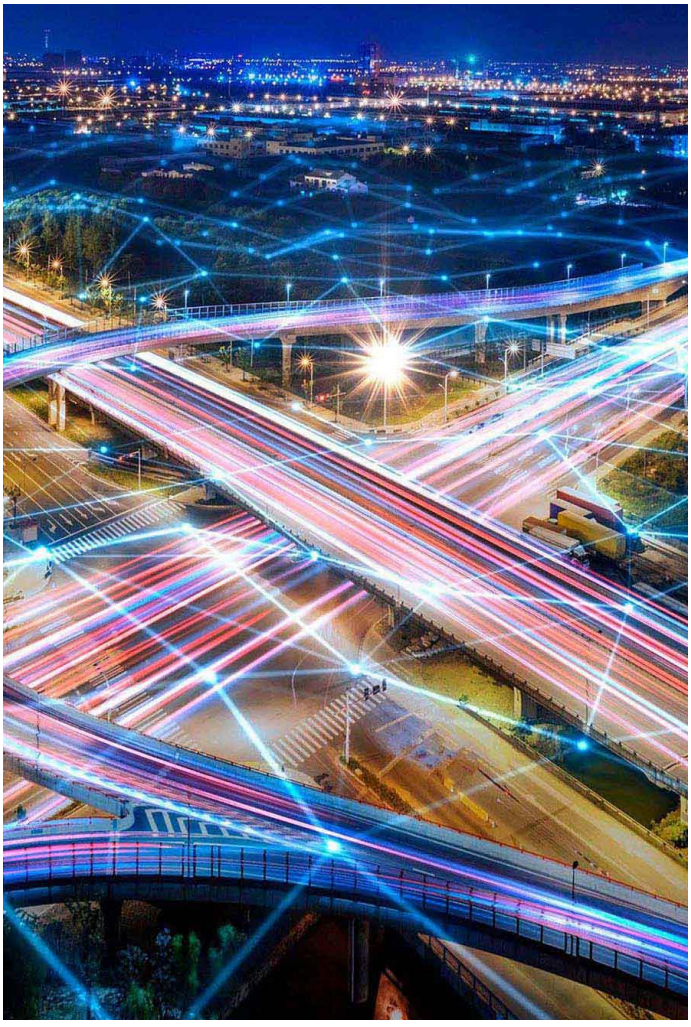
CONFIDENTIAL

Our Governance, Risk & Compliance solution

2026

Our Governance, Risk & Compliance (GRC) services

- Governance & Compliance
- Enterprise Risk Management
- Cybersecurity & Information Security
- Internal Audit



Outsourced Governance & Compliance function holders

Outsourced Compliance Officer

We provide independent compliance oversight, ensuring your organisation meets regulatory expectations and maintains robust, up-to-date compliance frameworks.

Outsourced Data Protection Officer

We oversee your data protection governance, monitor GDPR compliance, and act as your independent point of contact for supervisory authorities.

Outsourced Internal Audit function holder

We lead the internal audit function, delivering objective assurance, executing the audit plan, and strengthening governance and control effectiveness.

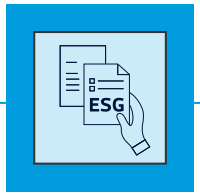
Outsourced Information Security Officer

We manage your cybersecurity governance, support policy development, strengthen controls, and provide structured reporting and incident-response guidance.

Outsourced Risk Management function holder

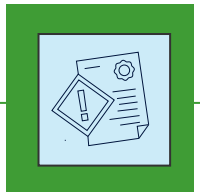
We oversee your risk management framework, ensuring risks are identified, assessed, monitored, and reported effectively across the organisation.

Other support services



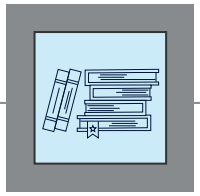
Framework design & implementation

We design and embed governance, compliance, and security frameworks tailored to your organisation's operations and regulatory environment.



Gap assessments

We assess current practices against regulatory, industry, or certification standards and deliver clear, actionable remediation recommendations.

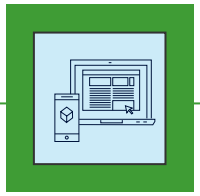


Readiness reviews

We perform pre-implementation and pre-inspection reviews to prepare your organisation for certifications, audits, and supervisory assessments.

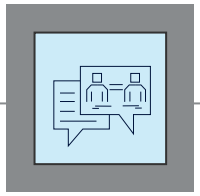
Policy & procedure development

We develop or enhance governance documents, ensuring policies and procedures are clear, practical, and aligned with best practice.



