

Public

Information Security Supplier Security Questionnaire

Webasto Group, November 2023



Public Part

The following slides can be shared with suppliers.

Note: These are only examples and neither recommendations nor complete.

Supplier Security Explained

Motivation

▪ Why Supplier Security?

- To fulfill our contracts, Webasto must ensure that suppliers can deliver or provide services to Webasto.
- Webasto must be able to assess the IT security or cyber resilience of the suppliers.

▪ What is the target of the questionnaire?

- The target is the IT landscape and organization of the supplier.
- The targets are **not** the services or products provided to Webasto.

▪ Is it sufficient to provide one of the requested certifications (TISAX, ISO 27001, SOC 2 Type 2)?

- The questions must always be answered.
- If a supplier holds a relevant certification, only evidence of the certification must be uploaded.

Supplier Security Explained

Question 1: CISO

Public

One person responsible for Information Security **MUST** be appointed and known to all employees.

Why?

- Without defined responsibilities and management support, IT and Information Security cannot be implemented in a company.

Possible Evidence

- Letter of Appointment
- Organizational Chart

LETTER OF APPOINTMENT

Sub: Letter of Appointment as Chief Information Security Officer (CISO) for ISO 27001:2013

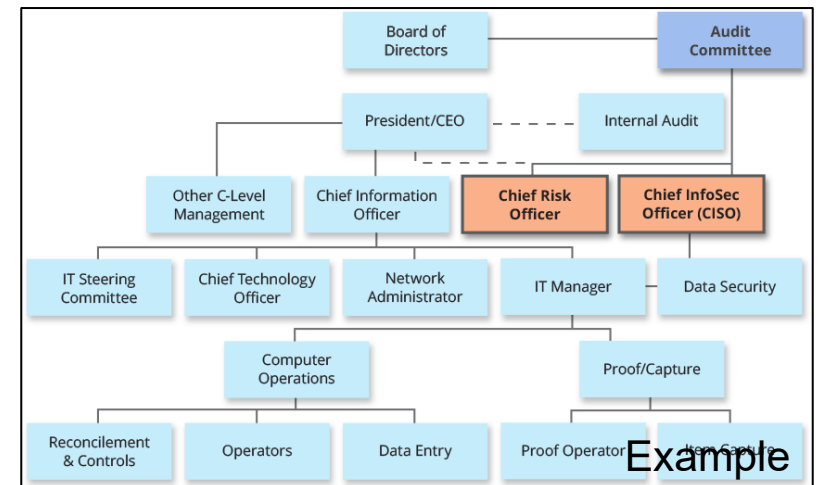
Dear

This is to inform you that you are appointed as CISO for ISO 27001 with effect from

In addition to your existing responsibilities following are the additional responsibilities:

1. Ensure that processes needed for the Information Security Management System (ISMS) are established, implemented and maintained in accordance with the standard requirements.
2. Ensuring the promotion of awareness of customer requirements and Legal requirements, Information security requirements communicated to employees and contractors.

Example



Supplier Security Explained

Question 2: ISMS

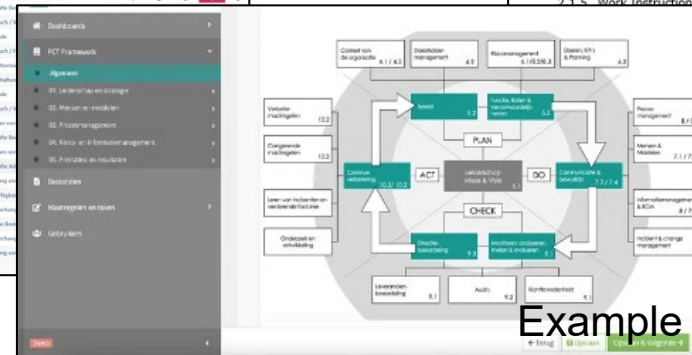
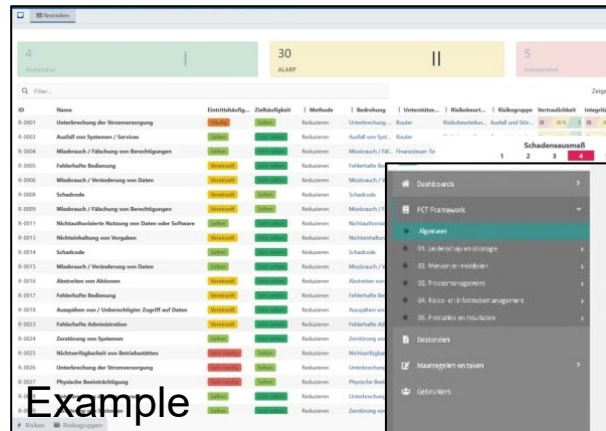
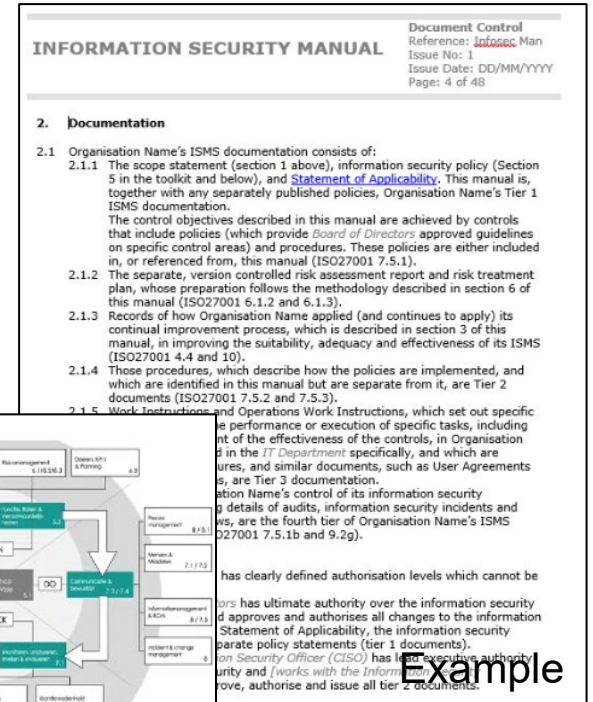
The supplier **MUST** have an Information Security Management System (ISMS) that covers at least the security organization, policies and risk management.

