TORAGUARD

0330 024 6060 | info@toraguard.com
www.toraguard.com

A STRATEGIC GUIDE FOR UK INVESTMENT MANAGEMENT FIRMS.

Integrating Cybersecurity into Enterprise Governance, Risk and Compliance.

A holistic approach to managing cybersecurity risks efficiently and effectively.

READY TO GROW YOUR FIRM WITH CONFIDENCE?

Cybersecurity GRC, done right, can help you:

Gain confidence your cybersecurity risks are being managed with similar rigour and transparency as financial and operational risks.

Empower your board and senior leadership to make informed decisions on cybersecurity risk.

Reduce the risk of incidents by embedding cyber security into your organisation's core governance and compliance activities.

Save time and reduce complexity by automating repetitive GRC tasks, freeing up resources for strategic initiatives.

Stay ahead of regulatory scrutiny by aligning with FCA, GDPR, and operational resilience requirements.

Build trust with clients, regulators, and partners by showing that cybersecurity is a visible part of your risk management culture.

If you are already thinking about how to achieve the outcomes above, then you are on the right track.

Read on for more on how Cybersecurity GRC can build internal and external stakeholder confidence in the operating model that supports your business strategies.

Why Cybersecurity GRC matters for your firm?

Cybersecurity risk is increasingly becoming a fundamental component of enterprise risk and board-level decision-making.

While many firms have made strides in traditional GRC areas, such as financial risk and regulatory compliance, cybersecurity often remains siloed or insufficiently embedded in enterprise governance structures. This fragmentation creates blind spots that can be exploited by increasingly sophisticated threat actors.

In the investment management industry, where data integrity, client trust, and regulatory scrutiny are paramount, the stakes are particularly high. A breach not only endangers sensitive information but also risks reputational damage, regulatory penalties, and loss of investor confidence. Firms must therefore develop a unified approach to managing cyber risks, treating them with the same strategic attention as any other core business risk.

We proffer a comprehensive exploration of Cybersecurity GRC, tailored for senior decision-makers in the investment management sector. It demystifies key concepts, outlines regulatory imperatives (including FCA and GDPR), and presents practical guidance on aligning cybersecurity with enterprise risk frameworks. Drawing on deep industry experience, we highlight how a measured, value-driven approach enables firms to mature their cyber posture while supporting business objectives.

In an increasingly digitised and regulated environment, investment management firms all over the world, face a growing need to integrate cybersecurity into their broader Governance, Risk and Compliance (GRC) strategies. As cyber threats evolve in sophistication and regulatory expectations become more demanding, firms must adopt a proactive, business-aligned approach to cybersecurity risk.

WHY CYBERSECURITY GRC MATTERS FOR YOUR FIRM?

This whitepaper presents:

A sector-specific overview of cyber risks faced by UK investment managers.

Regulatory mandates from the FCA, GDPR, and voluntary standards such as Cyber Essentials and ISO 27001.

A framework for integrating cybersecurity into enterprise GRC programs.

Real-world insights from consulting engagements, including a detailed case study.

A maturity model to benchmark and advance your firm's Cyber GRC capability.

We explore how cybersecurity intersects with other pillars of operational resilience, including business continuity, third-party risk management, and ESG reporting. By bridging gaps between technical teams and senior leadership, this approach fosters a culture of accountability, continuous improvement, and strategic alignment.

Key takeaways:

Cybersecurity goes beyond an IT issue; it's a board-level risk and compliance matter.

Investment management firms can save time and money by addressing cybersecurity risks through integrated GRC strategies.

A robust Cybersecurity GRC framework helps firms mitigate risk, stay compliant and build trust with clients and regulators.

Practical integration requires cross-functional collaboration, executive sponsorship, and continuous improvement.

Our aim is to equip readers with practical, actionable insights, whether they are CISOs advocating for GRC alignment or COOs and CROs seeking clarity on cyber risk in the broader enterprise context. In doing so, we reflect the core values of our firm: deep expertise, trusted partnerships, and measured value.

THE CASE FOR ACTION.

Relevant Industry Statistics.