Incident / breach support

We support you in managing incidents and breaches, guiding containment, investigation, documentation, and regulatory reporting.

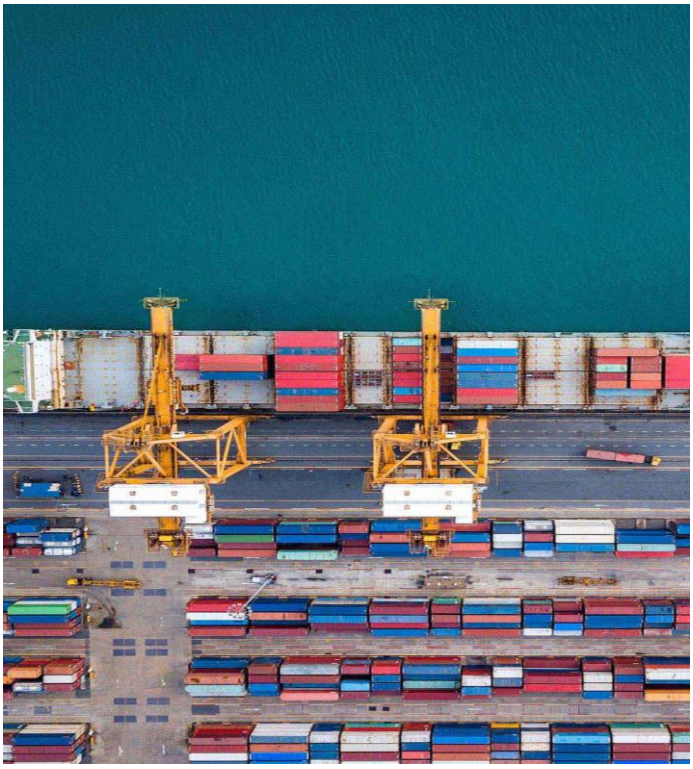


Ongoing advisory

We offer continuous, on-demand guidance to support day-to-day compliance, risk, and governance queries.

Regulatory Compliance Services: Strengthening your control environment

Our Regulatory Compliance Services are designed to give your organisation complete peace of mind by ensuring that your operations, governance structures, and reporting obligations always meet regulatory expectations. Whether you require targeted support or the full delegation of responsibility, we can take on key roles such as Compliance Officer or Data Protection Officer, providing independent oversight, expert guidance, and hands-on management of your regulatory requirements. Every service is tailored to strengthen your compliance framework and help you stay ahead of evolving obligations.



How we support your Regulatory Compliance framework

01

Outsourced Compliance Officer
We provide you with compliance officer services through an outsourcing arrangement, ensuring your organisation meets regulatory expectations and maintains robust, up-to-date compliance frameworks.

02

Regulatory Compliance advisory
We help you interpret regulatory obligations and integrate them effectively into your operations.

03

Follow-up & monitoring
We track remediation actions and validate that audit or review findings are fully resolved.

04

Governance review
We assess governance structures, roles, responsibilities, and reporting lines to ensure transparency and accountability.

05

Licensing & registration management
We manage the licensing lifecycle, from application and variation to renewal, ensuring smooth and compliant submissions.

06

Regulatory reporting
We prepare regulatory reports accurately and on time, meeting supervisory expectations.

07

Regulatory Compliance testing
We conduct risk-based testing to evaluate conduct-related risks and the effectiveness of controls and business practices

08

Training & awareness
We deliver tailored compliance training to enhance staff understanding of regulatory requirements and good conduct practices.

Our Regulatory expertise

Specialist knowledge to support your requirements

- Regulatory frameworks across financial and non-financial sectors
- Conduct, governance, and compliance control environments
- Knowledge of regulatory requirements issued by the MFSA, MGA, FIAU and other regulators.
- Anti-money laundering and Counter Financing of Terrorism (AML/CFT) regulatory expectations and best practices
- Data protection and privacy requirements
- Conduct risk and consumer protection considerations
- Regulatory reporting obligations and methodologies
- Policy and governance framework design
- Regulatory change interpretation and horizon scanning

Strengthening your Data Protection Governance and Compliance

Our Data Protection services help you build and maintain a strong, compliant, and operationally effective privacy framework. Whether you require an Outsourced Data Protection Officer or targeted support, we help your organisation meet GDPR and local legislative obligations while embedding a culture of privacy and accountability.

We provide end-to-end support across governance, operational practices, documentation, monitoring, and incident response, ensuring your data protection environment remains robust, defensible, and aligned with regulatory expectations.

How we support your Data Protection framework

01

Outsourced Data Protection Officer
We provide you with data protection officer services through an outsourcing arrangement, ensuring your organisation meets data protection expectations and maintains robust, up-to-date data protection frameworks.