Why?

- Without dedicated and independent personnel, defined and communicated policies and a risk management for the whole organization, effective IT and Information Security is not possible.

Possible Evidence

- ISMS Tool (Screenshot)
- ISMS Documentation
- Slides explaining ISMS



Supplier Security Explained

Question 3: Mobile Devices

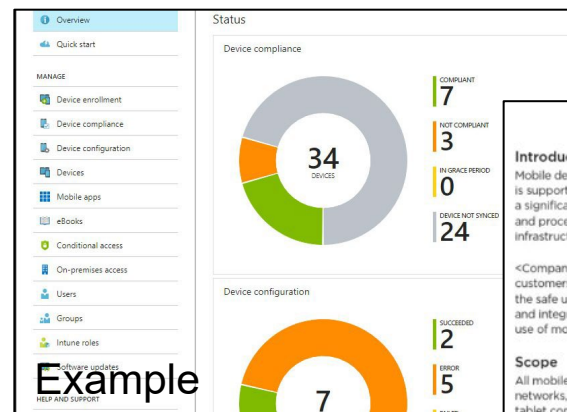
The supplier **SHOULD** have a concept covering the management and protection of mobile devices (smartphones, tablets, laptops and storage devices).

Why?

- Mobile devices are part of every companies IT, but small, portable devices can be stolen or lost and concepts like Bring your Own Device (BYOD) or its flavors add additional complexity and risks.

Possible Evidence

- Mobile Device Policy
- BYOD concept
- MDM* Suite (Screenshot)



Example

<Company> Mobile Device (BYOD) Policy

Introduction

Mobile devices, such as smartphones and tablet computers, are important tools for the company to achieve business goals. However, mobile devices (personal or company-owned) pose a significant risk to company information security and data protection. If the appropriate policies and procedures are not applied, they can be a conduit for unauthorized access to the company's infrastructure. This can subsequently lead to costly data leakages and system infections.

<Company> developed this mobile device policy to protect our information assets in customers, intellectual property and reputation. This document outlines a set of practical guidelines for the safe use of all mobile devices when accessing the corporate network and is intended to ensure the integrity of <Company's> data and technology infrastructure. <Company> reserves the right to restrict or prohibit the use of mobile devices if users do not abide by the policies and procedures outlined in this policy.

Scope

All mobile devices, whether owned by <Company> or owned by employees, that have access to the company network, data and systems, not including corporate IT-managed laptops. This includes smartphones, tablet computers. Limited exceptions to the policy may occur where there is a business justification. A risk assessment must be conducted by management and written approval provided in advance.

In order to have access to the company network, employees must agree to the terms and conditions set forth in this policy, and install required software onto their mobile devices.

Example

Mobile Phone Policy

The following are <COMPANY NAME>'s guidelines for using a mobile phone during work hours. Mobile phones are an essential part of our lives; at the same time, they pose severe health and safety concerns for our employees. Keeping in mind the safety of our employees, the following Mobile Phone Policy is adopted by the company. Each and every person must adhere to the code of practice.

<COMPANY NAME> puts its employees and visitor's safety at the forefront and is committed to ensuring a safe and healthy environment; as such, the use of mobile phones is strictly prohibited, except in the designated areas.

The policy applies to all employees, contract workers, contractors, and visitors to the company site.

A mobile phone includes any electronic device capable of communicating, processing data, or recording.

The use of personal mobile phones is strictly prohibited in the following areas:

- On operational plants, machinery, or any other equipment
- While assisting in any operation of plant, machinery, or equipment
- While working above the ground
- On the roads in the company premises
- While carrying out any work duty within the company's premises
- While driving vehicle
- While attending meetings

To ensure the privacy and safety of confidential information, using mobile phones to record confidential information is strictly prohibited.

The company encourages allowing the mobile phone in the following situations:

- In designated areas where they are considered safe
- For work-related communication where it is necessary
- To communicate any emergency
- To keep track of work progress or work-related tasks

In the interest of the public, all personnel are reminded not to use mobile phones while on roads.

Example

*MDM: Mobile Device Management

Supplier Security Explained

Question 4: Cloud Policy

The supplier **SHOULD** have a concept covering the access, use and protection of cloud services unless no externally provided IT services are used.

