

Evidence Of The Competence Of The People Working In Information Security

# 1. Introduction

**1.1 Purpose**

The purpose of this document is to define how ABC-FinTech ensures that personnel working in roles that affect the organization’s information security performance are competent. This includes determining necessary competencies, evaluating training, education, and experience, and maintaining documented evidence of competence.

**1.2 Scope**

This document applies to all personnel within ABC-FinTech who have a role in the organization’s Information Security Management System (ISMS). It includes employees, contractors, and third-party service providers working under the organization’s control.

# 2. Competency Requirements for Information Security Roles

**2.1 Determining Competency Requirements**

ABC-FinTech determines the necessary competence for each role related to information security by:

* Reviewing the specific responsibilities of the role.
* Aligning competencies with the skills and qualifications required to manage the confidentiality, integrity, and availability (CIA) of information assets.
* Mapping role requirements to industry certifications, educational qualifications, and relevant experience.

**2.2 Competency Table for Key Roles**

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Required Competencies | Education/Certifications | Experience |
| Chief Information Security Officer (CISO) | Strategic management of ISMS, incident response, compliance, risk management | Master's in Information Security, **CISSP**, **CISM**, ISO 27001 Lead Implementer | 10+ years in cybersecurity leadership |
| Information Security Analyst | Threat detection, vulnerability management, security monitoring | Bachelor's in IT/Security, **CEH**, **Security+**, **ISO 27001 Foundation** | 2-5 years in security operations |
| Risk & Compliance Manager | Compliance management, risk assessment, regulatory adherence | Bachelor's in Law/IT, **CISA**, **CRISC**, **ISO 27001 Lead Auditor** | 5-7 years in compliance and risk management |
| SOC (Security Operations Center) Manager | Incident handling, monitoring, real-time threat analysis | Bachelor's in IT/Computer Science, **CISSP**, **CEH** | 5-8 years in incident response |
| Database Administrator (Security) | Data encryption, database security management | Bachelor's in IT, **Oracle Certified Professional**, **CISM** | 3-5 years in database security |
| Vendor Management Lead | Third-party risk management, contract management | Bachelor's in Business/IT, **CISA**, **CRISC** | 3-5 years in vendor management and security assessments |

# 3. Ensuring Competence Through Education, Training, and Experience

**3.1 Initial Hiring and Onboarding**

When hiring new personnel for information security roles, ABC-FinTech ensures that candidates meet the required qualifications based on:

* **Education:** Academic degrees in relevant fields (e.g., Information Security, IT).
* **Certifications:** Industry-recognized certifications such as **CISSP**, **CISM**, **CEH**, **ISO 27001 Lead Implementer**, or equivalents.
* **Experience:** Prior work experience relevant to the specific role and the security challenges of a FinTech company.

**3.2 Ongoing Training and Development**

ABC-FinTech provides ongoing training for all employees in information security roles to ensure that their skills remain current and aligned with evolving threats and regulatory requirements. This includes:

* **Annual Security Awareness Training** for all employees.
* **Advanced Security Training** for IT security personnel covering new security tools, emerging threats, and regulatory updates.
* **Certification Support:** Encouraging and financially supporting employees to obtain relevant industry certifications such as **CISSP**, **CISA**, **ISO 27001 Lead Auditor**.

**3.3 Specific Training Requirements by Role**

|  |  |  |
| --- | --- | --- |
| Role | Required Ongoing Training | Frequency |
| CISO | Executive-level cybersecurity strategy, regulatory compliance updates | Bi-annually (internal & external seminars) |
| Information Security Analyst | Threat detection systems, incident response techniques | Quarterly (hands-on labs, online courses) |
| Risk & Compliance Manager | Risk management frameworks, regulatory changes (e.g., GDPR, PCI-DSS) | Bi-annually (certification refreshers, regulatory seminars) |
| SOC Manager | Real-time threat analysis, incident response simulations | Quarterly (tabletop exercises, simulated attacks) |
| Database Administrator (Security) | Database security protocols, encryption standards | Annually (database vendor updates, workshops) |
| Vendor Management Lead | Third-party risk management, contract security requirements | Annually (vendor security workshops) |

# 4. Acquiring and Evaluating Competence

**4.1 Acquiring Necessary Competence**

In cases where gaps in competence are identified (e.g., due to new technology, processes, or regulatory changes), ABC-FinTech takes the following actions:

* **Training Programs:** Design and deliver targeted training programs, either in-house or through external providers.
* **Mentoring and Coaching:** Assign senior staff or external consultants to mentor employees in areas requiring development.
* **Certification Sponsorship:** Support employees in obtaining new certifications relevant to their role.

**4.2 Evaluating Competence**

The effectiveness of actions taken to improve competence is evaluated by:

* **Performance Reviews:** Regular performance reviews assessing the employee’s ability to meet information security responsibilities.
* **Competency Audits:** Annual competency audits to review the qualifications, certifications, and training records of personnel in key roles.
* **Incident Response Evaluation:** Evaluating the employee’s effectiveness during real incidents and simulated exercises (e.g., red team/blue team exercises).
* **Training Feedback:** Gathering feedback on the relevance and effectiveness of training programs to ensure continuous improvement.

# 5. Documented Evidence of Competence

ABC-FinTech retains the following records as documented evidence of competence for individuals in information security roles:

**5.1 Documentation Records**

* **Employee CVs and Resumes:** Containing details of education, certifications, and relevant experience.
* **Certification Records:** Copies of relevant industry certifications (e.g., **CISSP**, **CISM**, **CEH**, **ISO 27001**).
* **Training Records:** Documentation of training courses completed by personnel, including dates, content, and feedback.
* **Performance Reviews:** Documented performance evaluations focused on the employee’s competence in information security.
* **Audit Reports:** Results of competency audits and corrective actions taken to address any gaps.

**5.2 Retention of Documentation**

* **Certification Records:** Retained for the duration of employment plus 3 years.
* **Training Records:** Retained for 5 years to demonstrate compliance with ongoing training requirements.
* **Performance Reviews:** Retained for the duration of employment plus 3 years.

# 6. Monitoring and Review

**6.1 Ongoing Monitoring**

ABC-FinTech monitors the competency of its personnel through:

* **Annual Performance Reviews:** Managers assess the competencies of employees in their roles, including their information security skills.
* **Continuous Professional Development (CPD):** Employees are encouraged to continually develop their skills through learning and certifications.
* **Security Incident Performance Reviews:** Incident reports are reviewed to evaluate the effectiveness of staff responses, identifying any areas where additional training may be needed.

**6.2 Competence Review Cycle**

ABC-FinTech will conduct an annual review of competence requirements for information security roles. Adjustments to the competency framework will be made in response to:

* Changes in technology and tools.
* Regulatory changes (e.g., updates to ISO standards).
* Results from internal audits or external certification audits.

# 7. Conclusion

ABC-FinTech’s approach to ensuring and documenting the competence of personnel in information security roles is aligned with ISO 27001:2022 standards. By maintaining a focus on continuous development, regular evaluation, and proper documentation, ABC-FinTech ensures its personnel are equipped to handle evolving security challenges.

**Approved by:**

**CEO, ABC-FinTech**  
**Date: 17 Jan 2024**