02

Data Protection framework development
We design and enhance your data protection governance framework, ensuring alignment with GDPR, local legislation, and sector-specific requirements.

03

Record of Processing Activities (RoPA) support
We help you create, update, and maintain a complete and compliant RoPA, ensuring processes, data flows, and legal bases are clearly and accurately captured.

04

Data Protection Impact Assessments (DPIA) & Legitimate Interest Assessments (LIA)
We support the execution, review, and documentation of DPIAs and LIAs to ensure risks to individuals' rights and freedoms are identified, assessed, and mitigated.

05

Data Protection monitoring & assurance
We perform independent reviews and effectiveness testing of your privacy controls, governance arrangements, and operational practices.

06

Training & awareness
We deliver bespoke data protection training to staff and management to raise awareness, support compliance, and reinforce a culture of privacy.

How we support your Data Protection framework

07

FRIA for High-Risk AI Systems

We conduct Fundamental Rights Impact Assessments (FRIAs) as required under Article 27 of the EU AI Act, helping you assess and document how high-risk AI systems may affect individuals' rights and freedoms.

Our Data Protection expertise

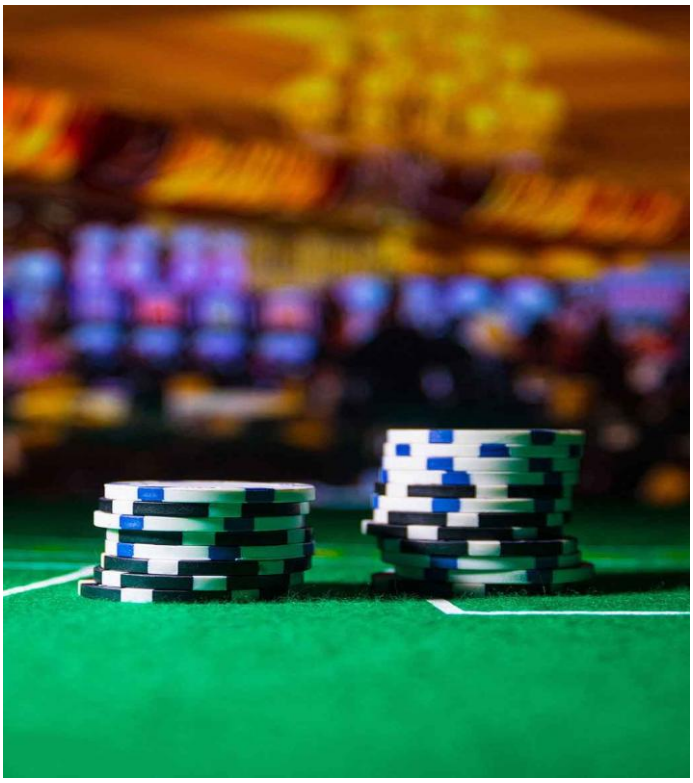
Specialist knowledge to support your requirements

- GDPR and local data protection regulatory frameworks
- Data protection governance, roles, and accountability structures
- Privacy risk assessments, DPIAs, LIAs, and high-risk processing reviews
- Record of Processing Activities (RoPA) design, maintenance, and validation
- Data subject rights management and compliance
- Personal data breach assessment, response, and notification procedures
- Vendor and third-party data processing due-diligence and contractual reviews
- Development and enhancement of policies, procedures, and privacy notices
- Data lifecycle management, retention policies, and secure-processing controls
- Independent monitoring, audits, and effectiveness reviews
- Staff training, awareness, and cultural privacy uplift initiatives

Anti-Financial Crime Regulation Compliance

Our Anti-Financial Crime services strengthen your organisation's ability to prevent, detect, and respond to a wide range of illicit activities. We support you in building robust, risk-based frameworks that address money laundering, terrorist financing, sanctions breaches, fraud, bribery and corruption, market abuse, tax evasion, and other emerging financial crime risks.

Through advisory, assessment, independent reviews, and operational support, we help you maintain regulatory compliance with applicable laws whilst safeguarding the reputation and integrity of your business.



How we support your Anti-Financial Crime framework

01

Financial Crime framework
We design and enhance financial crime frameworks that integrate AML/CFT, fraud risk management, anti-bribery & corruption, market abuse controls amongst others

02

Fraud Risk Management support
We help you design fraud prevention and detection controls, conduct fraud risk assessments, and support investigations with structured methodologies.

03

Anti-Bribery & Corruption programme
We develop ABC policies, risk assessments, due-diligence measures, and third-party screening frameworks to meet global anti-corruption standards.

