & Evidence provided by Vendor Personnel (Name & Role)
1	1.0 Information Security Management Program	1.1 Security Policy	Does the organization have documented, approved and implemented information security policies and standards that include security best practices (e.g. based on international standards such as ISO 27001) for setup, operation and usage of the service?				
2	2.0 Human Resources Security	2.1 Roles and Responsibilities	Does the organization have a documented, approved and implemented policy and procedures to define user security roles, responsibilities and their required competencies (e.g. definition on user and security roles for the provided service/system)?				
2	2.0 Human Resources Security	2.2 Screening	Does the organization conduct pre-employment background checks prior to commencement of [illegible]				

Indicate appropriate evidence or references supporting the answer, such as: file, document, screenshot, policies, procedures, network & data flow diagrams, recent PEN Test results, remediation efforts & resolution, Current Security Certifications, and independent audit reports (e.g.,SSAE -18 SOC 2 Type II, ISAE 3402 SOC 2 Type II).

Indicate appropriate third party responsible (Name, role) for the control presented in the question.

4. XaaS TECHNICAL QUESTIONNAIRE tab (*only for XaaS providers*)

XaaS - GENERAL TECHNICAL INFORMATION

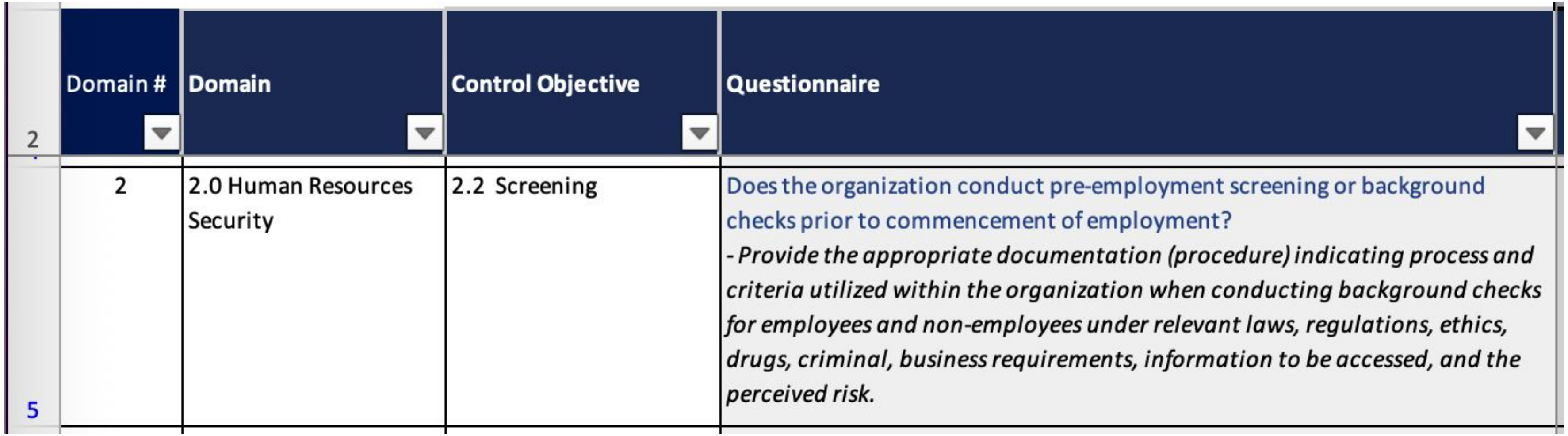
Select the answer: Yes / No.

