# UNIT-2

## Scrum Security Review

Table 1: Secure Software Processes in Scrum

|  |  |
| --- | --- |
| **Scrum Stage** | **Recommended Security Processes** |
| **Product Backlog** | Incorporate security requirements into user stories. Prioritize security features alongside functional features. Conduct threat modeling to identify potential security risks (Sharma & Bawa, 2020). |
| **Sprint Planning** | Define security-focused acceptance criteria for each user story. Allocate time for security testing within the sprint. Engage security experts in planning discussions (Rindell et al., 2020). |
| **Sprint Development** | Implement secure coding practices (e.g., input validation, encryption). Conduct peer code reviews with a focus on security vulnerabilities. Use automated security testing tools (Sharma & Bawa, 2020). |
| **Daily Scrum** | Include security updates in daily stand-ups. Address security-related impediments promptly. Ensure that any changes to security requirements are communicated to the team (Dixit & Bhushan, 2021). |
| **Sprint Review** | Demonstrate completed security features and discuss any security issues encountered. Gather feedback from stakeholders on security aspects of the product (Sharma & Bawa, 2020). |
| **Sprint Retrospective** | Reflect on security practices and identify areas for improvement. Plan actions to enhance security in future sprints. Document security lessons learned (Sharma & Bawa, 2020). |

## Blog Post: Managing Cybersecurity Risks from the Inside

### Unit 2: Scrum Security Review - Blog Post: Managing Human Factors to Strengthen Cybersecurity

While technology often focuses on a way to avoid cyber threats, human factors remain one of the biggest vulnerabilities to cybersecurity. Intentional or even unintentional human errors can easily lead to breaches in data security, among other security issues. Fortunately, the ISO/IEC Standard 27000 has provided some necessary strategies that will help mitigate such risks through the effective management of the people. Following are five important aspects on which concentration is required**:**

**1. Access Control (ISO/IEC 27000, 3.1):**

Access control becomes very important while limiting access to sensitive information and systems. The implementation of strict access controls coupled with periodic permission review assists in preventing unauthorized access. By allowing staff to have only the access required to perform their function, it reduces the likelihood of an internal threat.

**2. Information Security Policy (ISO/IEC 27000, 3.5):**

A well-defined information security policy lays down the Acceptable Use of the resources and sets the benchmark for implementing security practices. Notifications through regular training are required to be given to the employees to understand these policies. Clear guidelines help reduce accidental or intentional breaches.

**3. Security Awareness, Education, and Training (ISO/IEC 27000, 3.13):**

Continuous education among the staff helps employees to identify and understand the nature of threats such as phishing and data mishandling. Security awareness entrainments contribute to proactive employees in actually helping an organization protect against these kinds of cyber threats.

**4. Incident Management (ISO/IEC 27000, 3.8):**

In this context, an effective incident management process will help with timely detection and incident response. Training employees on reporting suspicious activities will ensure that potential security threats are identified on time and dealt with to minimize damage.

**5. Monitoring (ISO/IEC 27000, 3.10):**

Continuous monitoring of user activity is the only sure way to spot erratic behavior that may imply there was a data breach. Regular log analysis will help organizations identify and contain insider threats. Addressing these five focus areas will help organizations keep human-linked cybersecurity risks in perspective and make their defenses robust against insider threats.

**References:**

Rindell, K., Ruohonen, J., Holvitie, J., Hyrynsalmi, S., & Leppänen, V. (2021). Security in agile software development: A practitioner survey. *Information and Software Technology*, *131*, 106488.

Dixit, R., & Bhushan, B. (2019). Scrum: An Agile software development process and metrics. *Journal on Today's Ideas-Tomorrow's Technologies*, *7*(1), 73-87.

Mimecast. (2024) *The State of Email & Collaboration Security Report 2024*. Available from: [Mimecast Report](https://mysecuritymarketplace.com/reports/human-risk-ai/). [Accessed 26/08/2024].

International Organization for Standardization. (2018) *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Available from: [ISO Standard](https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en). [Accessed 26/08/2024].

Sharma, A., & Bawa, R. K. (2022). Identification and integration of security activities for secure agile development. *International Journal of Information Technology*, *14*(2), 1117-1130.