ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Informatik
& Security

fh
st.pölten

Audit Report

MCR – SS 2023 – Security Auditing

Andone Alexandru (is220021)
Flita-Vasile Adrian (cr221504)
German Maria-Alexia (is230002)
Grigoras Ana-Maria (is220013)
Nema Alexandru David (is220017)
Zota Ana-Maria (is220020)
Lecturer: Jakub Pasikowski
Date: 10. Mai 2023

Table of Contents

1. Document Information 3

2. Audit Scope 4

3. Audit Time Frame 4

4. Executive Summary 5

5. Summary of Findings/Mitigation Priority 6

5.1 High Findings (Non-conformities) 6

5.2 Medium Findings (Deviations) 7

5.3 Low Findings 7

6. Audit Findings 8

7. Conclusion 16

8. Appendix 18

8.1 Risk Assessment Matrix 18

8.2 Prioritization (Risk based approach) 19

1. Document Information

Document Information	
Company:	ABC Audit GmbH
Document title:	Audit Report
Version:	V 1.0
Date:	14.05.2023
Auditors	Andone Alexandru, Flita-Vasile Adrian, German Maria-Alexia, Grigoras Ana-Maria, Nema Alexandru David, Zota Ana-Maria
Reviewed by:	
Approved by:	
Classification:	Confidential

Recipients/Auditee		
Name	**Title**	**Department**
Philipp Reisinger	CISO	Management Board
Jakub Pasikowski	IT Director	Corporate IT

Quality Assurance				
	Date	**Name**	**Title**	**Done**
Issue	12.05.2023	Flita-Vasile Adrian Nema Alexandru David	Auditor	X
Review	13.05.2023	Andone Alexandru German Maria-Alexia	Auditor	X
Approved	14.05.2023	Grigoras Ana-Maria Zota Ana-Maria	Auditor	X

History of Document			
Version	Name	Name	Description
V 1.0	25.03.2021	Audit Report	Final Document

2. Audit Scope

In light of recent security incidents, ACME Corp is looking to enhance its organization-wide information security and is contemplating obtaining ISO 27001 certification. The authors of this report conducted a comprehensive mock audit to assess the current status of their information security and determine the steps required for certification readiness. The audit report examines the compliance of ACME Corp with ISO 27002 and the CIS CSC Controls.

Specifically, the following domains have been audited:

- ISO/IEC 27001:2013 Riskmanagement
- ISO/IEC 27002:2022 8.23-8.34
- CSC Top 18 Topic 3,1

An interview-based approach was utilized as the chosen method for conducting the audit.

The primary emphasis of this audit is on ACME Corp's primary location situated in Innsbruck, Austria.

On 14.05.2023, a concluding meeting was held with ACME Corp's accountable management, including Philipp Reisinger, the CISO, and Jakub Pasikowski, the IT Director.

3. Audit Time Frame

Date	**Time** Beginning/ End	**Processes to be audited/ Necessary resources**	**Participant/ Department** Name/Position
13.04.	9:00 - 9:30	Opening Meeting	Management department
13.04.	10:00 - 11:00	Surveillance Audit 1: Kickoff	C-level board / CISO meeting
13.04.	11:30 - 12:30	Implementation of audit checklist	IT department
13.04.	12:30 - 13:15	Lunch Break	All

13.04.	13:15 - 14:15	Implementation of audit checklist and vulnerability scanning tools	Networking department
14.04.	10:00 - 12:00	Implementation of audit checklist	Application development teams
14.04.	12:15 - 13:00	Q&A	General Staff
15.04.	9:00 - 12:00	Penetration Testing	System Administrators
15.04.	12:30 - 13:00	Internal Audit and results (Final Audit Report)	Auditors
15.04.	13:30 - 14:00	Closing Meeting	All

4. Executive Summary

After conducting the audit at ACME Corp. in Innsbruck (Austria), the External Audit team has reported a total of **8** observations. Among these observations, **3** are considered high-risk findings (non-conformities) from the External Audit's perspective, which are deemed critical to the business and could potentially block the ISO 27001 certification process. Even though these non-conformities do not hinder the organization's continuous operations, they should be treated as top priorities by the management and resolved promptly to ensure ISO certification. However, all identified observations require an appropriate and timely response from management to ensure the proper functioning of daily operational tasks at ACME Corp.