■ Why?

- Using external cloud or IT services potentially brings benefits regarding costs, cost efficiency, personnel and static hardware costs. However, it also introduces new challenges because there is less direct control over the hardware, software, services or personnel.

■ Possible Evidence

- Cloud Computing Policy
- Provider Risk Assessment

Supplier Security Requirements Questionnaire			
Supplier name:			v1.2
Supplier contact name:			
Supplier contact function:			
Date of the completion:			
Area	Requirement	Compliance Level	Score
Organizational Security	One person responsible for Information Security MUST be appointed and known to all employees.	Partially compliant	6
	The supplier MUST have an Information Security Management System (ISMS) that covers at least: - information security organization, - information security policies and controls, - an information security risk management process.	Partially compliant	6
	ISO 27001 A.5.1.1 and A.5.1.2		
	The supplier SHOULD have a concept covering the management and protection of mobile devices (smartphones, tablets, laptops and storage devices). ISO 27001 A.6.2 and A.6.3	Partially compliant	3
Operational Security	The supplier SHOULD have a concept covering the access, use and protection of cloud services unless no externally provided IT services are used. ISO 27017 CLD.4.3, CLD.8.1.5, CLD.9.1.1, CLD.9.1.2 and CLD.12.1.3	Partially compliant	3
	The supplier MUST have an awareness program/training for the employees. ISO 27001 A.7.2.1 and A.7.2.2	Partially compliant	3
	The supplier MAY have Information Security certifications (e.g. ISO 27001, TISAX, SOC 2 Type 2)	Partially compliant	3
	The supplier MUST have a backup concept. Backups SHOULD be tested at least annually. ISO 27001 A.12.3.1	Partially compliant	6
Production Security	The supplier MUST have a Business Continuity Management / Disaster Recovery Plan. ISO 27001 A.17.1.1, A.17.1.2, A.17.1.3 and A.17.2.1	Partially compliant	6
	The supplier MUST have implemented measures to protect against scamphishing/fraud emails. ISO 27001 A.12.2.1	Partially compliant	6
	The supplier MUST have implemented 2-Factor-Authentication for all remote access and all cloud services. ISO 27001 A.9.4.2, A.13.1.2 and A.14.1.2	Partially compliant	6
	The supplier MUST have an antivirus solution that is centrally monitored. ISO 27001 A.12.2.1	Partially compliant	6
	The supplier MUST have a patch management concept including regular patch intervals, OS updates and software updates. ISO 27001 A.12.6.1	Partially compliant	6
	The supplier SHOULD have a log management concept. ISO 27001 A.12.4.1, A.12.4.2 and A.12.4.3	Partially compliant	3
	The supplier SHOULD have network segmentation for production systems. ISO 27001 A.13.1.1 and A.13.1.3	Partially compliant	3
	Software development and testing guidelines SHOULD have a software development and testing guideline unless no software is developed. ISO 27001 A.14.2.1	Partially compliant	3
		Compliance Score:	60%

Information security policy

Cloud computing

Version	Date	Who	What
DRAFT	October 2022	Gary Hinson	Template prepared for SecAware

Policy summary

The information risks associated with cloud computing must be properly identified, evaluated and treated, using suitable information security controls.

Applicability

This policy applies throughout the organisation as part of the corporate governance framework. It is particularly relevant to Information Owners who are considering or already using cloud computing. This policy also applies to third party employees working for the organisation whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behaviour) to uphold our information security policies.

Policy detail

Background

Cloud computing presents both risks and opportunities. Cloud computing services provided by commercial organisations (Cloud Service Providers) through the Internet. The services provided range from servers on a large scale to numerous customers represent larger and more complex applications. Information is usually processed and stored remotely, in the cloud, rather than locally within the organisation.

Aside from information risks conventionally associated with IT, cloud computing introduces further risks relating to the supplier relations and cloud technology. Commercial cloud services provided on a large scale to numerous customers represent larger and more complex applications. Information is usually processed and stored remotely, in the cloud, rather than locally within the organisation.

On the other hand, there are several advantages to cloud computing such as reduced costs, specialisation, access to a pool of IT and support resources, geographical diversity and 'access from anywhere'. Cloud computing can also be used as a flexible and suitable option provided the associated information risks are identified and treated appropriately. Failing to do so would be negligent.

Example

Copyright © 2022, Inc1 Ltd.

Supplier Security Explained

Question 5: User Awareness

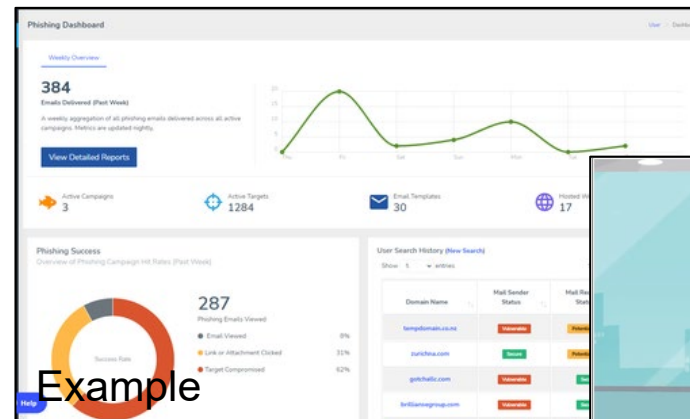
The supplier **MUST** have an awareness program/training for the employees.