04

Market Abuse & Conduct Risk controls
We help design and strengthen controls to prevent insider dealing, market manipulation, and other trading-related abuses.

05

Financial Crime monitoring & testing
We support onboarding and periodic reviews, conduct file remediation, and perform independent quality assessments across all financial crime domains.

06

Training & awareness
We deliver tailored financial crime training covering typologies, red flags, case studies, sanctions, ABC, market abuse, fraud, and emerging threats.

Our Anti-Financial Crime expertise

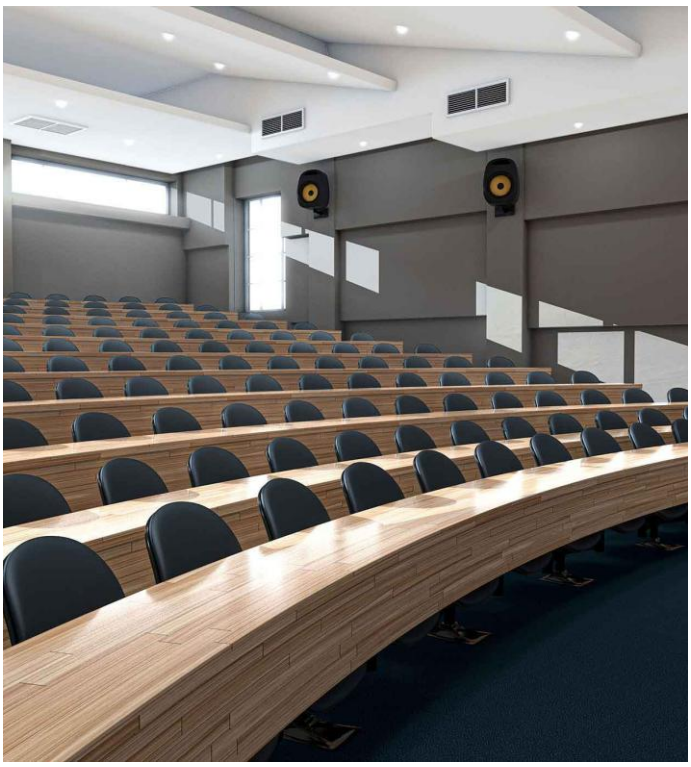
Specialist knowledge to support your requirements

- Financial crime regulatory frameworks and global standards
- ML/TF, proliferation financing, and complex financial-crime typologies
- Fraud risk assessments, fraud control design, and investigation support
- Anti-bribery and corruption (ABC) programmes and third-party due diligence
- Market abuse prevention, trading surveillance, and conduct risk controls
- Financial crime risk assessment methodologies (enterprise-wide and thematic)
- Customer lifecycle controls (CDD, EDD, periodic review, remediation)
- Transaction monitoring models, risk indicators, and alert investigation techniques
- Financial crime governance, roles, committees, and reporting frameworks
- Regulatory inspections preparation and remediation support

Board Effectiveness Review services

Effective boards and committees are critical to strong governance, strategic oversight, and long-term organisational resilience. Our Board Effectiveness Review Services are designed to help boards and committees evaluate how well they are functioning, identify areas for improvement, and enhance overall performance in line with regulatory expectations, governance best practice, and stakeholder expectations.

We conduct independent, structured, and proportionate board effectiveness reviews that assess board and committees' composition, dynamics, information flows, decision-making, and oversight arrangements. Our approach is practical and constructive, supporting boards in strengthening collective and individual performance while reinforcing transparency, accountability, and sound governance outcomes.



How we support your Board Effectiveness

01

Board and committee effectiveness assessments
We assess the effectiveness of the board and committees focusing on roles, responsibilities, decision-making processes, and governance outcomes.

02

Board composition and skills evaluation
We review board structure, diversity, independence, and skills mix against strategic objectives, regulatory expectations, and governance best practice.

03

Board dynamics and culture assessment
We evaluate board behaviours, interactions, challenge, and culture to identify factors that support or hinder effective discussion and decision-making.

04

Role clarity and governance frameworks
We assess clarity of roles between the board, committees, senior management, and key function holders to ensure effective oversight and accountability.

05

Information flows and reporting effectiveness
We review the quality, timeliness, and relevance of board and committee papers to support informed oversight and sound decisions.

06

Individual director assessments
Where required, we carry out confidential evaluations of individual directors' contributions, development needs, and ongoing suitability.

07

Action planning and follow-up support
We provide clear, prioritised recommendations and support implementation, including follow-up reviews to track progress and improvement.

