

IBF Standards: Checklist Submission

Industry Segment	Future-Enabled Skills
Job Specialisation	Risk & Governance in Digital World
Objective Statement	Understand and manage risks in a digitised world of financial services

Competency Unit	1	Threat Intelligence and Detection (Similar to Technical Skills & Competencies (TSC): Risk Management, Governance and Regulatory Compliance- Security Governance)
Proficiency Level: 4		
Performance Criteria		
1.1. Assess adherence of applications and infrastructure components to security standards and baselines		
1.2. Identify lapses in organisational security standards or issues that may endanger information security and integrity		
1.3. Develop specific action plans for different business units, based on corporate security policies, standards and guidelines		
1.4. Evaluate technologies and tools that can address security gaps and facilitate alignment with security policies		
1.5. Introduce security controls in line with corporate security policies and frameworks		
1.6. Roll out security guidelines and protocols, ensuring understanding and compliance		
1.7. Review adequacy of information security controls		
1.8. Highlight areas for improvement and propose solutions		
Curriculum and Learning Outcomes		
<ul style="list-style-type: none"> • Organisation security operational procedures • Implementation process and considerations for security policies and protocols • Types of security controls and implementation procedures • Techniques for assessment of processes against security standards 		

Competency Unit	2	Threat Intelligence and Detection (Similar to Technical Skills & Competencies (TSC): Risk Management, Governance and Regulatory Compliance- Security Governance)
Proficiency Level: 5		
Performance Criteria		
2.1. Identify existing security risks, threats and vulnerabilities and analyse gaps in current organisational security policies		
2.2. Develop corporate security policies based on organisation's direction, to ensure business operations are well protected		
2.3. Recommend improvements, updates or modifications to current security policies and practices, to address potential security gaps		
2.4. Introduce suitable technologies, processes and tools to monitor, guide and maximise compliance with security policies		
2.5. Drive communication of corporate security policies and implementation of security protocols		
2.6. Establish internal processes to regularly review adequacy of information systems' security controls against set benchmarks		
Curriculum and Learning Outcomes		
<ul style="list-style-type: none"> • Security gap analysis 		

• Security threats and system vulnerabilities
• Critical elements of corporate security policies
• Security frameworks
• Key messages to drive in communication of security standards

Competency Unit	3	Threat Intelligence and Detection (Similar to Technical Skills & Competencies (TSC): Risk Management, Governance and Regulatory Compliance- Security Governance)
Proficiency Level: 6		
Performance Criteria		
3.1. Set direction for the organisation's corporate security policies, frameworks and protocols, in line with business requirements and the external environment		
3.2. Endorse proposals for updates or enhancements to corporate security policies		
3.3. Establish benchmarks and targets for information systems operations and processes to be regularly reviewed against		
Curriculum and Learning Outcomes		
• Potential internal and external threats to organisational security		
• Emerging trends and developments in security management and practices		
• Industry standards and best practices for organisational security		
• Impact of changes in security protocols on the organisation		
• Industry best practices and benchmarks for security frameworks		