Why?

- Cyber attacks and malware shifted towards attacking users instead of servers or services. As a result, users must be trained not to disclose confidential information on the phone or execute suspicious e-mail attachments.

Possible Evidence

- Anti-Phishing Simulation (Screenshot)
- Awareness Trainings (Screenshot)
- Training Schedule and content



Example



Example

Spear Phishing

A personalised phishing attack targeting a specific individual or organisation.

Understand how spear phishing works to protect yourself, your family & your organisation.

Step 1: The Homework
Scammers start by researching their target. Social media is a common place for scammers to discover specific information about you.
Stay Safe Be careful what sensitive information you post on social media (i.e. birthdays, addresses, etc). Configure your privacy settings to limit visible information.

Step 2: The Scam
Scammers send you a personalised email. To make it seem legit, they'll include your name, personal information and even your interests.
Watch Out Remember to scan for S.C.A.M. (see below) before clicking on links or opening attachments sent to you.

Step 3: The Click
If you've clicked on a link, you've likely unwittingly installed malware on your device, or handed scammers your personal details.
Be Vigilant Recognise spear phishing tactics including a sense of urgency, authority or appealing to your curiosity before you click.

Step 4: The Breach
If you've been phished, the repercussions could include time and money to fix the damage, loss of reputation or possible fines.
Protect Yourself! If you receive a phishing email, report the phish to your IT Department at work, or Scamwatch at home.

Don't forget SCAN for S.C.A.M.

SENDER Check for unusual domain names and organisations using free email services.
CONTENT Red flags might include poor spelling, incorrect grammar or a sense of urgency.
MANAGEMENT Hover over links before clicking; check for IP addresses in URLs; don't fill in forms or open suspicious attachments.

Example

Supplier Security Explained

Question 6: Security Certifications

Public

The supplier **MAY** have Information Security certifications (e.g. ISO 27001, TISAX, SOC 2 Type 2)

■ Why?

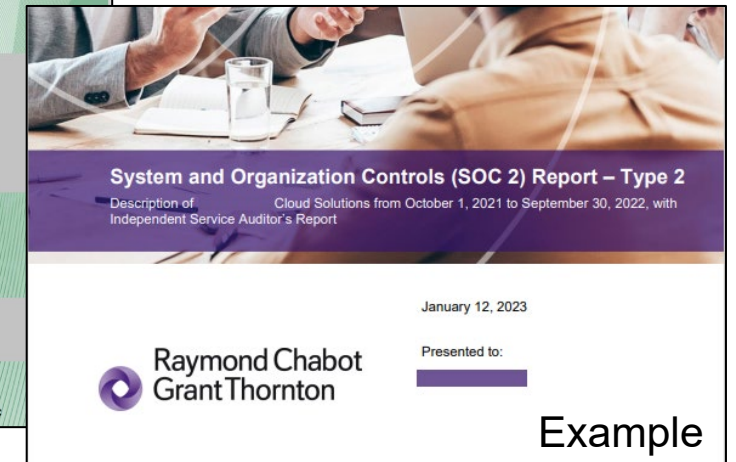
- Security certifications are evidence that an accredited external auditor did review the security measures of the supplier. In general, this includes all of the questions that are part of this questionnaire.

■ Possible Evidence

- TISAX Label (to be shared through ENX**)
- ISO 27001 certificate
- SOC2 Type 2 report (first page & ToC*)



Example



*ToC: Table of Content.

**If the supplier has TISAX Labels, they know what to do. Our Participant ID is PH15Z4.

Supplier Security Explained

Question 7: Backup and Recovery

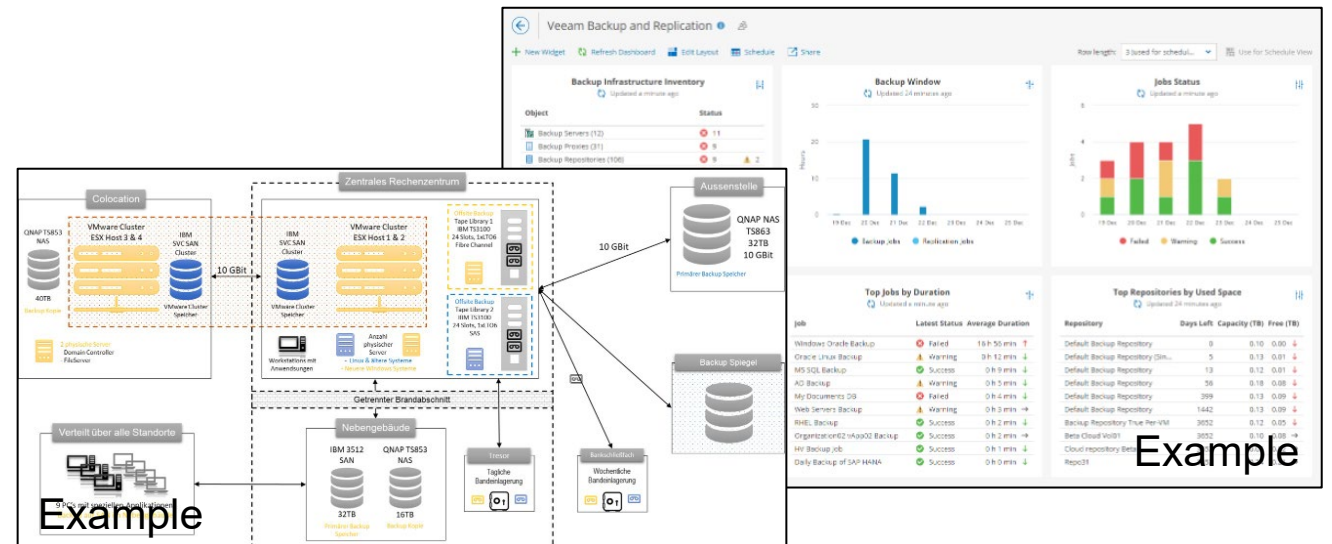
The supplier **MUST** have a backup concept. Backups **SHOULD** be tested at least annually.

