# CERTSec Cybersecurity Recommendations

Date: 28.06.2023
To: TEST AG
From: CERTSec Automated Report Generation Tool

## Subject: Actionable Steps to Fulfill the Remaining Cost-Aware Baseline Certification Requirements

Dear Management of Company **TEST AG**,

Congratulations on your decision to pursue the **Cost-Aware Baseline** Certification! To fulfill each of the requirements, please find below detailed guidance with actionable steps, benefits, estimated timeline, and potential challenges:

## Requirement 1: Continuous Threat and Vulnerability Evaluation

To fulfill this requirement, Company TEST AG should implement the following steps:

1. Establish a process to identify and evaluate threats and vulnerabilities on an ongoing basis.

2. Utilize threat intelligence sources and conduct periodic vulnerability scans to gather relevant information.

3. Assess the likelihood of the identified threats and vulnerabilities being exploited, considering the business context.

**Benefits:** Continuous threat and vulnerability evaluation allows for timely detection and mitigation of potential risks, reducing the likelihood of successful cyberattacks.

**Timeline:** Implementation of this process can be completed within 1 to 3 months, depending on the complexity of the organization's IT infrastructure.

**Potential Challenges:** Challenges may include resource allocation for regular evaluation, keeping up with evolving threats, and integrating vulnerability assessment tools.

## Requirement 2: Prioritization of Identified Risks

To fulfill this requirement, Company TEST AG should implement the following steps:

1. Review all identified risks and categorize them based on their criticality and potential impact on business operations.

2. Consider the likelihood of each risk being exploited, potential damage, and cost of mitigation.

3. Assign priority levels to each risk based on criticality, ensuring that mitigation efforts are focused on high-priority risks.

**Benefits:** Prioritizing identified risks helps allocate resources efficiently, ensuring that high-priority risks are addressed promptly, minimizing potential financial and operational impacts.

**Timeline:** Completion of risk prioritization can be achieved within 2 to 4 weeks, depending on the organization's risk landscape.

**Potential Challenges:** Challenges may include subjective assessment of risk criticality, aligning risk prioritization with business objectives, and obtaining consensus among stakeholders.

## Requirement 3: Regular Review of Identified Risks

To fulfill this requirement, Company TEST AG should implement the following steps:

1. Schedule and conduct annual reviews of identified risks and their respective mitigation measures.

2. Establish a change management process to trigger risk review whenever there are significant changes in the organization's IT infrastructure, third-party relationships, or regulatory environment.

3. Ensure that risk reviews involve relevant stakeholders, including IT, operations, compliance, and legal teams.

**Benefits:** Regular risk reviews enable timely identification and mitigation of emerging risks, keeping the cybersecurity posture up-to-date with evolving threats and changes in the business environment.

**Timeline:** Implementing regular risk reviews can be accomplished within 2 to 3 months, and then conducted annually thereafter.

**Potential Challenges:** Challenges may include ensuring consistent participation of stakeholders, managing the review process efficiently, and coordinating efforts across different departments.

## Requirement 4: Use of Cost-Efficient Cybersecurity Solutions

To fulfill this requirement, Company TEST AG should implement the following steps:

1. Define clear evaluation criteria, including cost, effectiveness, ease of implementation, and integration capabilities.

2. Conduct a comparative analysis of potential cybersecurity solutions using metrics such as Return on Security Investment (ROSI).

3. Prioritize the implementation of cost-efficient solutions with a high ROSI, while considering the identified risks and business requirements.

**Benefits:** Using cost-efficient cybersecurity solutions helps maximize the value of investments, ensures optimal resource allocation, and improves the overall cybersecurity posture.

**Timeline:** Implementation of these steps can be completed within 2 to 4 months, depending on the scale and complexity of the organization's IT systems.

**Potential Challenges:** Challenges may include finding suitable cost-efficient solutions that align with specific business requirements, conducting accurate ROSI calculations, and managing integration with existing systems.

## Requirement 5: Consideration of Cyber Insurance

To fulfill this requirement, Company TEST AG should implement the following steps:

1. Conduct a comprehensive assessment of potential financial impacts resulting from security incidents and data breaches.

2. Evaluate available cyber insurance options and their coverage scope.

3. Make an informed decision to invest in cyber insurance, considering cost, coverage limits, policy terms, and the organization's risk appetite.

**Benefits:** Cyber insurance provides financial protection against potential losses caused by cybersecurity incidents, reducing the organization's financial risk exposure.

**Timeline:** The evaluation and acquisition of cyber insurance can be completed within 1 to 2 months, depending on the complexity of the coverage assessment and negotiation process.

**Potential Challenges:** Challenges may include aligning insurance coverage with specific risks, understanding policy terms and exclusions, and finding insurance providers that offer suitable coverage for the organization's industry and size.

We believe that following these actionable steps will significantly improve Company TEST AG's cybersecurity posture and help in achieving the Cost-Aware Baseline Certification. As with any implementation, challenges may arise, but with proper planning and guidance, these challenges can be overcome effectively.

If you have any further questions or need assistance during the implementation process, please do not hesitate to reach out for professional guidance.

**Best regards,**
CERTSec Team