Our Board Governance expertise

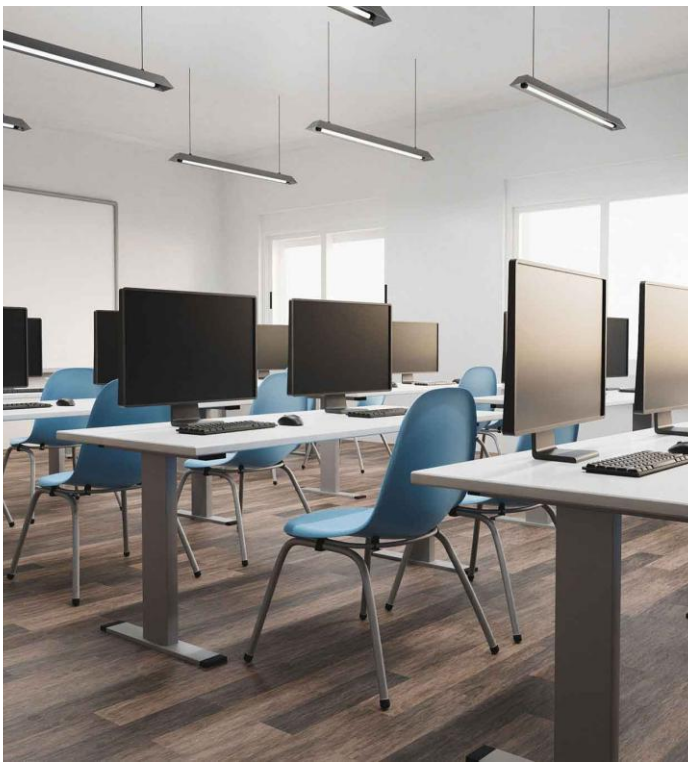
Specialist knowledge to support your requirements

- Board effectiveness reviews across financial and non-financial sectors
- Knowledge of corporate governance codes and regulatory expectations (including MFSA and EU frameworks)
- Board and committee role design and governance structures
- Board skills, succession, and diversity considerations
- Governance culture and behavioural risk considerations
- Practical, board-level reporting and action-oriented recommendations

Pay Transparency Directive services

The EU Pay Transparency Directive introduces enhanced obligations aimed at addressing gender pay gaps and strengthening transparency and fairness in remuneration practices. Our Pay Transparency Directive Services support organisations in understanding, implementing, and embedding these requirements into their existing remuneration, HR, and governance frameworks.

We provide practical, risk-based support to help organisations assess readiness, implement compliant processes, manage data and reporting obligations, and reduce exposure to legal, regulatory, and reputational risk, while supporting fair and transparent pay practices across the organisation.



How we support your Pay Transparency compliance

01

Directive readiness and gap assessment
We assess your current remuneration, HR policies, and data practices against Pay Transparency Directive requirements to identify gaps and risks.

02

Pay data mapping and analysis
We support the collection, structuring, and analysis of pay data, including gender pay gap calculations and pay level comparisons.

03

Remuneration and role framework review
We review job architecture, grading, and pay-setting practices to support objective, gender-neutral criteria and consistent application.

04

Policy and procedure development
We assist with the development or enhancement of remuneration, recruitment, and pay review policies aligned with Directive requirements.

05

Reporting and disclosure support
We support the preparation of mandatory disclosures and internal reporting, ensuring accuracy, consistency, and regulatory alignment.

06

Training and awareness
We deliver targeted training for management, HR teams, and relevant stakeholders to support consistent and compliant implementation.

Our Pay Transparency expertise

Specialist knowledge to support your requirements

- In-depth knowledge of the EU Pay Transparency Directive
- Gender pay gap analysis and remediation support
- Remuneration governance and controls
- Job evaluation and pay equity considerations

Enterprise Risk Management services: Building resilience and insight

Our Enterprise Risk Management Services help you build a resilient and proactive risk culture by identifying and managing the risks that could impact your operations, strategy, and long-term success. When needed, we can take on the responsibilities of the Outsourced Risk Management Function Holder, giving you an independent, expert-led risk function that strengthens oversight and supports strategic decision-making. Our approach ensures that risk governance, reporting, and controls are robust, forward-looking, and aligned with regulatory expectations.

How we strengthen your Risk Management framework

01

Outsourced Risk Management function holder
We oversee your risk management framework, ensuring risks are identified, assessed, monitored, and reported effectively across the organisation.

02

Risk identification & management
We help you identify, assess, and manage operational, strategic, and regulatory risks that may impact your organisation.

03

Incident & breach management
We support investigation, escalation, and recovery efforts when incidents occur, including root-cause analysis.

04

Third-Party Risk Management
We assess suppliers, outsourced partners, and vendors to strengthen oversight and ensure appropriate risk controls.