To underscore the urgency and value of Cybersecurity GRC integration, consider the following:

300x

Financial services organisations are 300 times more likely than other companies to be targeted by a cyber attack.

$5.9 m

The average cost of a data breach in the financial sector. This is £1.5 million above the global average of $4.45 million.

$1 m

The ransom amount paid by nearly 39% of financial institutions that experienced ransomware attack in 2023.

4x

In 2023, firms that had mastered cybersecurity were nearly four times better at stopping breaches.

Cybersecurity threats are now among the top risks facing investment management firms. From ransomware to data exfiltration, the threat landscape demands that cybersecurity be embedded in enterprise risk management. This paper explores how firms can integrate cybersecurity considerations into their GRC frameworks to meet regulatory demands and strengthen operational resilience.

UNDERSTANDING CYBERSECURITY GRC IN THE INVESTMENT MANAGEMENT CONTEXT.

Cybersecurity GRC refers to the integration of cybersecurity governance, risk management, and compliance practices into an organisation's broader enterprise risk framework. Rather than being siloed in the IT department, cyber risk becomes a shared responsibility that is monitored, managed and aligned with the firm's operational and strategic objectives.

When cybersecurity is integrated into GRC, it means cyber threats are not treated as isolated technical glitches, but as enterprise-wide risks that can materially impact client trust, operational continuity, and regulatory standing.

For investment firms, this translates into embedding cyber risks into your ERM systems, assigning oversight at the board and executive levels, ensuring that controls map to FCA, GDPR, and ISO 27001 frameworks, and regularly testing your ability to detect, respond to, and recover from incidents.

"Firms that integrate cybersecurity into ERM well, end up creating a culture where security is embedded in decision-making, gaining a competitive edge in due diligence processes and building credibility with clients."
– Gerrad Olisa-Ashar, Director Strategic Growth and Partnerships

The championship golf course analogy for Cybersecurity GRC.

GRC FUNCTION	CHAMPIONSHIP GOLF COURSE ANALOGY	GRC FOR INVESTMENT MANAGEMENT FIRMS
Governance	The club's leadership setting the rules of play, membership standards, and long-term vision for the course.	The Board sets the tone at the top and determines the firm's risk appetite and cybersecurity standards necessary to support the long-term vision of the firm.
Risk	The course superintendent and marshals monitoring hazards like storm damage, diseased greens, or overcrowding and deciding which to prevent, mitigate or accept.	The CEO, supported by the Executive team, determining the appropriate strategies for identifying, prioritising, and managing cybersecurity risk.
Compliance	Meeting external requirements from governing bodies, regulators, and safety authorities; from R&A rules in tournaments to health and safety standards.	Activities carried out by senior leadership, to ensure that the firm has and maintains a strong regulatory standing with appropriate bodies like the FCA and ICO.

Just as a golf club's reputation depends on the quality, safety, and governance of its course, an organisation's resilience depends on how well it embeds Cybersecurity GRC. Without governance, play becomes chaotic. Without risk management, hazards become crises. Without compliance, the course could lose its licence to operate. Together, Cybersecurity GRC ensures the 'course', your business, is trusted, resilient, and prepared to perform under pressure.

Cyber risk in the Investment Management context.

Investment managers operate in a highly interconnected and regulated environment. Their business models rely on the trust of clients, the confidentiality and availability of financial data, and the seamless functioning of digital platforms. This makes them uniquely vulnerable to a range of cybersecurity threats.

Moreover, the increasing adoption of cloud infrastructure, remote work arrangements, and API-based connectivity with clients and partners has expanded the attack surface. These dynamics require investment firms to reframe cybersecurity not just as an IT control, but as an enterprise-wide concern that needs formal governance, monitoring, and integration into decision-making.

Key industry-specific cyber risks include:

THIRD-PARTY RISK.
Investment firms often rely on a complex ecosystem of custodians, fund administrators, cloud service providers, and data vendors. A breach or disruption at a third-party can have direct operational and regulatory consequences.

DATA EXFILTRATION AND IP THEFT.
Sensitive trading algorithms, client portfolios, and research data are high-value targets for cybercriminals and nation-state actors.