Finding ID	Description
8.25	No rule abot code scans within the company.
8.34	No verification of the security settings on employees' personal devices.
CSC 3	If the device is not encrypted with bitlocker find a solution in order to wipe the data not only if the device receives an internet connection.

Final Audit impression:
Following the audit conducted at ACME Corp. in Innsbruck (Austria), the External Audit team has identified 3 non-conformities that require immediate attention from the management.

- Firstly, there is no established rule about code scans within the company, which could potentially leave the company's systems vulnerable to cyberattacks.
- Secondly, there is no verification process in place to ensure that the security settings on employees‘ personal devices are properly configured, creating a security risk for the organization.
- Finally, if a device is not encrypted with BitLocker, there is currently no solution to wipe the data if the device receives an internet connection.

ACME Corp. has an incomplete Information Security Management System (ISMS), and this report outlines all necessary steps for achieving the expected ISMS implementation. It is crucial that the identified non-conformities are immediately addressed, and mitigation actions are defined and assigned to the relevant personnel for prompt execution. Based on the observations made during the audit, the Audit team has determined that ACME Corp. does not meet the fundamental requirements specified by ISO 27001. Therefore, the organization is not yet considered ready for certification against this standard.

5. Summary of Findings/Mitigation Priority

Overall, the majority of the identified observations pertain to the absence of standardization and insufficient implementation of best practices. The tables below provide a concise summary of the observations made during the audit.

5.1 High Findings (Non-conformities)

Ref. ID	Finding	Mitigation Time
8.25	No rule abot code scans within the company.	Within 1 week
8.34	No verification of the security settings on employees' personal devices.	
CSC 3	If the device is not encrypted with bitlocker find a solution in order to wipe the data not only if the device receives an internet connection.	

5.2 Medium Findings (Deviations)

Ref. ID	Finding	Mitigation Time
8.23	No web filtering is implemented while working remotely	Within 1 month
8.25	No training for security coding is held	
8.28	No licenses for external libraries.	

5.3 Low Findings

Ref. ID	Finding	Mitigation Time
8.23	The awareness training is not mandatory	Within 3 months
CSC 1	No procedure is established in case of a piece of equipment is out of date or sold.	

6. Audit Findings

<table>
<tr><td>8.25</td><td colspan="3">Secure development life cycle</td></tr>
<tr><td colspan="4">Observation:

No rule abot code scans has ever beem established within the company.</td></tr>
<tr><td colspan="3">Risk (High):

Without a defined protocol for conducting regular code scans, the company is vulnerable to a range of cybersecurity threats, including malware, viruses, and other malicious code that could be present in its systems. This risk is compounded by the fact that these threats are constantly evolving and becoming more sophisticated, making it imperative for organizations to maintain a proactive and vigilant approach to information security.</td><td>Priority: 1</td></tr>
<tr><td colspan="4">Recommendation:

This protocol should include the frequency of scans, the scope of systems to be scanned, and the appropriate measures to be taken in response to identified vulnerabilities or threats. Additionally, the company should ensure that all relevant stakeholders are trained on the importance of code scans and are provided with the necessary tools and resources to implement the protocol effectively.</td></tr>
<tr><td rowspan="2">Management Response:</td><td>Fully agreed</td><td>Partially agreed</td><td>Disagreed</td></tr>
<tr><td>X</td><td></td><td></td></tr>
</table>

8.34	Protection of information systems during audit testing

Observation:
No verification of the security settings on employees' personal devices has ever been established.

Risk (High):	**Priority: 1**
Without proper security settings, personal devices used for work purposes can become an entry point for cyber attackers to gain unauthorized access to the company's data and systems. Such access can result in data breaches, theft of intellectual property, and other malicious activities that can have serious financial, legal, and reputational consequences for the organization.	