05

Reporting to the Board
We prepare clear and insightful risk dashboards, reports, and summaries for senior leadership.

06

Risk Management assessment
We evaluate the maturity and effectiveness of your risk framework, methodology, and governance arrangements

07

Training & awareness
We deliver risk-focused training to embed a strong risk culture across your organisation.

Our Risk Management expertise

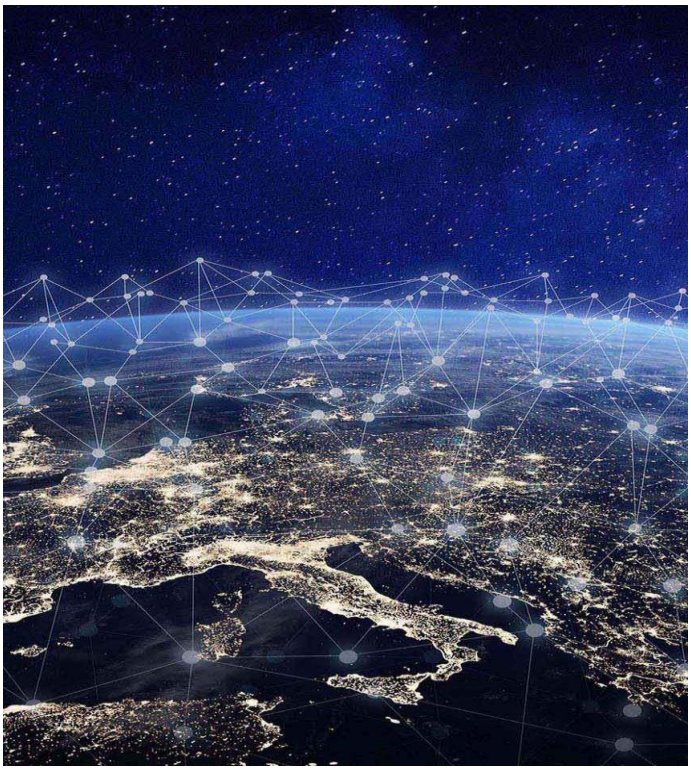
Specialist knowledge to support your requirements

- Risk frameworks and methodology design and evaluation
- Operational, strategic, financial, and regulatory risk assessment
- Risk governance, committee structures, and escalation models
- Third-party and outsourcing risk management
- Incident, breach, and root-cause analysis techniques
- Risk appetite development and embedding
- Risk reporting, dashboards, and board-level communication
- Control assessment and monitoring methodologies
- Maturity model assessments and capability benchmarking

Cybersecurity Governance & Compliance services

Our Cybersecurity Compliance Services support organisations in building resilient, secure, and regulatory-aligned environments. We provide structured governance, expert advisory support, and practical guidance across multiple regulatory frameworks, ensuring that controls, policies, and incident-response capabilities remain effective and aligned with best practice.

Our services cover leading standards and regulations, including ISO/IEC 27001:2022, DORA, NIST, NIS2, and sector-specific assurance requirements.



How we strengthen your Cybersecurity positioning

01

Cybersecurity advisory
We guide you through implementing and aligning with key cybersecurity frameworks including ISO27001, DORA, and NIS2.

02

Cybersecurity audit
We conduct independent and internal audits across ISO27001, DORA, NIST 2, and NIS2.

03

IT General Controls (ITGC) audit
We review your core IT controls to assess the effectiveness of access management, change management, and operational processes.

04

Gambling Commission audits
We perform MGA systems and compliance audits as well as UKGC security audits to ensure adherence to gaming regulatory requirements.

05

Point-of-Sale (POS) Security audits
We assess the security and reliability of POS environments, identifying weaknesses in payment processing and supporting infrastructure.

06

Gap analysis & preparedness assessments
We evaluate your current alignment with ISO/IEC 27001:2022, DORA, and NIS2 requirements, identifying deficiencies and defining clear remediation priorities.

How we strengthen your Cybersecurity positioning

07

IT maturity assessments
We assess the maturity of your IT environment to determine capability levels, improvement opportunities, and readiness for future resilience needs.

08

Basic penetration testing & vulnerability assessments
We conduct light-touch penetration testing and vulnerability assessments to identify security weaknesses and support timely remediation.

09

Co-Sourcing
We work alongside your internal teams to provide additional cybersecurity expertise, strengthening capacity while maintaining full organisational control.

10

Tailor-made IT Audits & gap assessments
We design and deliver customised IT audits and gap assessments aligned to your specific systems, risks, and regulatory obligations.

