Public

Information Security
Supplier Security Questionnaire

Webasto Group, November 2023

Public

Public Part

The following slides can be shared with suppliers.

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

Supplier Security Explained
Motivation

Public

- **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

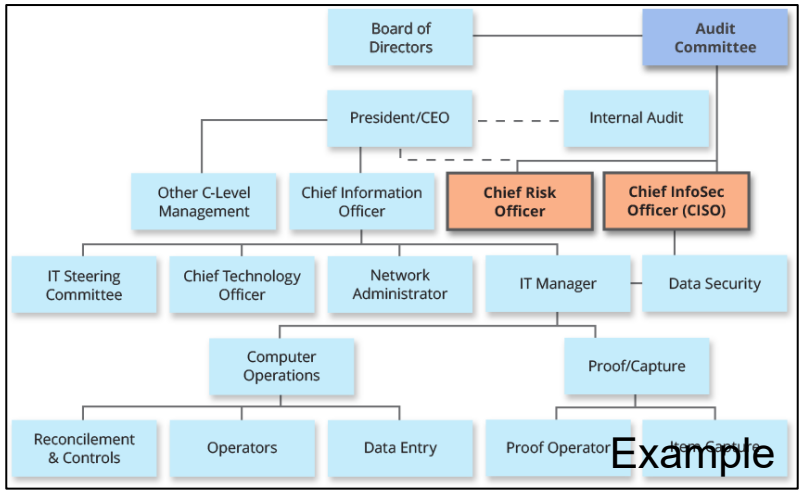
Dear

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 re
communicated to employees and contractors

Example



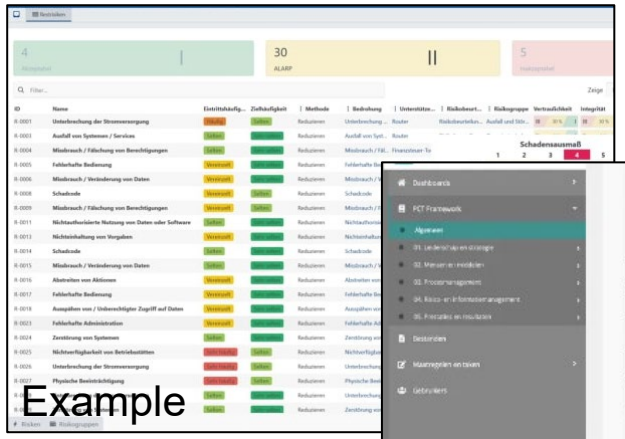
Example

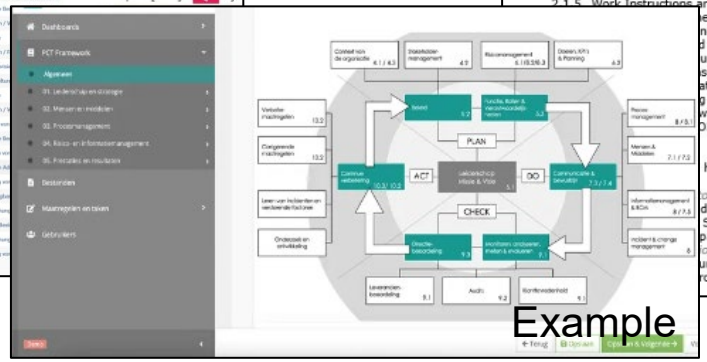
Supplier Security Explained
Question 2: ISMS

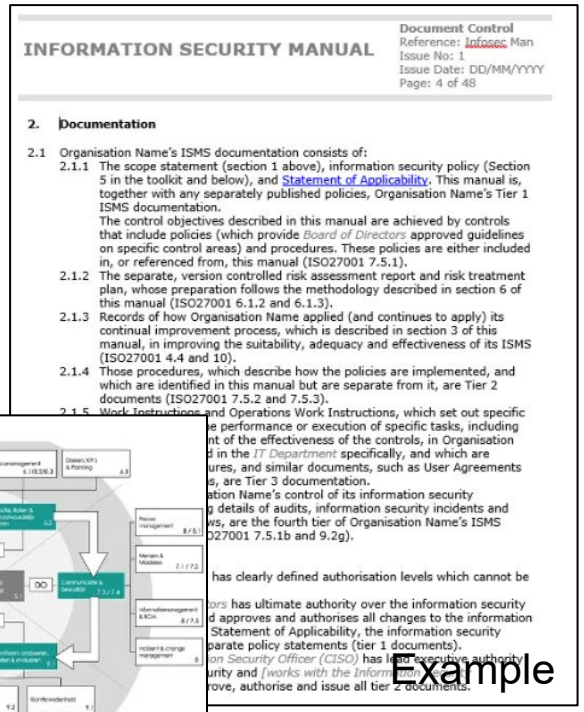
Public

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


Example


Example


INFORMATION SECURITY MANUAL

Document Control
Reference: Infosec Man
Issue No: 1
Issue Date: DD/MM/YYYY
Page: 4 of 48