Recommendation:
Addressing the risk associated with the lack of verification of security settings on employees' personal devices is to establish a clear policy for verifying and enforcing security settings on all personal devices used for work purposes. This policy should include guidelines for device security, such as requiring devices to be encrypted, having up-to-date anti-virus software installed, and having strong passwords. The policy should also include guidelines for accessing the company's data and systems from personal devices, including remote access protocols, use of virtual private networks (VPNs), and authentication requirements.

Management Response:	**Fully agreed**	**Partially agreed**	**Disagreed**
	X		

CSC 3	Data protection

Observation:
If the device is not encrypted with bitlocker find a solution in order to wipe the data not only if the device receives an internet connection.

Risk (High):	**Priority: 1**
This presents a significant risk of data breaches and intellectual property theft, which can have severe financial and reputational consequences for the organization. Additionally, if the device does not receive an internet connection, the data wiping solution may not be effective, leaving the data vulnerable to unauthorized access. Therefore, it is crucial for organizations to have strong policies and procedures in place to ensure that all devices used for work purposes are encrypted and have an effective solution to wipe data in case of loss or theft, regardless of internet connectivity. Failing to do so can expose the organization to significant risks and potential harm.	

Recommendation:

1. Establish a policy requiring all devices used for work purposes to be encrypted with BitLocker or an equivalent encryption solution.
2. Implement a solution to remotely wipe data from all devices used for work purposes, even if they are not connected to the internet. This can be achieved through the use of a Mobile Device Management (MDM) solution or other remote management tool.
3. Ensure that all employees are trained on the proper use and maintenance of their work devices, including the importance of encryption and the risks associated with not having an effective solution to wipe data.

Management Response:	**Fully agreed**	**Partially agreed**	**Disagreed**
	X		

8.23	Web filtering
Observation: No web filtering has ever been implemented while working remotely	
Risk (Medium): Increased risk of malware and other cyber threats: Without web filtering, employees working remotely are more susceptible to malicious websites and phishing attacks, which can result in malware infections and other cyber threats. Data leakage: The absence of web filtering increases the risk of data leakage due to employees accessing websites and online services that are not secure or authorized by the company. Reduced productivity: Employees working remotely may be distracted by non-work-related websites, which can result in reduced productivity and potential loss of business. Compliance violations: Failure to implement web filtering may result in compliance violations and the company may be held liable for any legal or financial consequences.	**Priority: 2**
Recommendation: Implement a web filtering solution: ACME Corp. should implement a web filtering solution to monitor and filter internet traffic for remote employees. This solution should be able to block access to websites that are not authorized by the company or that pose a potential security risk. Define a web filtering policy: ACME Corp. should define a clear policy that outlines the types of websites that are allowed and prohibited for remote employees. This policy should be communicated to all employees and enforced through regular monitoring and audits. Provide training: ACME Corp. should provide training to employees on the importance of web filtering and how to use the web filtering solution effectively. This training should also include best practices for safe web browsing while working remotely.	

Management Response:	**Fully agreed**	**Partially agreed**	**Disagreed**
	X		

8.25	Secure development life cycle
Observation: A training about secure coding has never been held within the company.	
Risk (Medium): The lack of training for security coding as a high-risk finding, as it increases the likelihood of security vulnerabilities in the software developed by ACME Corp. Employees who are not trained in secure coding practices may unknowingly introduce vulnerabilities in the code, which could be exploited by attackers to gain unauthorized access to the organization's systems and data. Furthermore, the lack of training could result in employees not understanding the importance of secure coding practices, which could lead to a culture of complacency towards information security within the organization. This could ultimately result in reputational damage and financial losses for ACME Corp.	**Priority: 2**
Recommendation: Implement a training program for security coding to raise awareness and improve the knowledge of employees regarding secure coding practices. The training program should cover the basics of secure coding, such as code analysis, input validation, and authentication, as well as specific programming languages and frameworks used in the organization. The training should be mandatory for all employees involved in software development and should be regularly updated to reflect new security threats and vulnerabilities. Additionally, ACME Corp. should consider providing incentives for employees who complete the training and demonstrate good security coding practices.	