11

Register of Information (RoI) development and maintenance
We help you create and maintain your RoI in line with the requirements of the Digital Operational Resilience Act.

12

KnowBe4 partner
We implement and optimise the KnowBe4 platform while managing ongoing training, phishing simulations, and behavioural awareness initiatives.

13

Insight4GRC platform
We deploy and configure the Insight4GRC platform and provide ongoing management to ensure accurate data, effective reporting, and continuous compliance.

14

IT security & Compliance training
We deliver targeted IT security and compliance training for employees and Boards, ensuring clear understanding of responsibilities and emerging risks.

Our Cybersecurity expertise

Specialist knowledge to support your requirements

- ISO/IEC 27001:2022 gap assessments, internal audits, and implementation support
- DORA compliance, including RoI development, ICT risk management, and resilience testing
- NIST 2 audit services and compliance readiness
- NIS2 gap assessments and implementation guidance
- IT General Controls reviews and sector-specific audits (MGA, UKGC, POS)
- Tailor-made IT audit and assurance programmes
- Basic penetration testing and vulnerability assessments
- IT maturity assessments and co-sourcing models
- Policy, standard, and procedure development
- KnowBe4 implementation, configuration, management, and phishing simulations
- Insight4GRC platform implementation, configuration, and ongoing management
- Cybersecurity awareness, training, and Board-level education

Internal Audit Services

Our Internal Audit Services provide independent and objective assurance over your organisation's processes, controls, and governance arrangements. Whether you require targeted reviews or a fully outsourced Internal Audit Function, we deliver risk-based audits, actionable insights, and clear reporting to help you improve operational resilience and demonstrate strong oversight to regulators and stakeholders. Our approach supports transparency, accountability, and continuous improvement across your organisation.

How we deliver Internal Audit value

01

Managing and supporting your Internal Audit function
We provide Internal Audit Function holder services through outsourcing arrangements. Where required, we can also support your Internal Audit function through co-sourcing arrangements.

02

Internal Audit planning & execution
We deliver risk-based audits that evaluate the effectiveness of governance, operational, and compliance controls.

03

Remediation oversight
We verify that audit findings and recommendations are implemented fully and effectively.

04

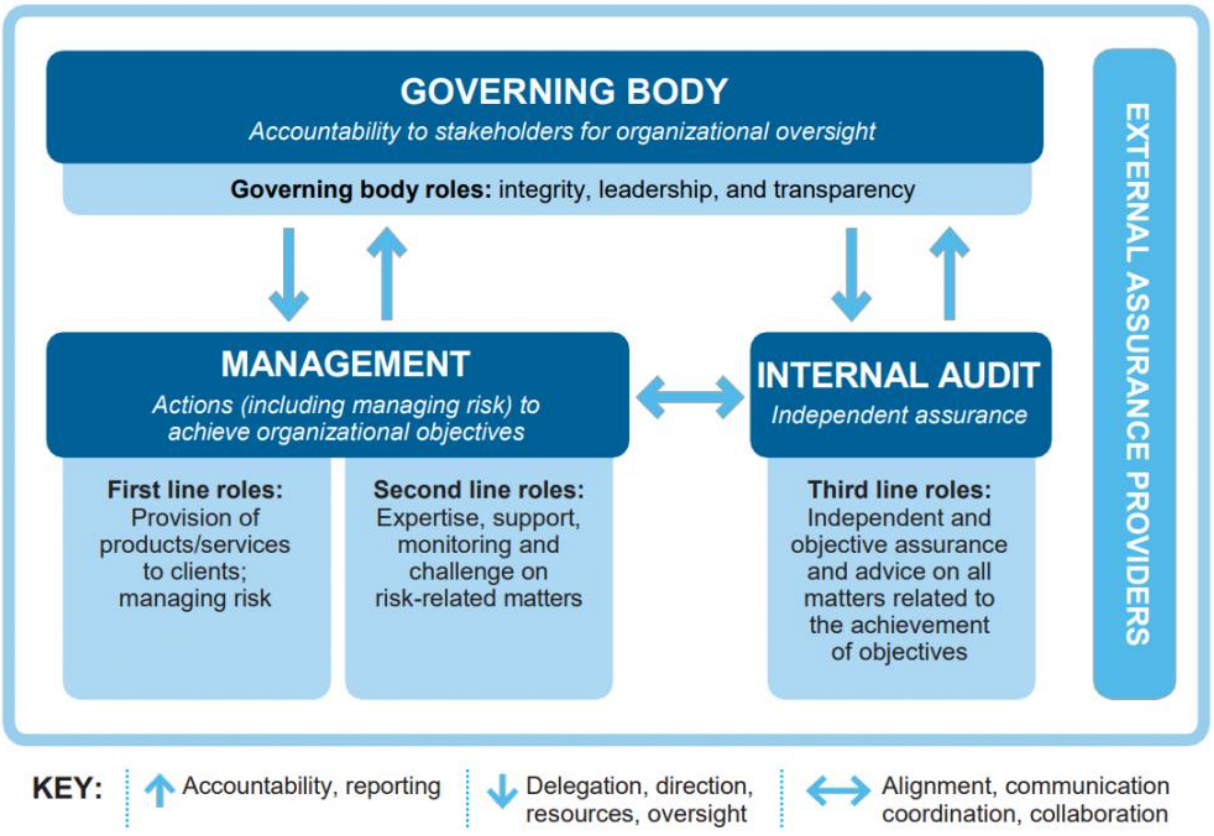
Thematic reviews
We conduct targeted deep-dive reviews into high-risk or emerging areas requiring enhanced scrutiny.