Fill out appropriate comments if applicable to support the answer provided

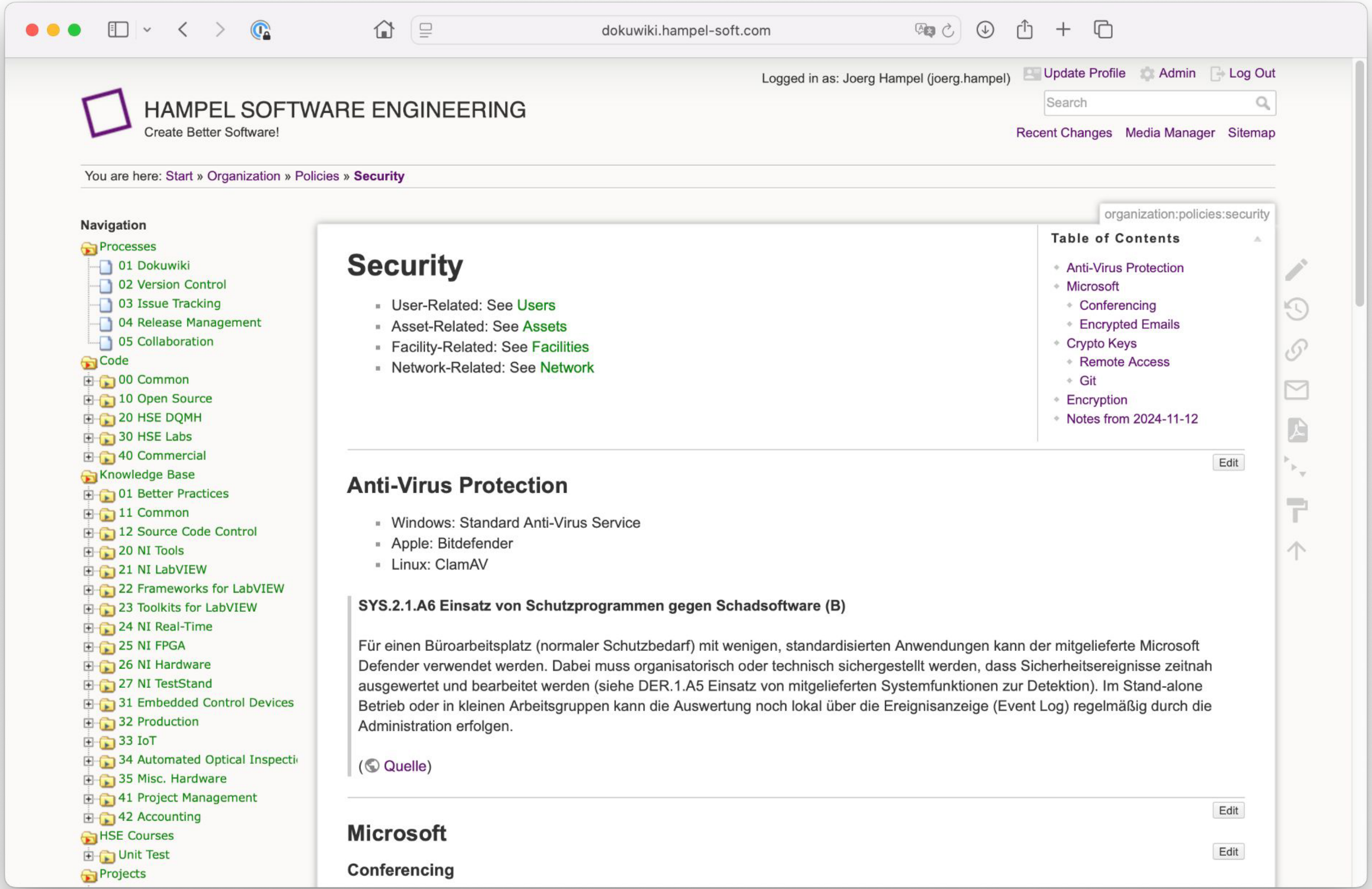
Answering Examples:

Domain #	Domain	Control	Questionnaire	Answer (Yes / No / Partially / Not	Answer Details	Evidence / Supportive Documentation	Answer & Evidence provided by Vendor Personnel

Are these *REALLY* applicable to us?



2	Domain #	Domain	Control Objective	Questionnaire
5	2	2.0 Human Resources Security	2.2 Screening	Does the organization conduct pre-employment screening or background checks prior to commencement of employment? *- Provide the appropriate documentation (procedure) indicating process and criteria utilized within the organization when conducting background checks for employees and non-employees under relevant laws, regulations, ethics, drugs, criminal, business requirements, information to be accessed, and the perceived risk.*



Security

- User-Related: See Users
- Asset-Related: See Assets
- Facility-Related: See Facilities
- Network-Related: See Network