Management Response:	**Fully agreed**	**Partially agreed**	**Disagreed**
		X	

<table>
<tr><td>8.28</td><td colspan="3">Secure coding</td></tr>
<tr><td colspan="4">Observation:
There is no license for external libraries purchased.</td></tr>
<tr><td colspan="3">Risk (Medium):
I would consider the lack of licenses for external libraries as a high-risk finding. The use of external libraries without proper licensing could result in legal and financial liabilities for ACME Corp. If the organization is found to be using unlicensed software, it could face legal action and financial penalties. Additionally, the use of unlicensed software may result in security vulnerabilities, as the organization may not receive updates and patches for the software. Attackers may be able to exploit these vulnerabilities to gain unauthorized access to ACME Corp's systems and data. Therefore, it is critical for the organization to ensure that all external libraries used in its software are properly licensed.</td><td>Priority: 2</td></tr>
<tr><td colspan="4">Recommendation:
Immediately establish a process for managing external libraries and ensuring that all external libraries used in the company's software are properly licensed. This can include conducting a thorough inventory of all external libraries currently in use, reviewing license agreements, and ensuring that appropriate documentation is in place. The organization should establish a policy that requires developers to obtain approval from the appropriate department before integrating any external libraries into the software. The policy should specify the process for obtaining and reviewing license agreements for the external libraries, and ensuring that all licenses are valid and up to date. Additionally, the organization should establish a process for monitoring and tracking the use of external libraries to ensure that all licenses are properly managed and renewed on time. This will help to prevent any legal or financial liabilities resulting from the use of unlicensed software.</td></tr>
<tr><td rowspan="2">Management Response:</td><td>Fully agreed</td><td>Partially agreed</td><td>Disagreed</td></tr>
<tr><td></td><td>X</td><td></td></tr>
</table>

<table>
<tr><td>8.23</td><td colspan="3">Web filtering</td></tr>
<tr><td colspan="4">Observation:
The awareness training is optional within the company.</td></tr>
<tr><td colspan="3">Risk (Low):
The lack of mandatory awareness training poses a risk to the security of the organization as employees may not have the necessary knowledge to identify and prevent security incidents. This can lead to increased vulnerabilities and potential breaches, which could result in loss of data, reputation damage, and financial impact. Additionally, it may result in non-compliance with regulatory requirements and standards.</td><td>Priority: 3</td></tr>
<tr><td colspan="4">Recommendation:
Implement mandatory awareness training for all employees. This training should cover essential security topics, including how to identify and report security incidents, how to use security tools and software, and best practices for secure communication and data handling. The training should also be regularly updated to reflect new threats and vulnerabilities. By implementing mandatory awareness training, the organization can improve its overall security posture and reduce the risk of security incidents.</td></tr>
<tr><td rowspan="2">Management Response:</td><td>Fully agreed</td><td>Partially agreed</td><td>Disagreed</td></tr>
<tr><td></td><td></td><td>X</td></tr>
</table>

<table>
<tr><td>CSC1</td><td colspan="3">Inventory and Control of Enterprise Assets</td></tr>
<tr><td colspan="4">Observation:
No procedure is established in case of a piece of equipment is out of date or sold.</td></tr>
<tr><td colspan="3">Risk (Low):
The risk of not having a procedure established in case of a piece of equipment being out of date or sold is that sensitive data or information could be left on the device and potentially be accessed by unauthorized individuals. Additionally, if the equipment is sold without proper data sanitization, the data could be exposed to external entities, leading to a breach of confidentiality. This lack of procedure also creates the risk of losing track of company assets and their corresponding data, potentially leading to financial losses or legal issues.</td><td>Priority: 3</td></tr>
<tr><td colspan="4">Recommendation:
Establish a clear procedure for handling outdated or sold equipment. This procedure should include guidelines for wiping all data from the equipment, ensuring proper disposal or recycling, and any necessary documentation. Additionally, there should be clear communication channels between relevant departments to ensure that all equipment is properly tracked and accounted for throughout its lifecycle. By implementing such a procedure, ACME Corp can better protect its sensitive information and reduce the risk of data breaches or other security incidents related to outdated or improperly disposed of equipment.</td></tr>
<tr><td rowspan="2">Management Response:</td><td>Fully agreed</td><td>Partially agreed</td><td>Disagreed</td></tr>
<tr><td>X</td><td></td><td></td></tr>
</table>