2. Documentation

2.1 Organisation Name's ISMS documentation consists of:

2.1.1 The scope statement (section 1 above), information security policy (Section 5 in the toolkit and below), and Statement of Applicability. This manual is, together with any separately published policies, Organisation Name's Tier 1 ISMS documentation.
The control objectives described in this manual are achieved by controls that include policies (which provide *Board of Directors* approved guidelines on specific control areas) and procedures. These policies are either included in, or referenced from, this manual (ISO27001 7.5.1).

2.1.2 The separate, version controlled risk assessment report and risk treatment plan, whose preparation follows the methodology described in section 6 of this manual (ISO27001 6.1.2 and 6.1.3).

2.1.3 Records of how Organisation Name applied (and continues to apply) its continual improvement process, which is described in section 3 of this manual, in improving the suitability, adequacy and effectiveness of its ISMS (ISO27001 4.4 and 10).

2.1.4 Those procedures, which describe how the policies are implemented, and which are identified in this manual but are separate from it, are Tier 2 documents (ISO27001 7.5.2 and 7.5.3).

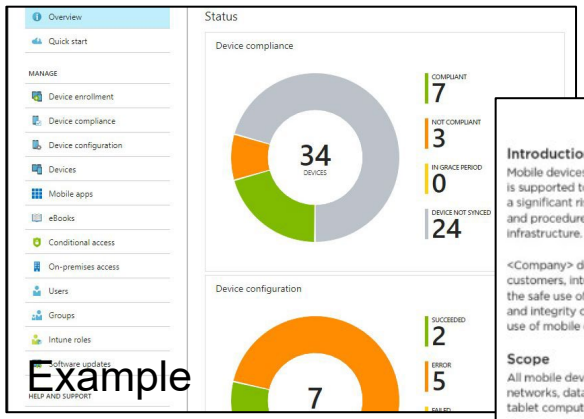
Example

Supplier Security Explained
Question 3: Mobile Devices

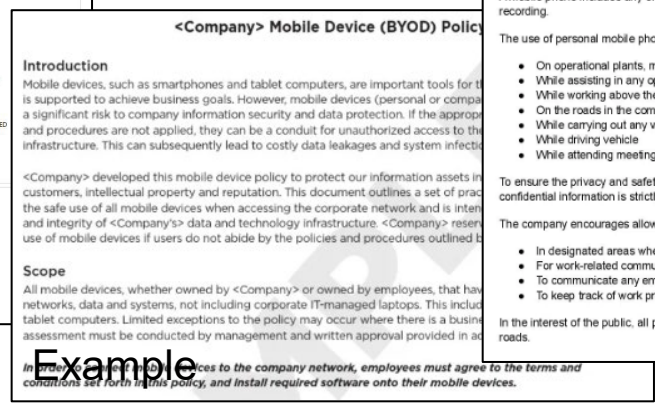
Public

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

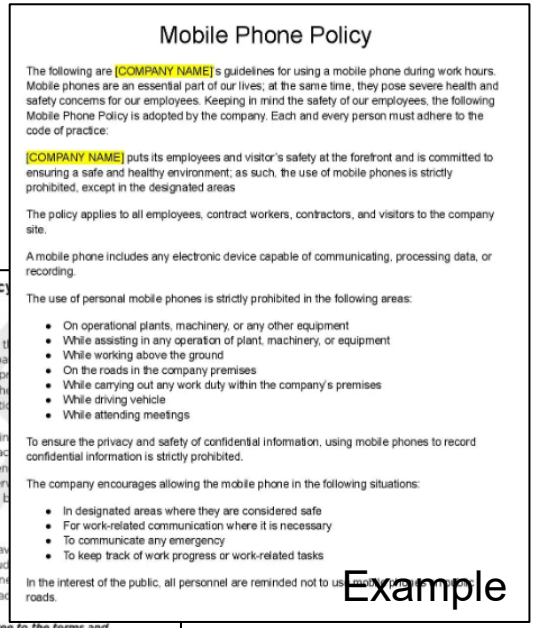
- **Why?**
  - Mobile devices are part of every companies IT, but small, portable devices can be stolen or lost and concepts like Bring your Own Device (BYOD) or its flavors add additional complexity and risks.
- **Possible Evidence**
  - Mobile Device Policy
  - BYOD concept
  - MDM* Suite (Screenshot)