Table of Contents

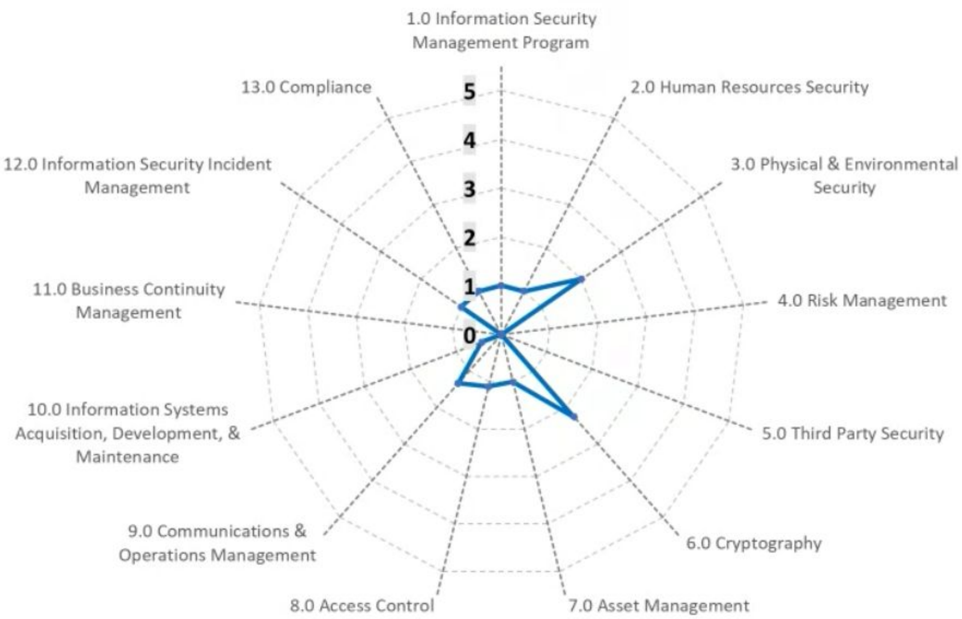
Anti-Virus Protection

- Windows: Standard Anti-Virus Service
- Apple: Bitdefender
- Linux: ClamAV

> **SYS.2.1.A6 Einsatz von Schutzprogrammen gegen Schadsoftware (B)**
>
> Für einen Büroarbeitsplatz (normaler Schutzbedarf) mit wenigen, standardisierten Anwendungen kann der mitgelieferte Microsoft Defender verwendet werden. Dabei muss organisatorisch oder technisch sichergestellt werden, dass Sicherheitsereignisse zeitnah ausgewertet und bearbeitet werden (siehe DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion). Im Stand-alone Betrieb oder in kleinen Arbeitsgruppen kann die Auswertung noch lokal über die Ereignisanzeige (Event Log) regelmäßig durch die Administration erfolgen.
>
> (Quelle)

Microsoft

Conferencing



Maturity Levels (see Appendix A for definitions)

5 – Optimizing

4 – Quantitatively Managed

3 – Defined

2 – Managed

1 – Initial

0 – Non-existent

A more strategic approach

What is out there?

- Legislation
  - European Union Cyber Resilience Act
- Organisations
  - BSI
  - NIST
- Standards and Frameworks
  - ISO 27001 (international standard)
  - NIST
    - Cybersecurity Framework 2.0 (private sector)
    - Special Publication 800-53 (federal sector)
    - Special Publication 1300 (system engineers and developers in SME)
  - BSI-200 (German federal guidelines)

EU Cyber Resilience Act (CRA)

- ❑ Mandatory security/design standards for digital products (software, hardware, IoT) sold in EU
  - ❑ All products with "digital elements" — hardware and software
- ❑ Binding regulations with fines for non-compliance
  - ❑ High-Impact Violations: €15 million or 2.5% of global annual turnover (whichever is higher)
- ❑ Applies extraterritorially to any product placed on EU market
  - ❑ Yes, also those coming from the US!

EU Cyber Resilience Act (CRA)

- Take cybersecurity into account
  - During development, including risk assessments, secure design (e.g., encryption, minimal attack surfaces), and secure defaults (e.g., no weak passwords, auto-updates). Mandatory vulnerability management and SBOM creation.
- Prove requirements
  - A declaration of conformity is required. For most products this is a self-assessment by the manufacturer, for a few it is an assessment by a 3rd party body.
- Disclose vulnerabilities
  - A single platform will be set up for reporting exploited vulnerabilities and major security incidents. All reports must be submitted through it.
- Secure during the entire support period
  - Security updates must be made available to the end user and vulnerabilities must be handled throughout the entire product life cycle. This support period is generally 5 years.

CRA equivalents in the US? There are none!

- Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA, 2022)
- CISA / NIST-led voluntary frameworks and policies
- Executive Order 14028 (Improving the Nation's Cybersecurity, 2021)
- Federal Information Security Modernization Act (FISMA, 2014)
- Sector-specific and proposed legislation
  - HIPAA (Health Insurance Portability and Accountability Act)

ISO 27001

- International standard for Information Security Management Systems
  - ISMS
- Released in 2005, revisions in 2013 and 2022
- Organizations can get certified against ISO 27001
- International recognition
- No easy guidelines to help to implement it
- Hard to implement for small companies

NIST Cybersecurity Framework 2.0

- ❑ Broad high-level guidance for improving cybersecurity across various sectors
- ❑ Released in 2024 (version 2.0)
- ❑ No official certification
- ❑ Flexible, provides guidelines and best practices

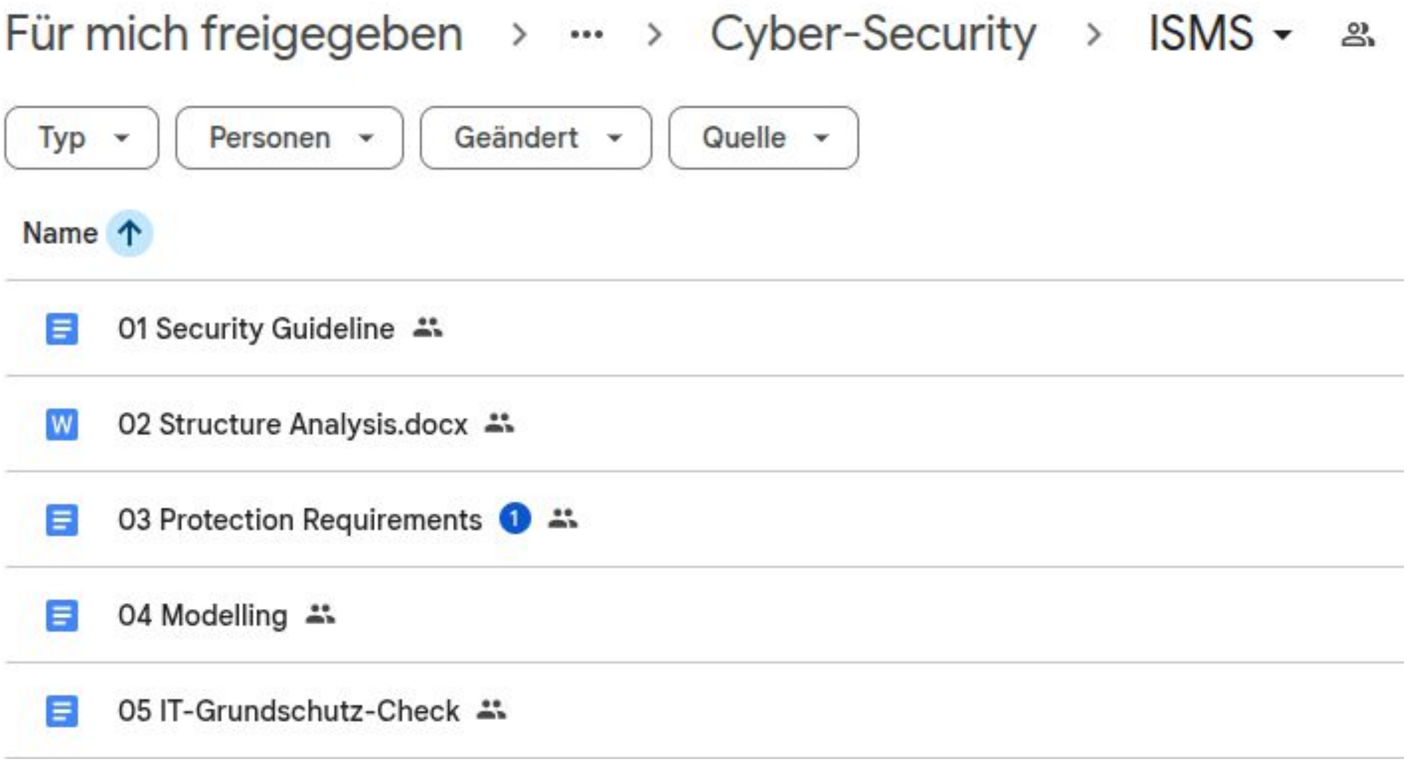
BSI Grundschutz (baseline protection)

- Includes standards like BSI 200-1, 200-2, 200-3
- Guidelines provided by the German Federal Office for Information Security
- Focus on implementing an ISMS
- **Comprehensive guidance** and modular, risk-based approach
- Lots of **training resources**, guidelines, and examples (also in English!)
- Integration with IT-Grundschutz (baseline protection) methodology
- Can be used as the basis for an **ISO 27001** certification

What is an ISMS?