Why?

- Most companies cannot produce or provide their services without their IT systems running their data being available. To ensure that data loss is not irreversible, regular backups of data and IT systems are essential.

Possible Evidence

- Backup & Recovery concept
- Backup & Recovery solution (screenshot)
- Recovery test result (excerpt)



Supplier Security Explained

Question 8: Business Continuity

The supplier **MUST** have a Business Continuity Management / Disaster Recovery Plan

Why?

- Being prepared to keep services and production available during incidents, cyber attacks or disasters is the only way to fulfill SLA requirements. To ensure this, relevant incidents must be identified, and countermeasures must be prepared and also tested.

Possible Evidence

- Business Continuity Concept
- Disaster Recovery Plan
- Disaster Recovery Test Protocol (excerpt)

Example

Result	Check	Details
[i] Info	RPO	Target RPO is 24:00:00 (HH:mm:ss)
✓ Success	Target RPO Met	Yes
✓ Success	VMs not meeting RPO	None
✓ Success	Worst RPO failure	None

Result	Check	Details
[i] Info	RTO	Target RTO is 01:00:00 (HH:mm:ss)
[i] Info	Duration	Test duration was 00:04:10 (HH:mm:ss)
✓ Success	Target RTO Met	RTO achieved

Lab Group	Start Time	End Time	Duration
start DataLab Appliance	18:05:19	18:07:28	00:02:09

BUSINESS CONTINUITY PLAN

Background:
This Business Continuity Plan is produced on the [INSERT DATE].

Aim

- The aim of this plan is to provide a reference tool for the actions required during or immediately following during the instance of an emergency or incident that threatens to disrupt normal business activities.
- An emergency and incident are a situation or event that may cause injury, loss of life, destruction of property, or cause the loss of the company's normal business operations to which would pose a threat.
- The plan aims to minimize the effect an emergency or incident may have on members of staff, the company's equipment, or premises and identify actions that may be taken to reduce any risks.

Business critical processes

- This Continuity Plan applies to the following business functions.
- The applied recovery team will utilize the necessary resources to restore and resume functions, in order of the highest priority based on the impact on the business.
- A Higher priority function is used for the restoration of the processes that are deemed to be business critical for the performance of the company and to reach its objectives.
- The following list aims to provide a guide to the Recovery team to restore functionality of the business:

Critical Business Function: [INSERT CRITICAL FUNCTION]

- To initiate the recovery plan for this business function, the function is expected to be interrupted or delayed for [INSERT HOURS].
- Description of function: [INSERT DESCRIPTION].
- Potential threat(s) to this function: [HIGHLIGHT POTENTIAL THREATS].
- Recovery procedures: [HIGHLIGHT RECOVERY PROCEDURE].
- Required resources: [HIGHLIGHT REQUIRED RESOURCES].

High-priority business function: [INSERT HIGH PRIORITY BUSINESS FUNCTION]

- To initiate the recovery plan for this business function, the function is expected to be interrupted or delayed for [INSERT HOURS].
- Description of function: [INSERT DESCRIPTION].
- Potential threat(s) to this function: [HIGHLIGHT POTENTIAL THREATS].
- Recovery procedures: [HIGHLIGHT RECOVERY PROCEDURE].
- Required resources: [HIGHLIGHT REQUIRED RESOURCES].

Medium-priority business function: [INSERT MEDIUM-PRIORITY BUSINESS FUNCTION]

- To initiate the recovery plan for this business function, the function is expected to be interrupted or delayed for [INSERT HOURS].
- Description of function: [INSERT DESCRIPTION].
- Potential threat(s) to this function: [HIGHLIGHT POTENTIAL THREATS].
- Recovery procedures: [HIGHLIGHT RECOVERY PROCEDURE].