Example



Example



Example

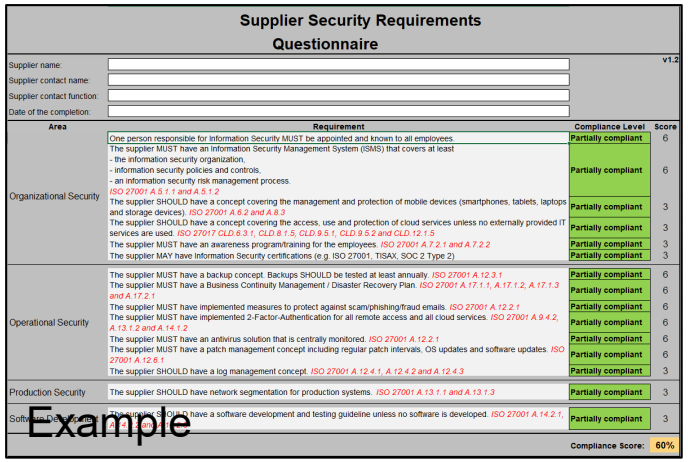
*MDM: Mobile Device Management

Supplier Security Explained
Question 4: Cloud Policy

Public

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



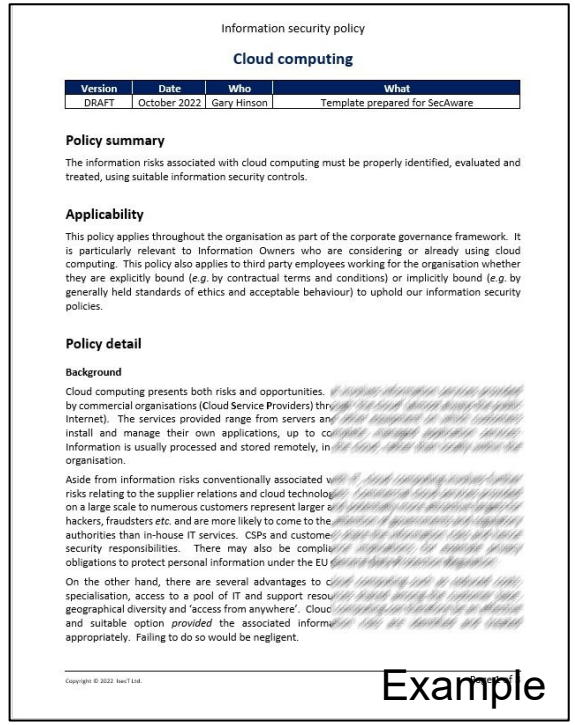
Supplier Security Requirements Questionnaire

v1.2

Supplier name:	
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 - the information security organization, - information security policies and controls, - an information security risk management process. *ISO 27001 A.5.1.1 and A.5.1.2*	Partially compliant	6
	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.8.3*	Partially compliant	3
	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.6.3.1, CLD.8.1.5, CLD.9.5.1, CLD.9.5.2 and CLD.12.1.5*	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
Operational Security	The supplier MUST have a backup concept. Backups SHOULD be tested at least annually. *ISO 27001 A.12.3.1*	Partially compliant	6
	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 scam/phishing/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
Production Security	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	The supplier 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%

Example



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.