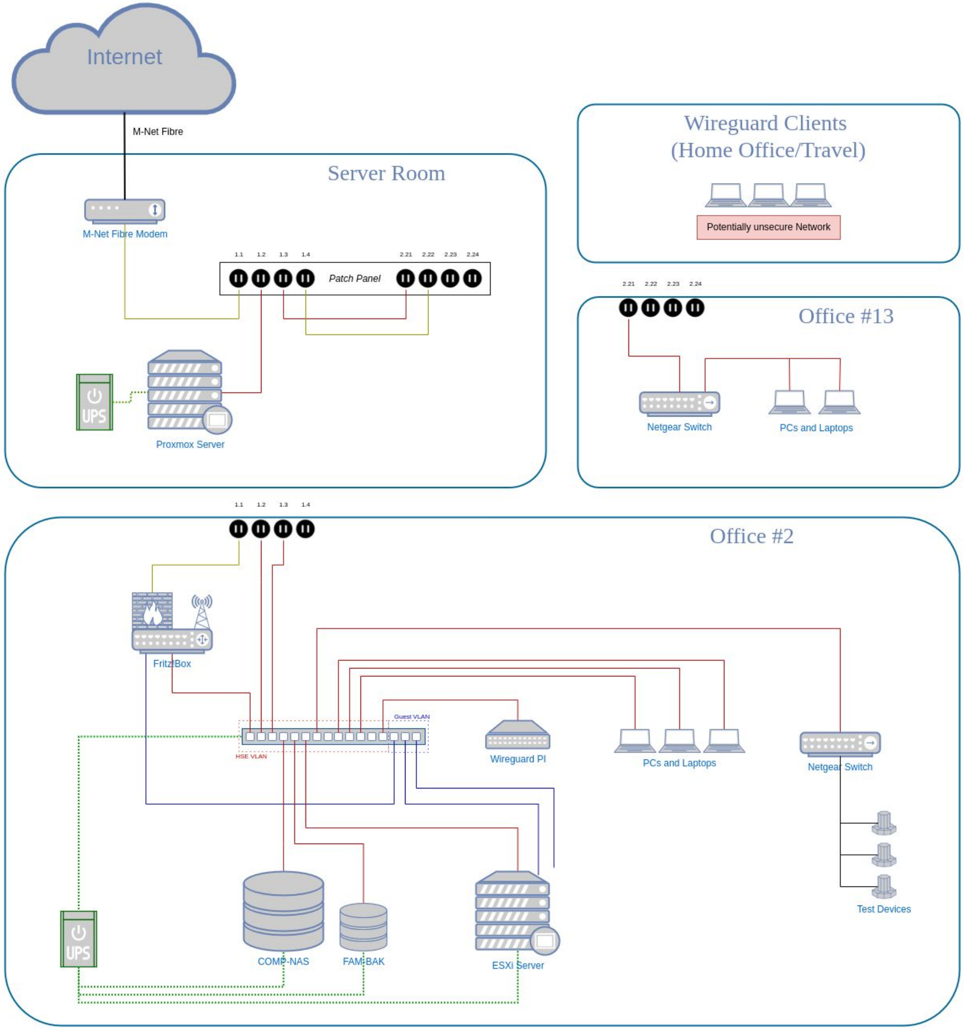
- ❑ A **structured set** of policies and procedures that define how your company manages and protects information security
- ❑ It typically includes **documentation** on assets, roles and responsibilities, risk assessments, access controls, incident response plans, business continuity measures, and compliance requirements
- ❑ The ISMS ensures a **systematic approach** to safeguarding company data and responding to security threats

The HSE ISMS



Für mich freigegeben › ··· › Cyber-Security › ISMS

- 01 Security Guideline
- 02 Structure Analysis.docx
- 03 Protection Requirements 1
- 04 Modelling
- 05 IT-Grundschutz-Check


