Step-by-Step Guide to Performing a Security Culture Maturity Model (SCMM) Assessment

1. Define Security Culture Maturity Levels

Before starting the assessment, define the maturity levels you'll be assessing. Most SCMM assessments use five levels:

- **Level 1: Ad-hoc** – Security is not formally addressed; it's reactive and inconsistent.
- **Level 2: Repeatable** – Basic security policies are in place but not consistently enforced.
- **Level 3: Defined** – Security processes are defined, documented, and communicated to employees.
- **Level 4: Managed** – Security practices are monitored, measured, and managed across the organization.
- **Level 5: Optimized** – Security culture is fully integrated and continuously improved within the organization.

2. Identify Key Focus Areas

Identify the focus areas or domains where security culture plays a role in your organization. Common areas include:

- **Leadership and Governance:** Does leadership promote a security-first culture?
- **Awareness and Training:** Are employees regularly trained on security best practices?
- **Incident Response:** Is there a proactive approach to handling incidents, and are employees aware of reporting procedures?
- **Employee Behavior:** How often do employees follow security policies and best practices?
- **Communication and Collaboration:** Is security discussed openly and integrated into all aspects of the business?
- **Technology and Tools:** Are the right security technologies and tools in place and used effectively?

3. Create an Assessment Questionnaire

For each focus area, create a set of questions to evaluate the security culture maturity. Use a rating scale (1 to 5, for example) to score each question, where:

- 1 = Not Implemented
- 2 = Partially Implemented
- 3 = Implemented, but Inconsistent

- 4 = Consistently Implemented
- 5 = Fully Optimized and Continuously Improved

Example Questions

Leadership and Governance:

1. Does leadership regularly communicate the importance of security to all employees?
2. Are security goals integrated into the company's overall business strategy?
3. Are there clear, documented security policies and procedures?
4. Is there a designated security leader or team responsible for overseeing security initiatives?
5. Do executives allocate sufficient resources (budget, personnel) to security programs?
6. Is there a security governance framework in place (e.g., defined roles, accountability)?

Awareness and Training:

1. Are employees required to complete security awareness training upon onboarding?
2. How frequently are refresher security training sessions provided to employees?
3. Is there a formal phishing awareness and prevention program in place?
4. Are different types of security training tailored to specific job roles or departments?
5. Do employees demonstrate an understanding of how to identify security risks (e.g., phishing, social engineering)?
6. Are there any consequences or follow-up actions for employees who fail phishing tests or security assessments?

Incident Response:

1. Is there a documented incident response plan (IRP) that is known to all relevant employees?
2. Are employees trained on how to recognize and report potential security incidents?
3. Is there an easy communication method established to report incidents?
4. Are incidents escalated and communicated to leadership in a timely manner?
5. Is there a designated incident response team responsible for handling incidents?
6. Are incident response simulations or drills (e.g., tabletop exercises) conducted regularly?
7. Are lessons learned from past incidents used to improve the response process?

Employee Behavior:

1. Do employees consistently follow company security policies (e.g., acceptable use, data handling)?
2. How often do employees report suspicious behavior or potential security risks?
3. Are employees incentivized to adopt secure behaviors (e.g., positive reinforcement)?

4. Are security violations (e.g., sharing passwords, leaving sensitive data unsecured) addressed promptly?
5. Do employees take responsibility for the security of their devices and data, whether working on-site or remotely?
6. Are employees encouraged to collaborate with the security team or leadership when they encounter security issues?

Communication and Collaboration:

1. Are security updates (e.g., new policies, threat alerts) communicated effectively across all departments?
2. Is there open dialogue between employees and the security team regarding security concerns or questions?
3. Does the company have cross-departmental security initiatives or committees that involve non-IT employees?
4. Are there regular security meetings or check-ins to discuss current threats, vulnerabilities, or best practices?
5. Are employees encouraged to provide feedback on security policies and their implementation?
6. Do teams collaborate during security initiatives (e.g., security assessments, audits, incident responses)?

Technology and Tools:

1. Are the security tools and technologies in use up to date and aligned with industry standards and regulatory / compliance requirements?
2. Are there automated tools in place to detect and respond to security incidents?
3. Are all systems and applications regularly patched and updated to address vulnerabilities?
4. Are employees trained on how to use security tools, such as multi-factor authentication (MFA) or encryption?
5. Is there a system in place to monitor and control access to sensitive data and systems?
6. Are employees provided with secure mobile devices and remote work solutions (e.g., VPN, encrypted communications)?