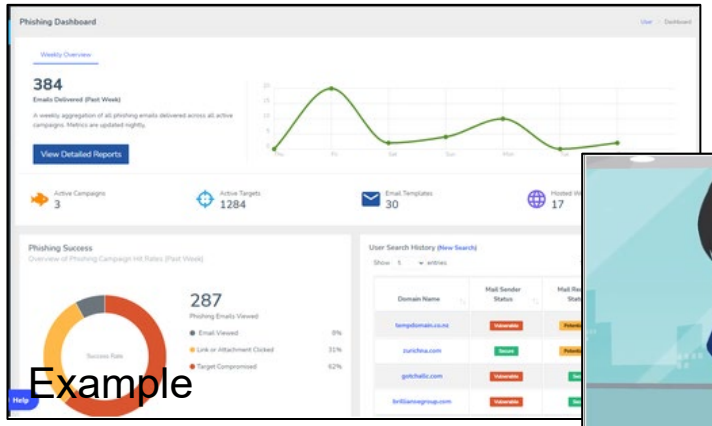
Example

Supplier Security Explained
Question 5: User Awareness

Public

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

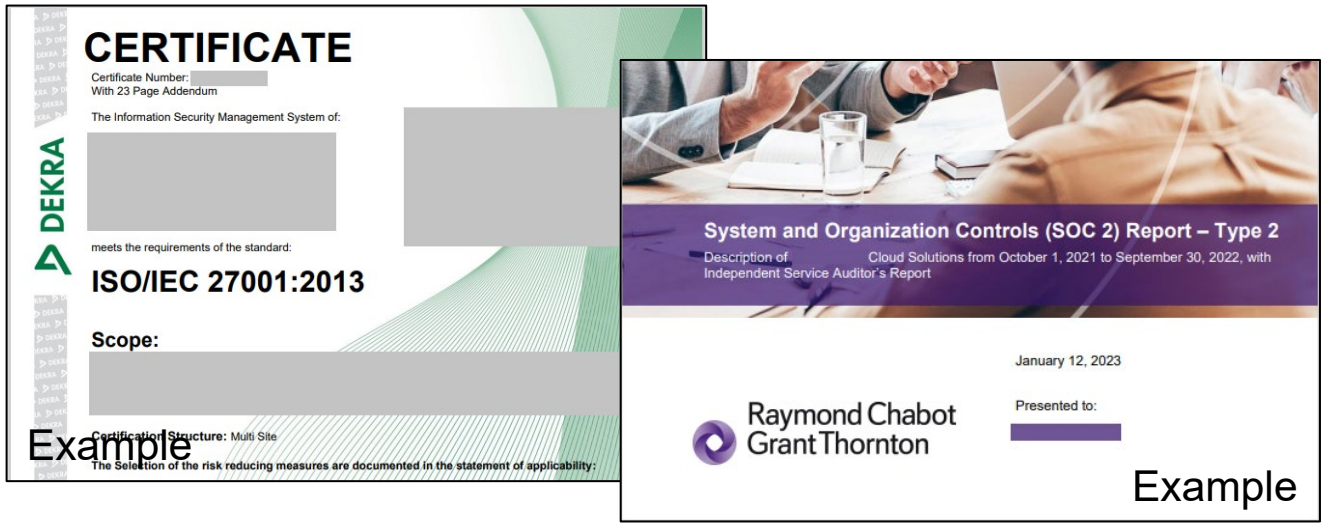


Supplier Security Explained
Question 6: Security Certifications

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*)



*ToC: Table of Content.
**If the supplier has TISAX Labels, they know what to do. Our Participant ID is PH15Z4.