Internet
M-Net Fibre
Server Room
M-Net Fibre Modem
1.1
1.2
1.3
1.4
Patch Panel
2.21
2.22
2.23
2.24
UPS
Proxmox Server
Wireguard Clients
(Home Office/Travel)
Potentially unsecure Network
2.21
2.22
2.23
2.24
Office #13
Netgear Switch
PCs and Laptops
1.1
1.2
1.3
1.4
Office #2
FritzBox
Guest VLAN
HSE VLAN
Wireguard PI
PCs and Laptops
Netgear Switch
Test Devices
UPS
COMP-NAS
FAM-BAK
ESXi Server

1. Business Processes

GP = Geschäftsprozess

Identifier	Name (Type)	Description	Responsible Employee
GP01	SW development (core process)	We write SW for others to use.	Developer Team
GP02	Consulting (core process)	Give training, code reviews, workshops, consulting in general.	Developer Team
GP03	Accounting & HR	We prepare the basics, then the tax consultant finalizes it.	HR Team

2. Used Software

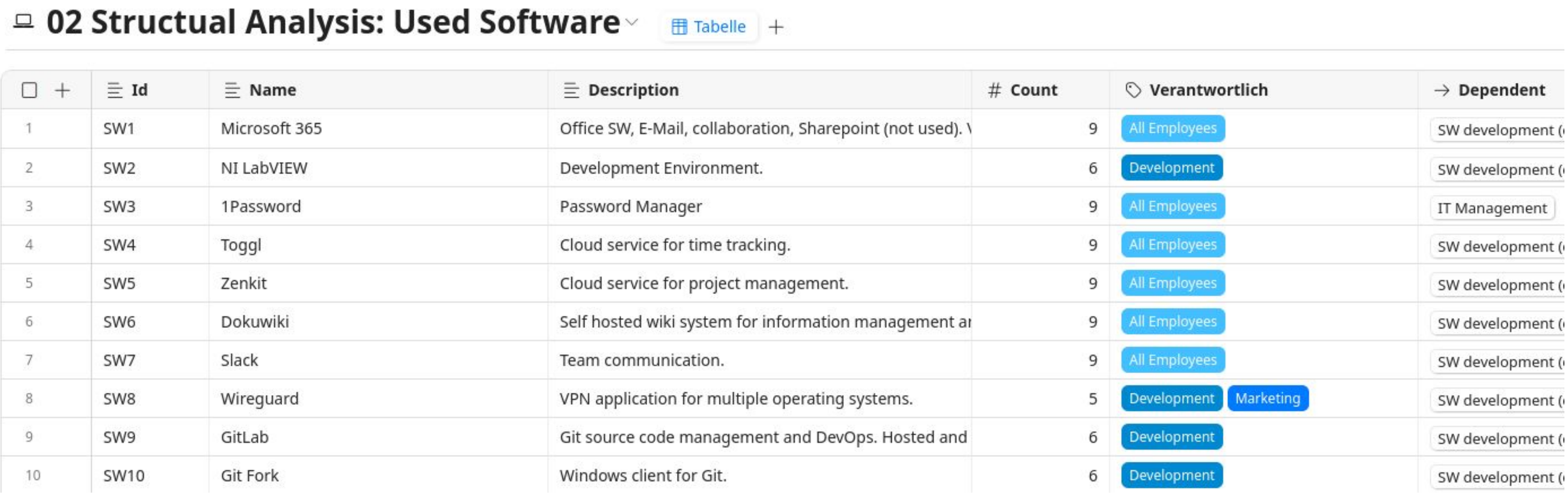
2.1 Applications

Identifier	Name	Description	Count	Responsible Employee
A001	Microsoft 365	Office SW, E-Mail, collaboration, Sharepoint (not used). Versions for web use, Windows, macOS, iOS, Android	9	All Employees
A002	NI LabVIEW	Development Environment (VM)	6	Development Team
A003	1Password	Password Manager	9	All Employees
A004	Toggl (cloud)	Time tracking	9	All Employees

3. IT Systems & Infrastructure

3.1 IT Systems

ID	System Type	Description	Location	Status
IT001	Personal Laptops	Everybody's workstation	On-premises / home office	Operational
IT002	Proxmox VM Server	Hosting Proxmox VMs	Server Room	Operational
IT003	ESXI Server	Hosting VMware VMs	Office #2	Operational
IT004	Comp-NAS	Synology DS716+II, data storage	Office #2	Operational
IT005	Comp-BAK	Synology DS214+, Backup	Office #2	Operational