7. Conclusion

Eight observations were made overall based on the audit that was conducted at ACME Corp. in Innsbruck, Austria, by External Audit.

The first finding is that there is no company policy regarding code scans. This exposes the business to dangers like coding flaws and breaches.

The security settings on employees' own devices are not being checked, which brings to the second observation. This puts the business at danger of intrusions and data breaches.

The third finding is that if a device is not Bitlocker-encrypted, there is no way to delete the data if the device is not connected to the internet. This puts the business at risk for data breaches.

The fourth finding is that while working remotely, no site filtering is used. As a result, the business is at danger from malware and phishing assaults.

The fifth finding is the absence of security coding training. This puts the business at danger of having security flaws and vulnerable code.

The sixth finding is the absence of any licenses for outside libraries. This puts the business at risk for both potential legal repercussions and security breaches.

A seventh observation is that awareness training is not mandatory. This puts the organization at risk that employees do not understand security policies and protocols.

The eighth and final caveat is that there are no procedures in place when a device is retired or sold. This exposes companies to the risk of data breaches and unauthorized access.

In general, almost all the findings found are related to lack of standardization and lack of best practices. Based on observations, the

basic requirements of ISO 27001 have not been met and ACME Corp. is therefore not currently considered willing to be accredited according to the referenced criteria.

Identified nonconformities require appropriate and timely administrative response to ensure the correct execution of all daily business operations at ACME Corp. confirmation. Top management should treat nonconformities as a high priority and remediate them in a short period of time to secure ISO certification.

8. Appendix

8.1 Risk Assessment Matrix

We assessed the risk grading of each identified finding according to the following risk matrix:

Risk Assessment Matrix		Risk Severity		
		Low	Medium	High
Risk Likelihood	Likely	Medium	High	High
	Possible	Low	Medium	High
	Unlikely	Low	Low	Medium

Risk Assessment Matrix values:

- Likelihood:
  Likely: May occur in days or on a few months
  Possible: May occur annually
  Unlikely: May occur from 1 up to 5 years

- Severity:

  Low: Negligible/non-existent or no significant impact or may cause limited impact/minimal economic loss to a small portion of the business

  Medium: Moderate impact on the organization's brand and moderate economic loss (negative but recoverable)

  High: Consequences that cause serious legal problems or large financial losses (significant efforts to recover)

8.2 Prioritization (Risk based approach)

Priority	Risk	Description
1	**High**	Findings relate to material matters underlying the internal control system. Observations in this priority class are likely to fall short of system goals and require immediate attention. In addition, all ISO 27001 requirements identified as "high" should fall into this category, as should all CIS controls targeted to his IG1 of Implementing CIS Controls.
2	**Medium**	Observations are primarily related to issues that have a significant impact on organizational operations management but do not require immediate attention.
3	**Low**	Observations that, if corrected, would generally improve internal controls, but are not material to the overall internal control system.

It is important to note that any requirement described in clauses 1-4 of the ISO 27001 standard should be considered a higher priority than any relevant control specified by the CIS framework. This is because compliance with these ISO requirements is necessary for an organization to be considered ISO-compliant. Therefore, even if a requirement/control is labeled as "Priority 1" in the CIS framework, its ISO relevance must be given priority and reflected as such in the Summary of Findings (High Findings) section of the audit report, as per chapter 4.1.