INSIDER THREATS.
Whether malicious or accidental, insiders with privileged access can introduce significant risk, particularly in firms with flat hierarchies or weak segregation of duties.

EMAIL COMPROMISE AND SOCIAL ENGINEERING.
Phishing attacks targeting senior executives or client relationship managers can lead to fraudulent fund transfers or data loss.

RANSOMWARE.
Ransomware incidents have evolved into board-level risks. Beyond the immediate disruption, ransomware incidents can halt client services, erode investor trust, and invite regulatory scrutiny.

Regulatory landscape for UK Investment Managers.

The regulatory bar is also rising. The FCA now expects firms to demonstrate operational resilience, including the ability to prevent, respond to, recover, and learn from disruptions.

Cybersecurity is a cornerstone of this resilience. Firms must therefore be prepared to evidence their control effectiveness, incident response plans, and governance structures in supervisory discussions.

UK investment managers must embed cybersecurity deeply into their GRC frameworks, not only to meet regulatory obligations, but to maintain credibility with investors, clients, and partners in an increasingly scrutinised digital and sustainability-driven environment.

Crucially, investors and boards are becoming more discerning. Cyber maturity is increasingly seen as a proxy for good governance and long-term viability. Asset owners and fund selectors may now ask about cybersecurity posture during due diligence.

"Investment management firms are getting the message and evolving their approach from reactive compliance to proactive cyber risk governance. This evolution begins with integrating cybersecurity into the firm's GRC architecture."

– George Wood, Director Cybersecurity Services

REGULATORY LANDSCAPE FOR UK INVESTMENT MANAGERS.

FCA REQUIREMENTS: SYSC RULES AND OPERATIONAL RESILIENCE.

The Financial Conduct Authority (FCA) holds firms to high standards of operational integrity under its Senior Management Arrangements, Systems and Controls (SYSC) sourcebook. SYSC 3.2 and SYSC 13 require firms to establish sound risk management systems and appropriate IT controls to mitigate operational and cyber risks.

In addition, the FCA's Operational Resilience framework mandates that firms identify important business services, set impact tolerances, and demonstrate their ability to continue delivery through severe disruptions, including cyber incidents. Cybersecurity is a fundamental component of both resilience testing and scenario planning.

GDPR AND DATA PROTECTION ACT (2018).

Firms must comply with the UK GDPR and the Data Protection Act, which mandate appropriate technical and organisational measures to protect personal data.

Key provisions include data breach reporting within 72 hours, data minimisation, secure processing, and clear accountability through data protection officers or equivalent roles. Investment firms processing client, employee, or third-party data are expected to demonstrate proactive data governance and incident response capabilities.

UK CYBER RESILIENCE ACT (PROPOSED).

The upcoming UK Cyber Resilience Act aims to enhance national cybersecurity standards, particularly for digital products and services. Although still in draft stages, this legislation is expected to introduce mandatory cybersecurity requirements for software and connected devices, with implications for investment managers using digital platforms and third-party solutions.

The Act will likely include provisions for vulnerability management, secure development practices, and vendor accountability. Firms should begin preparing by conducting a cybersecurity impact assessment on all digital assets and staying engaged with regulatory consultations as the framework evolves.

UK CYBER ESSENTIALS AND ISO 27001.

While not mandated, these frameworks provide a recognised baseline for cybersecurity maturity and can be referenced in regulatory, due diligence, and client conversations.

Cyber Essentials focuses on basic controls (e.g., patching, access management), whereas ISO 27001 is a broader standard encompassing governance, risk, and control management under an Information Security Management System (ISMS). Adoption signals a firm's commitment to best practices and ongoing risk reduction.

Building a robust Cybersecurity GRC Architecture.

What a good GRC Framework looks like:

GOVERNANCE.

Defining Roles, Responsibilities, and Reporting Lines

Effective cybersecurity governance starts with clear accountability. Boards and executives must ensure that roles and responsibilities are well-defined across business, IT, and security functions. A formal governance structure establishes reporting lines from operational teamsthrough senior management to the Board, providing visibility and oversight. This ensures cybersecurity decisions are business-aligned, risk-informed, and consistent with the organisation's strategic objectives.

RISK MANAGEMENT.