Example

Supplier Security Explained

Question 9: Phishing and Fraud Protection

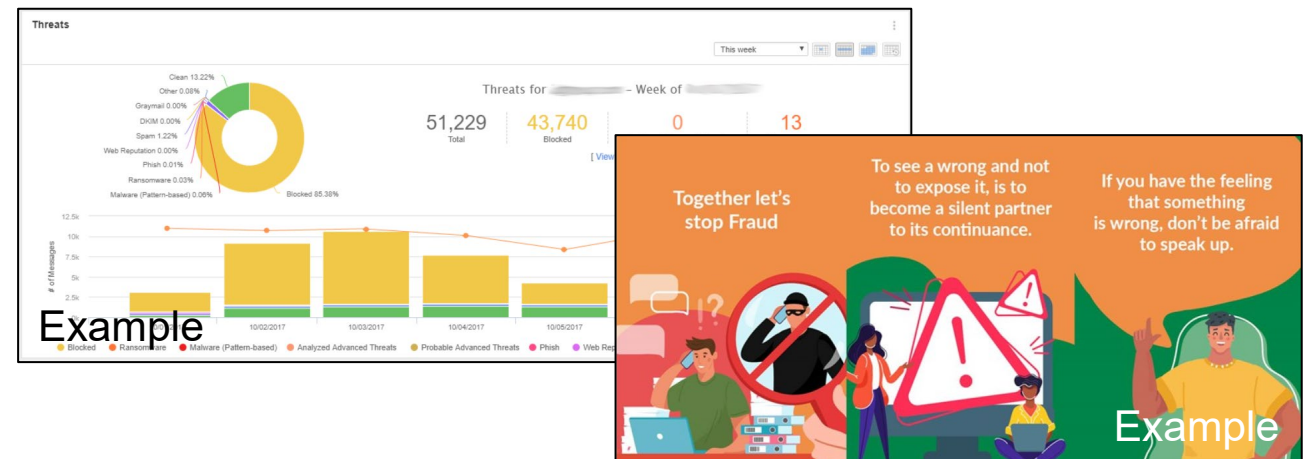
The supplier **MUST** have implemented measures to protect against scam/phishing/fraud e-mails.

■ Why?

- Spam, Scam, Phishing and Fraud e-mails are a growing threat to every company and account to over 90% of all e-mails. Dedicated solutions filter most of the incoming, unwanted e-mails to protect the receiving company.

■ Possible Evidence

- Anti Spam Solution (screenshot)
- Anti Fraud Trainings (screenshot / excerpt)



Supplier Security Explained

Question 10: Multi Factor Authentication (MFA)

The supplier **MUST** have implemented 2-Factor-Authentication for all remote access and all cloud services.

Why?

- User credentials are available for sale in the darknet or can be compromised using Phishing E-Mails or just guessed. The only but very effective solution against this is to require an additional factor like biometrics, an authenticator app or other MFA solutions.

Possible Evidence

- Multi-Factor Solution (screenshot)
- Multi-Factor Concept (document / slides)

The image displays three screenshots related to Multi-Factor Authentication (MFA) in Microsoft Entra ID:

- Left Screenshot:** Shows the 'Info' section of an MFA policy configuration. The 'Name' field contains 'Example: Device compliance app policy'. Under 'Access controls', the 'Grant' option is selected and circled in red. A red circle labeled 'Example' is also around the 'Access controls' section header.
- Middle Screenshot:** Shows the 'Select the controls to be enforced' section. The 'Grant access' radio button is selected and circled in red. The 'Require multi-factor authentication' checkbox is checked and circled in red. A red circle labeled 'Example' is around the 'Require multi-factor authentication' checkbox.
- Right Screenshot:** Shows the 'MULTI-FACTOR AUTHENTICATION VES1' configuration page. It includes a 'MFA events statistics' chart for 'Today' with the following data:

Event Type	Count
MFA successful	1
MFA cancelled	2
MFA failed	0
MFA help request	2
Configuration skipped	0

Below the middle screenshot is a Microsoft notification box titled 'More information required' with the text: 'Your organization needs more information to keep your account secure'. It includes links for 'Use a different account' and 'Learn more'. A 'Next' button is at the bottom right, and a red circle labeled 'Example' is around it.

Supplier Security Explained

Question 11: Anti-Virus Solution

Public

The supplier **MUST** have an antivirus solution that is centrally monitored.

■ Why?

- The only way to detect and prevent an outbreak of malware in the company network and IT systems is a centrally monitored anti-virus solution. EDR or XDR solutions provide more security and visibility, but an anti-virus solution is a mandatory minimum requirement.

■ Possible Evidence

- Anti Virus Solution Agent (screenshot)
- Anti Virus Management Dashboard (screenshot)

The image displays two screenshots related to anti-virus management. The left screenshot shows a management dashboard with a sidebar menu and a main content area. The sidebar includes options like Dashboard, Alerts, Logs & Reports, People, Devices, Global Settings, and Protect Devices. The main content area features a 'Most-Recent Alerts' table with columns for time, description, and severity. Below the alerts is a 'Usage Summary' section with a donut chart for 'Endpoint User Activity Status' showing 472 total users, categorized into 38 Active, 27 Inactive 2+ Weeks, 250 Inactive 2+ Months, and 148 Not Protected. To the right, 'Web Stats' shows 28 Web Threats Blocked and 6 Policy Warnings Issued. The right screenshot shows a Windows Security window with the 'Security providers' section expanded to 'Antivirus'. It lists 'Bitdefender Antivirus' as turned on and 'Microsoft Defender Antivirus' as turned off. Both screenshots have a semi-transparent 'Example' watermark.