Risk Management:

1. Does the company perform regular risk assessments to identify security vulnerabilities?
2. Are identified risks prioritized based on their potential impact and likelihood?
3. Is there a risk management process that involves employees from various departments?
4. Are security risks related to third-party vendors and partners regularly assessed?
5. Are security risks clearly communicated to employees and leadership?

6. Is the company's risk tolerance aligned with its security strategy?
7. Are leaders / risk owners held accountable for risks?

Compliance and Regulatory Awareness:

1. Are employees aware of the regulatory and legal requirements related to data protection (e.g., GDPR, CCPA)?
2. Does the company regularly audit its processes for compliance with relevant security regulations?
3. Is there clear guidance on how to handle sensitive data according to regulatory requirements?
4. Do employees understand the consequences of non-compliance with security regulations?
5. Are employees trained to recognize and respond to data breaches in compliance with legal requirements?
6. Are there regular updates on changes to security laws and regulations, and are employees informed about these changes?

Physical Security:

1. Are there physical security controls in place (e.g., keycard access, locked rooms) to protect sensitive areas?
2. Do employees understand their role in maintaining physical security (e.g., not allowing tailgating into secure areas)?
3. Are there processes in place for securing physical documents containing sensitive information?
4. Are there policies for the secure disposal of sensitive physical materials (e.g., shredding documents)?
5. Are security cameras and monitoring systems in place and actively monitored?
6. Is physical security integrated with cybersecurity practices (e.g., ensuring locked areas house critical IT infrastructure)?

Performance Measurement and Reporting:

1. Are key performance indicators (KPIs) used to track the effectiveness of security programs?
2. Does the company have a process for reporting and addressing security incidents or vulnerabilities?
3. Are security metrics regularly reviewed by leadership to guide strategic decisions?
4. Are there regular reports generated on employee compliance with security training and policies?
5. Does the company have a system for collecting and analyzing feedback on the effectiveness of its security initiatives?
6. Are there benchmarks in place to measure improvements in security culture over time?

Culture of Continuous Improvement:

1. Is security seen as a priority by all employees, not just IT or leadership?
2. Are employees encouraged to continuously seek ways to improve security in their daily work?
3. Does the organization invest in ongoing security education and awareness programs?
4. Are new employees quickly introduced to security best practices during onboarding?
5. Is security regularly reviewed and adjusted to adapt to new threats or business changes?
6. Are there rewards or recognition for employees who contribute to improving security culture?

4. Conduct Surveys and Interviews

Survey Employees: Send the assessment questionnaire to employees across different departments to get a comprehensive view of the organization's security culture.

Interview Key Stakeholders: In addition to surveys, conduct interviews with senior management, IT staff, and other key roles to gather deeper insights into the organization's security culture.

5. Analyze the Results

Score Each Area: For each focus area, calculate the average score based on the ratings provided in the survey and interviews.

Identify Maturity Levels: Based on the average scores, determine the maturity level for each focus area. For example:

- 1-2: Ad-hoc
- 3: Defined
- 4: Managed
- 5: Optimized

Identify Gaps: Look for areas where your scores are lower and identify gaps in your security culture. These areas will be your focus for improvement.

6. Create an Action Plan for Improvement

Set Priorities: Based on the identified gaps, prioritize the areas that need the most attention. Focus first on areas that pose the greatest risk to the organization.

Define Improvement Goals: Set specific, measurable goals for each focus area to move to the next level of maturity. For example:

Leadership and Governance: Improve executive involvement in security decision-making.

Awareness and Training: Increase the frequency and quality of security training for employees.

Assign Responsibilities: Assign team members or departments to be responsible for implementing changes in each focus area.

7. Monitor and Measure Progress

Track Progress: Regularly monitor progress in each focus area. Set up key performance indicators (KPIs) to measure the impact of improvements.

Schedule Regular Assessments: Conduct the SCMM assessment annually or after major changes in the company’s security environment to continuously improve the security culture.

8. Communicate Findings and Progress

Share Results: Present the findings of the assessment to senior leadership and key stakeholders. Use the results to drive discussions about improving the organization’s overall security culture.

Celebrate Success: Recognize improvements and celebrate success when your organization reaches higher maturity levels in specific areas.

9. Iterate and Improve

Security culture is not a one-time achievement. Continuously revisit the SCMM assessment process to adapt to new security challenges, technological changes, and business needs.