Integrating Cyber Risk into Enterprise Risk Management (ERM)

Cyber risk should not be managed in isolation. Embedding it within enterprise risk management processes ensures it is assessed alongside financial, operational, and strategic risks. Maintaining a centralised risk register that includes cyber threats enables Boards and executives to understand exposure, prioritise investments, and track remediation. This integration shifts cybersecurity from a purely technical concern to a core business risk with measurable impact on resilience, reputation, and regulatory compliance.

BUILDING A ROBUST CYBERSECURITY GRC ARCHITECTURE.

COMPLIANCE MANAGEMENT.

Mapping Regulatory Obligations to Control Environments

Financial regulators, data protection authorities, and industry bodies impose complex requirements on firms. An effective GRC framework translates these regulatory obligations into practical control environments that can be monitored and evidenced. This mapping enables executives to demonstrate compliance to regulators, clients, and investors while avoiding duplication and inefficiency. By linking compliance activities directly to business risks and controls, organisations create a more efficient, defensible, and resilient posture.

CONTROLS & MONITORING.

KPIs, KRIs, Audits, and Threat Intelligence

Executives require meaningful insights to oversee cyber resilience. This is achieved by defining key performance indicators (KPIs) and key risk indicators (KRIs) that measure the effectiveness of security controls. Internal audits provide independent assurance, while real-time threat intelligence enables proactive adjustment of defences. A mature controls and monitoring function ensures the Board receives accurate, timely, and actionable reporting, helping leadership steer the organisation with confidence in the face of evolving threats.

INCIDENT MANAGEMENT.

Response Planning Aligned with Business Continuity

Even the best defences cannot eliminate all cyber threats. A tested and well-structured incident response plan ensures the organisation can act decisively when incidents occur. Alignment with business continuity and crisis management processes allows executives to maintain operations, protect critical assets, and communicate effectively with regulators, clients, and stakeholders. By rehearsing these scenarios through simulations and table-top exercises, Boards and leadership teams can gain assurance that the organisation is prepared to respond and recover at speed.

10 Steps to integrating Cybersecurity into GRC architecture.

STEP.	KEY TEAMS INVOLVED.	INPUTS.	OUTPUTS.
01. Align leadership.	Board, Executive, Operational Resilience, Technology, Risk and Compliance.	Board Priorities, Business Strategy, Regulatory Expectations, SMCR Accountability.	Shared Vision, Executive Sponsorship, Defined Accountability for Cyber Risk and Compliance.
02. Conduct a cyber risk landscape review.	Operational Resilience, Technology, Risk and Compliance.	Threat Intelligence, Peer/Industry Benchmarks, Regulator Insights, Emerging Technology Risks.	Current and Emerging Risk Profile, Prioritised Risk Themes, Alignment to Business Impact.
03. Assess current GRC capabilities.	Operational Resilience, Technology, Risk and Compliance.	Risk Register, Regulatory Obligations, Incident & Resilience Plans, Audit Findings, Independent Reviews.	Capability Maturity Baseline, Gap Analysis, Strengths and Weaknesses Summary.
04. Define a cyber GRC strategy and target operating model.	Board, Executive, Operational Resilience, Technology, Risk and Compliance.	Business Objectives & Risk Appetite, Capability Assessment, Regulatory Expectations, Technology Landscape, Stakeholder Views.	Cyber GRC Strategy, Target Operating Model, Clarified Roles & Responsibilities, Updated Control Framework, GRC Roadmap.
05. Update governance structures.	Board, Executive, Operational Resilience, Technology, Risk and Compliance.	Existing Committees, Reporting Lines, Policy Framework, Escalation Processes.	Revised Committee Structures, Clear Reporting Flows, Updated Policies and Standards.

