Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

CSI IMPLEMENTATION MODEL

GO CLOUD GO SECURE

Phase 1: ANALYSE

- Step 1: Cloud Service List
- Step 2: Risk Mapping
- Step 3: Compliance

Phase 2: DEFINE

- Step 4: Roles & Responsibilities
- Step 3: Define Control Objectives
- Step 2: Risk Prioritisation
- Step 1: Policy Development

Phase 3: PLAN

- Step 1: Mitigation Actions
- Step 2: Control Mapping
- Step 3: Documentation
- Step 4: Training Program

Phase 4: IMPLEMENT

- Step 2: Training & Awareness
- Step 1: Technical Actions

Phase 5: VERIFY

- Step 1: Testing
- Step 2: Monitoring
- Step 3: Feedback

Co-funded by the European Union

Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

CSI IMPLEMENTATION MODEL

GO CLOUD GO SECURE

Phase 1: ANALYSE

Step 1: Cloud Service List
Create a full list of all cloud services used by your organization. Knowing what you use and what is critical is essential before assessment.

Step 2: Risk Mapping
The CSI Matrix identifies threats, vulnerabilities, and risks for each cloud service, providing a clear view of your organisation's key weaknesses.

Step 3: Compliance
Check your organisation's compliance with EU regulations and international standards to avoid fines, data loss, and reputation damage. Some require specific controls like access logging, encryption, and incident reporting.

Phase 2: DEFINE

Step 1: Policy Development
Draft a Cloud Security Policy that defines rules for secure cloud use, access control, and data protection, forming the backbone of your security framework.

Step 2: Risk Prioritisation
Use the CSI Matrix to score risks by likelihood and impact, focusing on the most urgent risks to guide mitigation.

Step 3: Define Control Objectives
Define clear mitigation objectives for each high-priority CSI Matrix risk to turn awareness into tailored action plans.

Step 4: Roles & Responsibilities
Assign clear roles - Cloud Admin manages platforms, Data Owner manages data access, Security Officer handles monitoring and incidents, Compliance Manager ensures regulatory adherence.

Phase 3: PLAN

Step 1: Mitigation Actions
For each high-priority CSI Matrix risk, define specific, actionable mitigation measures, ensuring fast and consistent implementation especially for SMEs lacking full-time security staff.

Step 2: Control Mapping
Create a mapping table linking mitigation actions to specific cloud services, clarifying what is protected and how controls are applied.

Step 3: Documentation
Prepare templates and checklists - such as Implementation Checklists, Incident Response Templates, and Audit Log Review forms - to support policy enforcement, auditing, and continuous improvement.

Step 4: Training Program
Design a practical CSI Training Program covering cloud basics, key vulnerabilities, and misconfigurations to effectively train personnel and prevent 80% of cloud security failures.

Co-funded by the European Union

Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

CSI IMPLEMENTATION MODEL

GO CLOUD GO SECURE

Phase 4: IMPLEMENT

Step 1: Technical Actions

Implement technical actions from Phase 3's roadmap, such as enabling MFA, encryption, IAM policies, and RBAC, using built-in tools like AWS Config and Azure Security Center - starting with quick wins like enabling MFA and RBAC.

Step 2: Training & Awareness

Implement your training plan from Phase 3, focusing on the Matrix and training material with short, practical modules tailored to your organisation's technical reality and risk profile.

Phase 5: VERIFY

Step 1: Testing

Conduct resilience testing through exercises, simulated attacks, control checks, and security assessments to verify that mitigation actions are correctly implemented, effective, and up to date, ensuring your organisation is prepared for real-world threats.

Step 2: Monitoring

Establish KPIs to monitor cloud security, enabling proactive management and tracking improvements; key indicators include failed logins, misconfiguration alerts, and outdated patches, visualized via a simple metrics dashboard.

Step 3: Feedback

Develop an incident registry logging each event's details, causes, impacts, and mitigations to update risk assessments, refine policies, and adapt training, ensuring a dynamic and evolving security framework.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the European Union