Central Bank of Malta
Job Description

Job Title: Information Security Governance, Risk and Compliance (GRC) Analyst			
Office:	**Operational Risk Management Office (ORMO)**	**Reports To:**	**Manager ORMO & Information Security Officer (ISO)**
Department:	**Risk Management and Payments Compliance**	**Date:**	**June 2026**

Job Overview:

The Information Security GRC Analyst, plays a key role in strengthening the Bank's information security and resilience posture. The incumbent works on governance, risk, and compliance, partnering closely with business and IT teams across the Bank to embed security best practices into everyday operations.

This role offers the opportunity to contribute to high-impact initiatives, learn about the European System of Central Banks (ESCB), and work in a collaborative team.

The incumbent will maintain and evolve the Bank's Information Security Management System (ISMS) in line with best practices and international standards, ensuring it remains practical, relevant, and effective across the Bank.

The incumbent will:

- Support business areas across the Bank by helping them align policies, procedures, and controls with the ISMS, while monitoring implementation and the effectiveness of risk mitigation measures.
- Operate and continuously improve the ISMS, including compliance reviews, on-site visits, control assessments, staff awareness activities, progress reporting, and maintaining a robust information asset register.
- Contribute to incident management and governance reporting, supporting the timely escalation, analysis, and reporting of information security incidents to relevant committees and decision-making bodies.
- Perform information security risk assessments across systems, processes, projects, and third-party arrangements, supporting informed risk-based decision-making.
- Support the implementation and ongoing enhancement of the Information Security Management System (ISMS), contributing to audit readiness and continuous improvement.
- Act as a subject-matter expert on governance, risk, and compliance frameworks, keeping abreast of regulatory expectations, supervisory developments, and industry best practices relevant to a central banking environment.
- Engage in Third-Party Risk Management (TPRM) activities by assessing and helping mitigate information security risks arising from outsourcing and supplier relationships.

Central Bank of Malta
Job Description

Technical / Functional Responsibilities:

Information Security GRC:

- Maintain, review, and update the ISMS, policies, and related templates to ensure alignment with international standards, ESCB policies, and best practices.
- Identify Business Area (BA) policies required to meet ISMS requirements.
- Coordinate with BAs on the development and alignment of such policies and review policy changes for ISMS alignment.
- Conduct on-site inspections through interviews, observation, data gathering, and cross-checking.
- Analyse inspection results, identify gaps and mitigation measures, and prepare inspection reports.
- Discuss findings with the relevant BA and finalise the resilience process.
- Prepare and present Compliance Status Reports to the Risk Committee.
- Follow up with BAs to ensure agreed mitigation measures and controls are implemented.

TPRM:

- Conduct third-party security due diligence and risk assessments.
- Review supplier ISMS frameworks, security controls, and contractual security requirements.
- Monitor remediation actions and ongoing supplier risk.
- Support incident handling and resilience assessments.
- Contribute to governance and risk reporting.

ISMS Planning and Support:

- Support the planning, coordination, and delivery of ISMS activities across business areas, including control implementation, risk assessments, incident reporting, audit follow-ups, and staff awareness and training.
- Act as a key support to the Information Security Officer, serving as an internal and external contact point for information security matters and contributing to governance activities, committee preparation, and follow-up actions.

Other:

.

- Adhere to established policies and procedures.
- Report on activities undertaken.
- Ensure a high standard of work and service quality.
- Perform any other duties as may be assigned from time to time.
- Act as a team player and maintain effective communication within the office and with Business Areas.

Central Bank of Malta
Job Description

Competencies and Proficiency Levels

Within the context of their specific tasks, the incumbent is expected to:

- Be truthful and honest;
- Have a positive, can-do attitude;
- Share the Bank's intolerance of sexism, homophobia, xenophobia and racism, and to be respectful and caring towards others irrespective of sexual, religious and political orientation;
- Carry out their tasks professionally and ethically;
- Communicate effectively;
- Have a sense of the value of time and priorities;
- Respect security and confidentiality; and
- Be able to lead and to work in teams as may be the case.

Where applicable, the incumbent will have the following competences at a specified level of proficiency

General Competencies	**N/A**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Analysis, research and problem solving				**X**		
Customer Care			**X**			
Computer and IT Literacy				**X**		
Managerial Competencies	**N/A**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Strategic Thinking and Planning			**X**			
Promoting Change through Creativity			**X**			
Leading People and Performance			**X**			
Managing Relationships			**X**			
Operations, Processes and Information Management			**X**			
Industry Awareness and Understanding			**X**			
Technical Competencies	**N/A**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Project and Program Management		**X**				
IT Security and Controls					**X**	
Governance, Risk Management & Control				**X**		
Integrity and Objective Judgement				**X**		

Central Bank of Malta
Job Description

Experience and Qualifications

- Candidates should either hold a professional qualification in information security (such as CISM or CISA or CISSP or CRISC) OR hold a Bachelor's degree (at MQF Level 6) in operational risk or business management or information technology or any other related discipline.
- Candidates should have at least 2 years of experience in Governance Risk Compliance or Information Security, or Audit.
- Preference will be given to candidates with proven experience with regulators, auditors, and external stakeholders
- Knowledge of risk management methodologies and GRC/TPRM platforms is an asset.
- Hands-on experience with ISMS, TPRM, or similar frameworks is an asset.
- Sound analytical skills, good quality in organisation of work, keeping to deadlines, delivery and reporting of work.
- Ability to communicate well, to train others and to deliver presentations.
- Highly motivated, with a proven ability to work on own initiative within a challenging / dynamic work environment.

Working Relationships and Lines of Communication

Internal **All business areas and levels of management**

External **ESCB, Third Party Vendors, External Audit**

Physical Dimensions

Nil

To Be Completed by Each Employee in the Role

Employee Name	
Employee Signature	**Date**
Head of Department Signature	**Date**