10 STEPS TO INTEGRATING CYBERSECURITY INTO GRC ARCHITECTURE.

STEP.	KEY TEAMS INVOLVED.	INPUTS.	OUTPUTS.
06. Integrate into risk registers and reporting.	Technology, Risk and Compliance.	Enterprise Risk Framework, Board Reporting Templates, Current KPIs/KRIs.	Cyber Risks Embedded in Enterprise Risk Register, Enhanced Reporting Dashboards, Risk Appetite Alignment.
07. Enhance compliance mapping and monitoring.	Technology, Risk and Compliance.	Regulatory Rulebooks (FCA, PRA, GDPR, ESG), Compliance Testing Plans, Audit Reports.	Mapped Obligations to Controls, Monitoring Framework, Evidence Packs for Regulators/Clients.
08. Test and refine.	Operational Resilience, Technology, Risk and Compliance.	Incident Response Playbooks, Continuity Plans, Simulation Exercises, Audit Feedback.	Lessons Learned Reports, Refined Playbooks, Validated Response and Recovery Capabilities.
09. Sustain and evolve.	Board, Executive, Operational Resilience, Technology, Risk and Compliance.	Performance Data (KPIs/KRIs), Threat Intelligence, Regulatory Updates, Technology Change Pipeline.	Continuous Improvement Cycle, Updated Strategy and Controls, Proactive Regulatory Alignment.
10. Embed into culture.	Board, Executive, Operational Resilience, Technology, Risk and Compliance.	Training And Awareness Programmes, Employee Surveys, Leadership Tone, HR Processes.	Risk-Aware Culture, Improved Staff Accountability, Measurable Uplift in Cyber Behaviours.

Supporting the case for Cybersecurity GRC.

"Cyber security is not just an IT concern – it is a business-critical risk. I urge all board members to engage with the Cyber Governance resources."

– RICHARD HORNE, CEO, UK NCSC.

"Operational resilience should be a point of consideration for boards and executives when planning major change programmes or making strategic business decisions."

– PRUDENTIAL REGULATION AUTHORITY (PRA) SUPERVISORY LETTER.

"The time is now for CEOs and boards to actively embrace corporate cyber responsibility as a matter of good governance."

– JEN EASTERLY, THEN-DIRECTOR, CISA.

"With cyber attacks becoming more frequent, harmful and costly, cyber resilience is now a crucial boardroom responsibility."

– DR ERIN YOUNG, INSTITUTE OF DIRECTORS.

Tooling and automation for cybersecurity GRC integration.

Technology is a critical enabler for integrating cybersecurity into GRC programs. The right tooling provides scalability, transparency, and consistency across core governance processes. For investment managers, automation helps overcome resource constraints and enhances assurance.

Tool selection should be guided by business needs, integration capabilities, and the firm's maturity level. Importantly, tooling should support—not dictate—the firm's governance processes. Adoption requires upfront investment in change management, data governance, and user training.

Key tooling areas include:

INTEGRATED GRC PLATFORMS.

Platforms like RSA Archer, ServiceNow GRC, and MetricStream allow centralised management of risk registers, control frameworks, compliance mapping, policy lifecycle, and audit workflows.

CYBER RISK QUANTIFICATION TOOLS.

Tools such as FAIR (Factor Analysis of Information Risk) support quantitative risk assessment by assigning financial values to cyber threats, improving business decision-making.

VULNERABILITY MANAGEMENT & THREAT INTELLIGENCE.

Integration of tools like Tenable, Rapid7, and Mandiant provides real-time visibility of the threat landscape, which can feed into risk registers and board reporting.

WORKFLOW AUTOMATION.

Automation of control testing, evidence collection, exception handling, and incident response (e.g. via SOAR tools) reduces manual effort and increases auditability.