02 Structual Analysis: Used Software

	Id	Name	Description	Count	Verantwortlich	Dependent
1	SW1	Microsoft 365	Office SW, E-Mail, collaboration, Sharepoint (not used). V	9	All Employees	SW development (
2	SW2	NI LabVIEW	Development Environment.	6	Development	SW development (
3	SW3	1Password	Password Manager	9	All Employees	IT Management
4	SW4	Toggl	Cloud service for time tracking.	9	All Employees	SW development (
5	SW5	Zenkit	Cloud service for project management.	9	All Employees	SW development (
6	SW6	Dokuwiki	Self hosted wiki system for information management ar	9	All Employees	SW development (
7	SW7	Slack	Team communication.	9	All Employees	SW development (
8	SW8	Wireguard	VPN application for multiple operating systems.	5	Development Marketing	SW development (
9	SW9	GitLab	Git source code management and DevOps. Hosted and	6	Development	SW development (
10	SW10	Git Fork	Windows client for Git.	6	Development	SW development (

Protection Levels

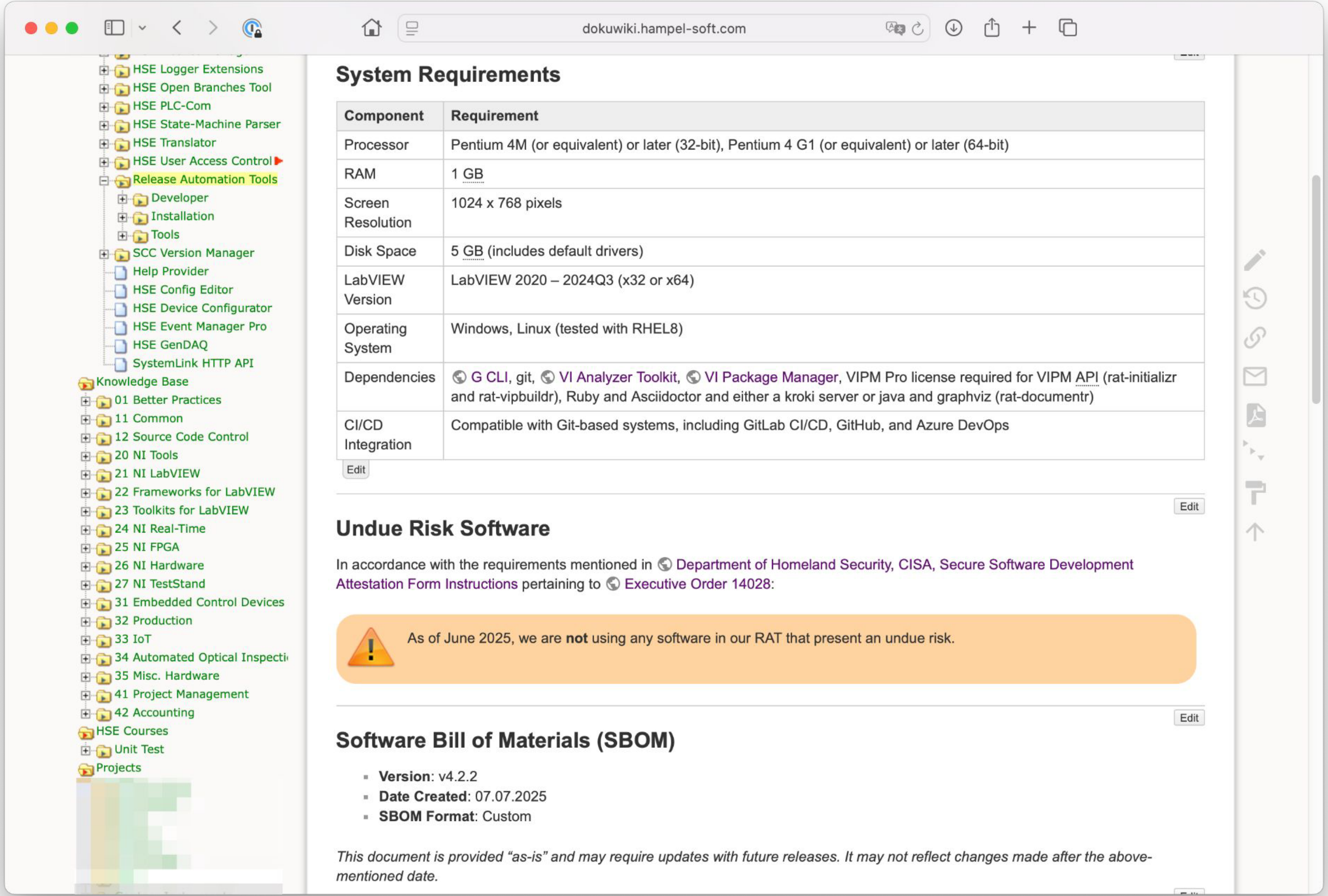
Potential loss is independent of downtime - those are separate cases.