Supplier Security Explained

Question 12: Patch Management

The supplier **MUST** have a patch management concept including regular patch intervals, OS updates and software updates.

■ Why?

- Unpatched Software has vulnerabilities that can be exploited by attackers. Not all updates can be applied immediately, and downtimes must be scheduled, but a Patch Management Concept enables a company to ensure availability and security of their IT systems.

■ Possible Evidence

- Patch Management Concept (excerpt)
- Patch Management Solution (screenshot)

Server Patch Management Process

1. Scope
This policy applies to all the Company's information systems and resources, whether they are owned or operated by the university or on its behalf. This policy must be followed by all Company-Related Persons who have access to company information or computers and systems that are managed or maintained on behalf of the organization.

2. Responsibilities

- Chief Information Officer: Examine and accept any modifications to the patch management procedure.
- Information security Analysts: Alert the technical staff on campus when new patches are available. Organize with the campus the review of new patches.
 - At the campus Change Management meetings, talk about patch releases.
 - upkeep of the vulnerability scanning tool; regular scanning of crucial systems for known flaws.
 - With the campus patch testing team and the patch server administrator, organize a review of new patches.

Server Patch Management Process

Types	Patch
Server	BIOS, firmware
Operating System	Service packs, patches, feature packs
Router and Switches	Firmware
Scanners	Driver, firmware

5. Patch Management Checklist

Server Name	Remediation Plan	Patching status	Operating system
Win2k12r	None	In process	Windows 10
Apexure	None	Completed	Windows 10
Aristo media	None	Not started	Windows 10
Fusion host	None	Pending	Windows 10

6. Penetration Testing

- Penetration testing of the internal network, external network, and hosted applications should be done at least once a year or if the environment changes significantly.
- Any exploitable vulnerabilities discovered during a penetration test will be fixed and retested to ensure they were fixed.

Patch Management Workflow

Policy	Severity	Classification	Patch	Product	Vendor	Release Date	Missing	Install...	Unins...
●	Important	Other Vendor	Wireshark (x64) 4.0.3	Wireshark	Wireshark	18-Jan-2023	1	0	Yes
●	Moderate	Other Vendor	Seven-Zip (x64) 19.0	7-Zip	7-Zip	-	4	0	Yes
●	Moderate	Other Vendor	Notepad ++ (x64) 8.4.8	Notepad ++	Notepad++	25-Dec-2022	1	0	Yes
●	-	Other Vendor	2021-06 Cumulative Update for .NET Framework 3.5, 4.7.2 an	Windows Server ...	Microsoft	-	1	0	Yes
●	-	Other Vendor	Security Intelligence Update for Microsoft Defender Antivirus	Microsoft Defend...	Microsoft	-	1	0	No
●	-	Updates	2022-02 Cumulative Update Preview for .NET Framework 3.5,	Windows Server ...	Microsoft	-	1	0	Yes
●	-	Other Vendor	Security Intelligence Update for Microsoft Defender Antivirus	Microsoft Defend...	Microsoft	-	1	0	No
●	-	Definition Updates	Security Intelligence Update for Microsoft Defender Antivirus	Microsoft Defend...	Microsoft	-	1	0	No
●	-	Definition Updates	Security Intelligence Update for Microsoft Defender Antivirus	Microsoft Defend...	Microsoft	-	1	0	No
●	-	Update Rollups	Windows Malicious Software Removal Tool x64 - v5.109 (KB8	Windows 11(Win...	Microsoft	31-Dec-2022	1	0	No
●	-	Other Vendor	2023-01 Cumulative Update Preview for .NET Framework 3.5, 4.8 and 4.8.1 for Wi...	Windows 11	Microsoft	10-Jan-2023	1	2	Yes
●	-	Other Vendor	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version...	Microsoft Defend...	Microsoft	19-Jan-2023	1	0	Yes
●	-	Other Vendor	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version...	Microsoft Defend...	Microsoft	-	1	0	No

Example

Example

Supplier Security Explained

Question 13: Log Management

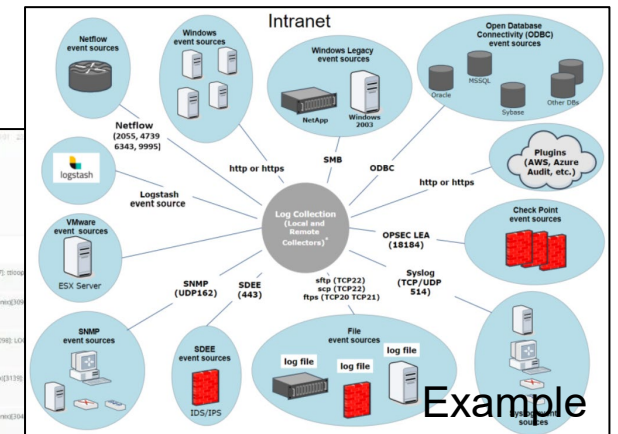
The supplier **SHOULD** have a log management concept.

Why?

- Most servers, applications, services and appliances create logs that can be used to prevent or solve problems and to ensure availability of production and services. However, those logs can only be used effectively, if they are collected and monitored in a controlled way.