05

Internal Audit charter, policies & procedures support
We draft or enhance the Internal Audit Charter, policies, and procedures to ensure clarity, independence, methodological consistency, and alignment with leading practice

Our Internal Audit methodology

- Our approach is predicated on the need to understand your business strategy and objectives, and what key stakeholders consider to be valuable.
- This methodology enables us to proactively plan, develop, deliver and measure the value we generate as your internal auditors.
- RSM International has developed an internal audit methodology that is based on the Institute of Internal Auditors' framework and standards. We adopt a risk-based approach which adapts to diversities at each respective company that will enable us to produce a composite internal audit plan. In this regard, our methodology focuses on processes and covers the various risks exposures at company level. Such methodology seeks to reinforce the responsibilities of management and the board for managing risk. Generally, the primary process owners are more easily identifiable. It also enables us to consider the risks managed by different owners throughout the relevant process flow.
- The approach is built on the three lines of defence concept with risk and controls being owned by the operations and a second and third line of defence in place to support and monitor implementation and execution.



Our Internal Audit expertise

Specialist knowledge to support your requirements

- Expertise across sectors including financial services, gaming, and listed entities
- Risk-based internal audit methodology and execution
- Governance, operational, IT, and compliance control assessment
- Thematic, deep-dive, and investigative reviews
- Audit planning, scoping, and annual planning cycles
- Audit charter development and enhancement
- Continuous follow-up tracking and validation
- Reporting for boards, audit committees, and senior leadership
- Internal audit effectiveness and maturity assessments

The Team

Gordon Micallef

Principal – GRC Advisory

E: gordon.micallef@rsm.com.mt

M: +356 99451641

Gordon Micallef is a Principal at RSM Malta with a background in IT auditing and governance, bringing over 24 years of experience integrating technology with business strategies. He lectures at the University of Malta and was a founding director of ISACA Malta, later serving on its international committee.

Gordon has led large-scale, complex projects across utilities, transport, and regulated industries, combining financial and technology expertise to deliver actionable solutions. His pragmatic, hands-on approach reflects RSM's values of efficiency, relevance, and integrity, and his leadership fosters professional growth and development across teams.

Dr Roberta Buhagiar

Director – GRC Advisory

E: roberta.buhagiar@rsm.com.mt

M: +356 79092590

Roberta holds a Doctor of Laws degree and is a warranted lawyer with extensive experience in regulatory compliance and corporate governance. Having started her legal career in 2008 as a litigation lawyer, she eventually specialised in regulatory compliance and led the legal and compliance function for insurers transacting both local and cross-border business. Before joining RSM Malta as GRC Director, she led the Regulatory Services division at a Governance, Risk, and Compliance (GRC) service provider, where she also served as Compliance Officer for both the firm and a diverse range of clients, including insurance intermediaries, fund managers, and investment firms.

Ruth Esposito

Manager – Regulatory Compliance

E: ruth.esposito@rsm.com.mt

M: +356 79011713

Ruth Esposito is a Manager in RSM Malta's Regulatory Compliance team, specialising in AML/CFT, data protection, compliance, risk management, and governance. She oversees client projects and delivers training to strengthen organisational resilience.

With nearly a decade of experience, Ruth previously held a senior role at Grant Thornton Malta and started her career with one of the Big 4 audit firms. She also has international exposure in Newcastle (UK) and London (UK). Ruth holds an MSc in Security Management, a BA (Hons) in Criminology, and an MQF Level 5 Certificate in AML/CFT, providing clients with practical and risk-focused compliance guidance.

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM Malta
Mdina Road
Ħaż-Żebbuġ, Malta
ZBG 9015
T +356 2278 7000
www.rsm.com.mt