- **Normal**
  Business processes will be affected only insignificantly at best.
  Potential financial loss is less than €2,500.
  Downtime of more than 24h is acceptable.
- **High**
  Business processes will be affected significantly.
  Potential financial loss is between €2,500 and €10,000.
  Downtime of up to 24h is acceptable.
- **Very High**
  Business processes are severely impaired.
  Potential financial loss is over €10,000.
  Downtime of more than 2h is not acceptable.

Reference: https://www.bsi.bund.de/dok/10990064

3. IT Systems

ID	Protection Level & Requirements	Reason
IT001 Personal Laptops	Confidentiality: **Very High**	The laptops can store personal data, sensitive business data and sensitive customer data.
	Integrity: **High**	Security vulnerabilities or malicious patches can impair business data and software for customers.
	Availability: **High**	Laptops are our primary working device.
IT002 Proxmox Server	Confidentiality: **Very High**	Virtual machines on the server can contain all sorts of sensitive business and customer data.
	Integrity: **High**	Incorrect data can usually be easily detected.
	Availability: **Normal**	We have no business critical applications on the server or in the hosted VMs.
IT003 ESXI Server	Confidentiality: **Very High**	Virtual Machines can contain sensitive data (currently being phased out). It is also planned to do accounting tasks in a VM.
	Integrity: **Very High**	Accounting data will need to have high integrity.
	Availability: **High**	Accounting data will need to have availability..



System Requirements

Component	Requirement
Processor	Pentium 4M (or equivalent) or later (32-bit), Pentium 4 G1 (or equivalent) or later (64-bit)
RAM	1 GB
Screen Resolution	1024 x 768 pixels
Disk Space	5 GB (includes default drivers)
LabVIEW Version	LabVIEW 2020 – 2024Q3 (x32 or x64)
Operating System	Windows, Linux (tested with RHEL8)
Dependencies	G CLI, git, VI Analyzer Toolkit, VI Package Manager, VIPM Pro license required for VIPM API (rat-initializr and rat-vipbuildr), Ruby and Asciidoctor and either a kroki server or java and graphviz (rat-documentr)
CI/CD Integration	Compatible with Git-based systems, including GitLab CI/CD, GitHub, and Azure DevOps

Undue Risk Software

In accordance with the requirements mentioned in Department of Homeland Security, CISA, Secure Software Development Attestation Form Instructions pertaining to Executive Order 14028:

As of June 2025, we are **not** using any software in our RAT that present an undue risk.

Software Bill of Materials (SBOM)

- **Version**: v4.2.2
- **Date Created**: 07.07.2025
- **SBOM Format**: Custom

This document is provided "as-is" and may require updates with future releases. It may not reflect changes made after the above-mentioned date.

Conclusion

★☆☆☆☆

Cannot recommend.

Joerg H.

Difficulties

- ❑ Know-How: Full ISO certification requires a dedicated cybersecurity expert
  - ❑ Someone who continuously keeps ISMS updated
- ❑ Compliance: Every employee must comply
  - ❑ CEO has responsibility
- ❑ Standards: Hard to read, understand and implement
  - ❑ Bureaucratic legalese
- ❑ Resources: Daily business vs. CS work
  - ❑ “Organisational debt / wealth”

Status

- We’re right in the middle of things
- 50% of BSI Grundschutz implemented
  - Goal: Finalize by the end of this year
- ISO 27001 certification
  - Goal: Audit in 2026

Resources

- Cyber Resilience Act
  - https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- ISO/IEC 27001:2022
  - https://www.iso.org/standard/27001
- NIST SP 800-53
  - https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- BSI Grundschutz
  - https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
- BSI Certification
  - https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/zertifizierung-und-anerkennung_node.html

..IT'S OK TO HAVE FUN!

Center of Excellence

INSTRUCTOR

DEVELOPER

ARCHITECT

LabVIEW CHAMPION

DQMH FRAMEWORK

DQMH Trusted Advisor

DSH WORKSHOPS

WUERZBURG LabVIEW USER GROUP bit.ly/WUELUG

ALA

Partner