Possible Evidence

- Log Management Concept (excerpt)
- Log Management Solution (screenshot)



Supplier Security Explained

Question 14: Production – Network Segmentation

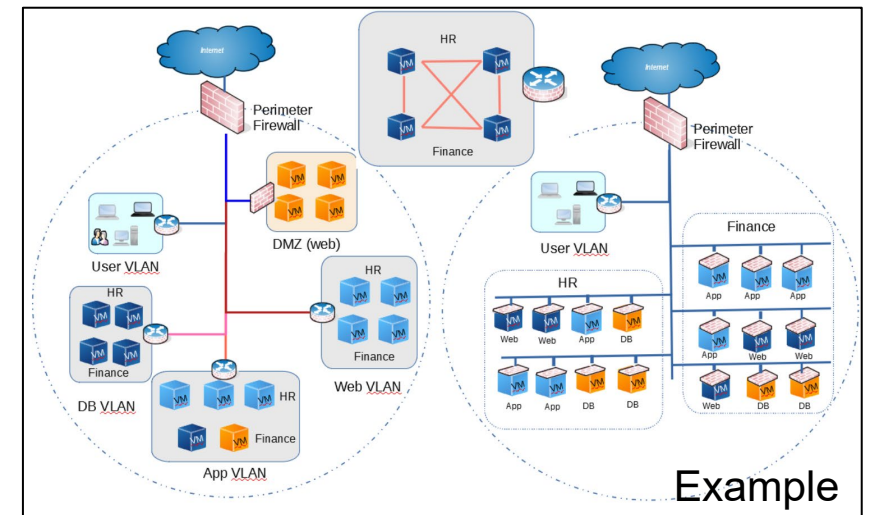
The supplier **SHOULD** have network segmentation for production systems.

■ Why?

- Network segmentation limits the spreading of malware in computer networks and reduced effects of misconfigurations. Especially in production environments or for legacy systems, network segmentation might be the only way to isolate and protect vulnerable systems.

■ Possible Evidence

- Network Blueprint (excerpt)
- VLAN List and Description



Supplier Security Explained

Question 15: Software Development

The supplier **SHOULD** have a software development and testing guideline unless no software is developed.

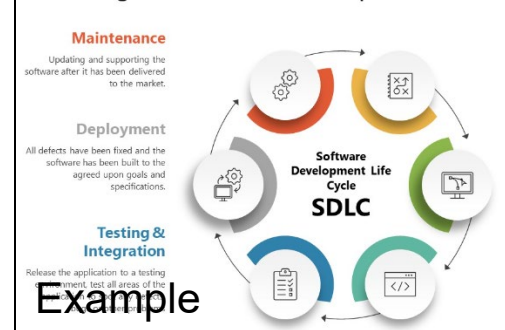
Why?

- A software development guideline including software lifecycle management and software testing will greatly reduce the probability of bugs or misconfigurations. This is true for classical and agile software development concepts.

Possible Evidence

- Software development guideline (excerpt)
- Software testing guideline (excerpt)
- Software lifecycle management concept

SDLC Diagram PowerPoint Template



1. Functional Test Plan Scope	
In Scope	Out of Scope
In Scope List functions that are tested.	Out of Scope List functions that are not tested.

2. Functional Test Plan Assumptions and Constraints	
Functional Test Plan Assumptions	
Assumption List the functional test plan assumptions.	
Functional Test Plan Constraints	
Constraint List the functional test plan constraints.	

3. Functional Test Team Roles & Responsibilities		
Name	Roles	Responsibilities
Name List names of people involved in functional testing.		
Name List names of people involved in functional testing.		

4. Functional Test Entry Criteria	
ID	Criteria
4.1	Entry Criteria Factors that must be present to enable the start of the functional test. Example: environment state is available.

5. Functional Test Cases	
ID	Test Cases
5.1	Test Case Identify the test cases along with the expected results. Example: Login with a corporate user account.

2. Internal Documentation Standards

If done correctly, internal documentation improves the readability of a software module. Many of the general software development guidelines are focused on using good internal documentation practices. The SISPEG has agreed that a file containing one or more software modules or a shell script file should have a comment block at its beginning containing the following basic information:

- The name of the author who created the file
- The date the file was created
- The author's development group (e.g. HSEB, HSMB)
- Description (overview of the purpose of the modules)

Note that a module is a method, function, or subroutine.

Each module contained within the source file should be preceded by a block of comments showing the following:

- The name of the module
- The name of the original author (if the module author is different than the author of the file.)
- The date the module was created
- A description of what the module does
- A list of the calling arguments, their types, and brief explanations of what they do
- A list of required files and/or database tables needed by the routine, indicating if the routine expects the database or files to be already opened
- All of the non system routines called by this module (optional)
- Return values
- Error codes/exceptions
- Operating System (OS) specific assumptions, e.g. this routine expects binary files to be Little Endian or this routine uses OS specific language extensions. (optional)
- A list of locally defined variables, their types, and how they are used. (optional)
- Modification history indicating who made modifications, when the mods were made, and what was done. (optional, if the modification history is being logged using CM software).

Appendix A of this document contains internal documentation templates. Appendix B contains an example of software modules which use these internal documentation standards.

3. Coding Standards

General coding standards pertain to how the developer writes code. The SISPEG has come up with a small set of items it feels should be followed in regards to programming language being used.

Example