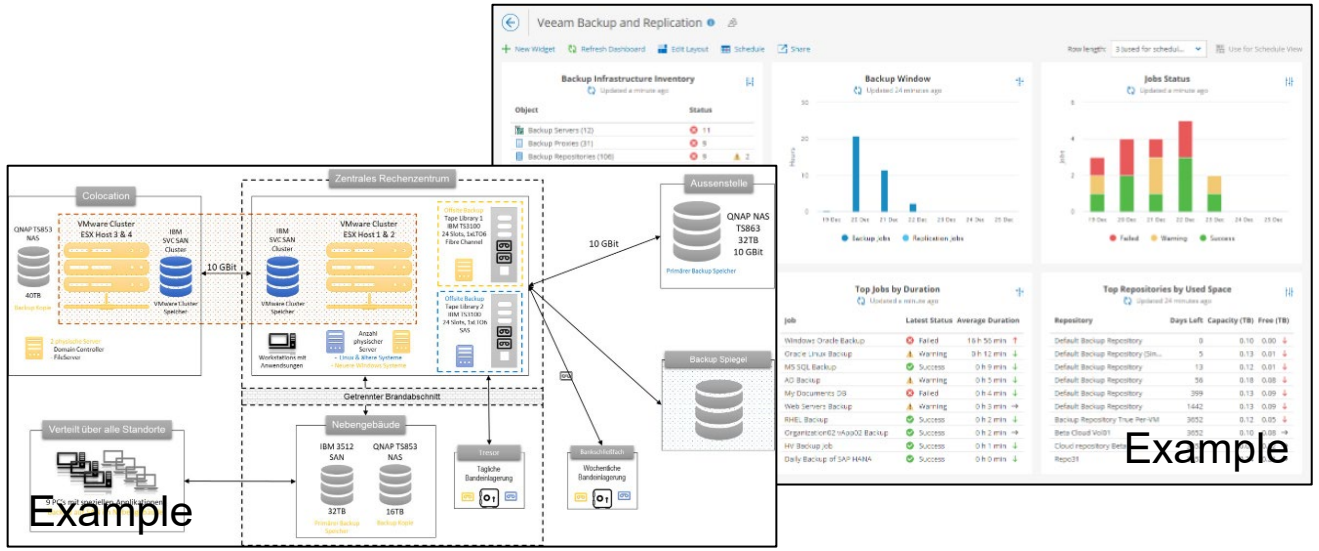
Supplier Security Explained

Question 7: Backup and Recovery

Public

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)



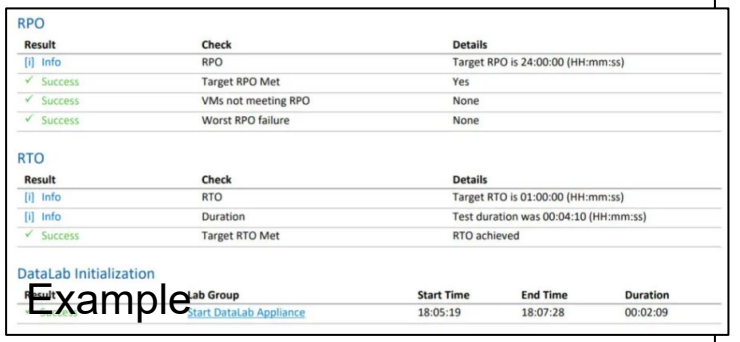
Supplier Security Explained

Question 8: Business Continuity

Public

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. Tho 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)



RPO

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

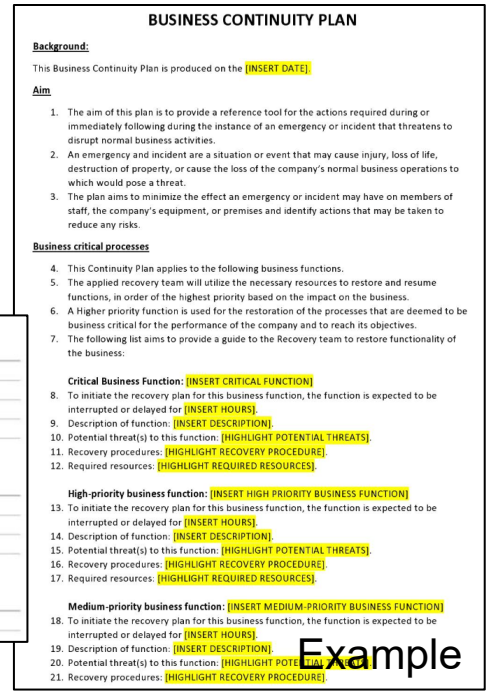
RTO

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

DataLab Initialization

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

Example



BUSINESS CONTINUITY PLAN

Background:

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

Aim

1. 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.
2. 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.
3. 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

4. This Continuity Plan applies to the following business functions.
5. 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.
6. 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.
7. The following list aims to provide a guide to the Recovery team to restore functionality of the business:

Critical Business Function: [INSERT CRITICAL FUNCTION]

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

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

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

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

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

Example

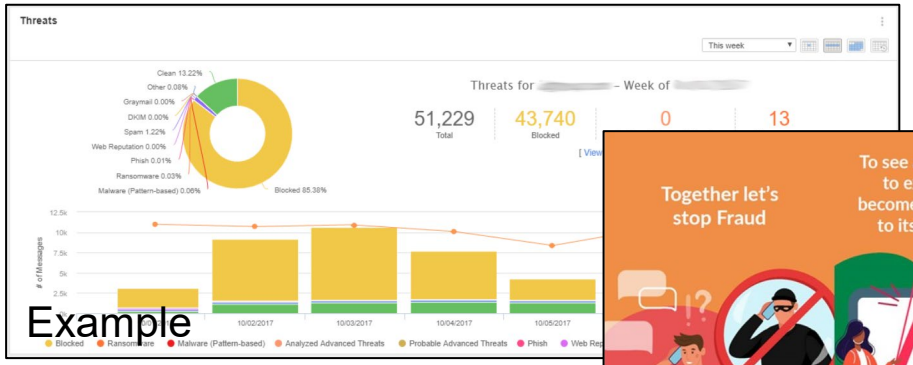
Supplier Security Explained

Question 9: Phishing and Fraud Protection

Public

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)



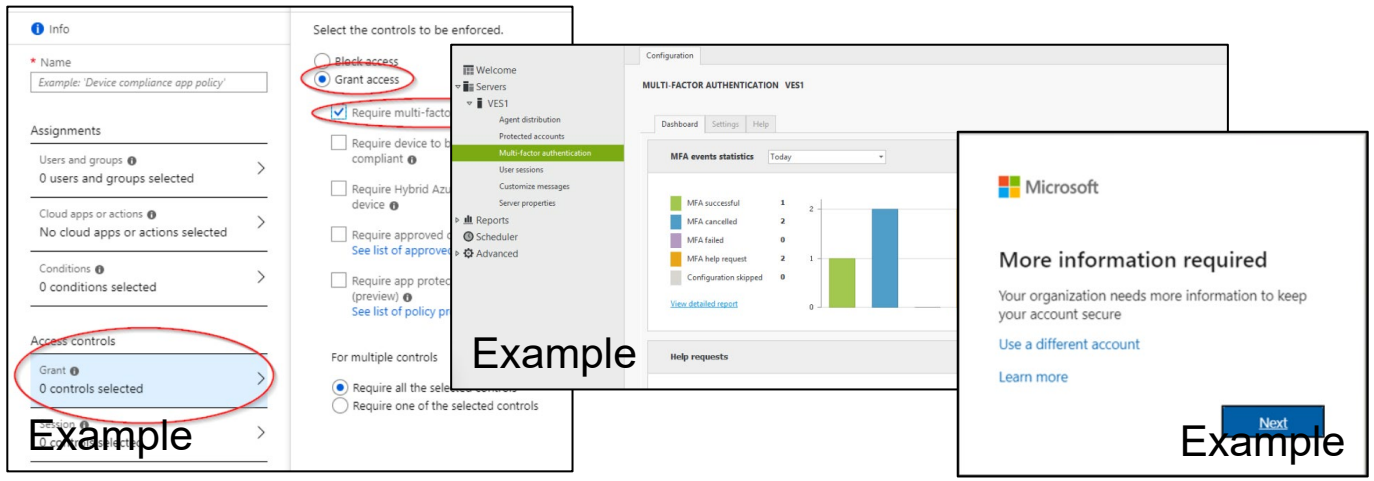
Supplier Security Explained

Question 10: Multi Factor Authentication (MFA)

Public

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)

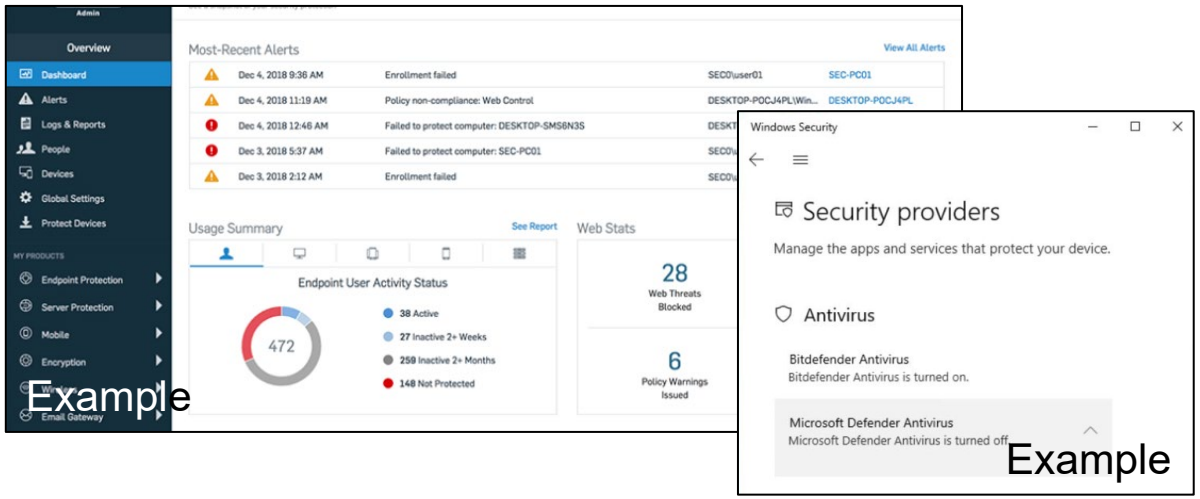


Supplier Security Explained
Question 11: Anti-Virus Solution

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)

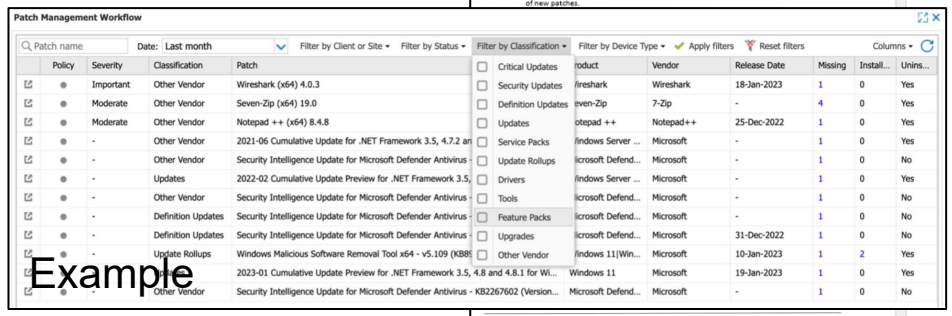


Supplier Security Explained
Question 12: Patch Management

Public

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)

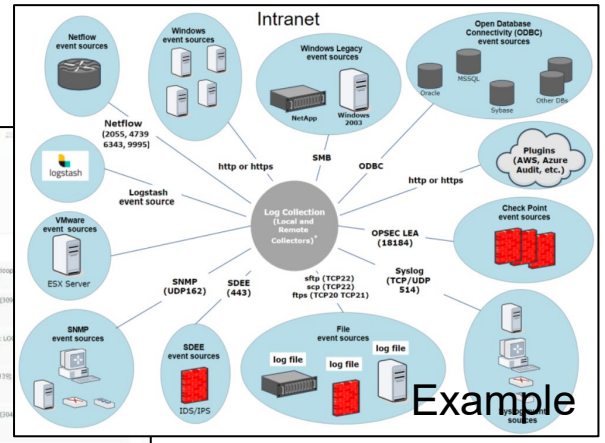


Supplier Security Explained
Question 13: Log Management

Public

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)



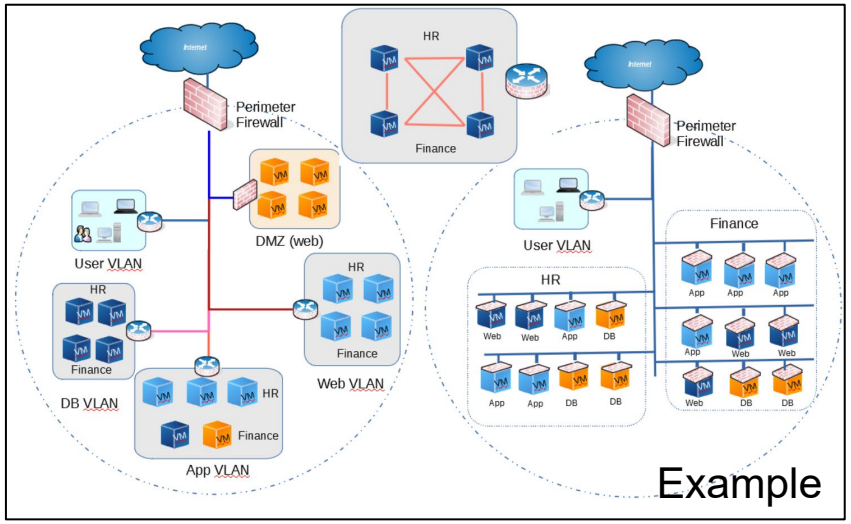
Supplier Security Explained

Question 14: Production – Network Segmentation

Public

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

Public

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