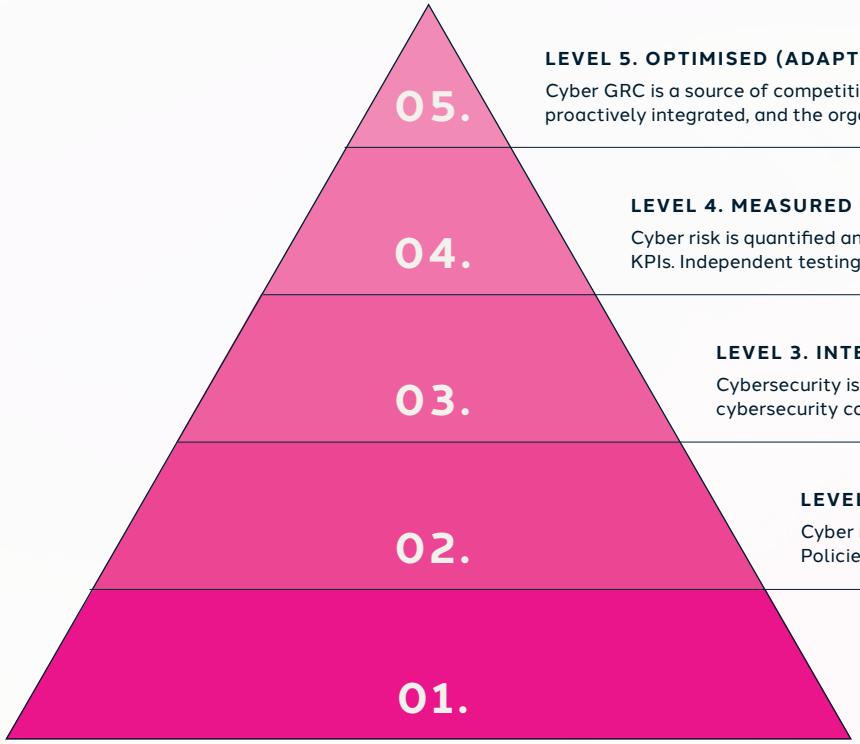
THIRD-PARTY RISK PLATFORMS.

Tools such as FortifyData, KYND, and BitSight help assess and monitor the cybersecurity posture of vendors and counterparties, supporting third-party risk management efforts.

DASHBOARD & REPORTING TOOLS.

Business intelligence platforms like Power BI and Tableau can visualise KRIs and KPIs, enhancing executive-level insight and oversight.

Maturity model for Cyber GRC.



LEVEL 5. OPTIMISED (ADAPTIVE AND STRATEGIC)

Cyber GRC is a source of competitive advantage. Lessons learned are institutionalised, threat intelligence is proactively integrated, and the organisation continuously adapts its strategy to the evolving risk landscape.

LEVEL 4. MEASURED (DATA-DRIVEN)

Cyber risk is quantified and monitored using performance metrics and analytics. Board reporting includes cyber KPIs. Independent testing and third-party audits validate control effectiveness.

LEVEL 3. INTEGRATED (MANAGED AND ALIGNED)

Cybersecurity is embedded into enterprise GRC frameworks. Risk and compliance teams collaborate, and cybersecurity controls are mapped to business objectives and regulatory requirements.

LEVEL 2. DEFINED (REPEATABLE PRACTICES)

Cyber risk assessments occur periodically, with some coordination between risk, compliance, and IT teams. Policies exist but may not be fully enforced. Regulatory compliance is pursued tactically.

LEVEL 01. INITIAL (AD HOC)

Cybersecurity and GRC activities are uncoordinated. Risk assessments are informal, and responses are reactive. Governance structures are weak or absent.

Progressing through these levels typically requires executive buy-in and consistent messaging, technology investment in GRC tools and security monitoring platforms, training and upskilling of staff, and ongoing refinement of governance structures. This model can be used as a diagnostic tool during maturity assessments or strategic planning sessions, as well as a way to communicate progress to the board and other stakeholders.

Cybersecurity GRC case study.

Elevating cyber risk to the board.

CHALLENGE.

In 2020, a medium-sized investment manager (£5bn AUM) needed assurance that cybersecurity risks were being effectively governed. Despite solid IT practices, cyber risk was managed purely as a technology issue, leaving the Board without the visibility or oversight to address it as a strategic business risk.

SOLUTION.

Working with the firm's leadership team, cybersecurity was integrated into its governance, risk, and compliance framework. This included mapping regulatory obligations, embedding cyber risks into the enterprise risk register, establishing Board-level reporting, and aligning incident response plans with business continuity.

OUTCOME.

Cybersecurity is now treated as a core business risk with direct Board oversight. The leadership team has clear visibility of exposures, assurance over regulatory compliance, and confidence that the firm is resilient against evolving threats, supporting both investor trust and long-term business growth.

Conclusion.

Cybersecurity GRC is not a one-time project but an ongoing organisational journey. For business and security leaders, (CEOs, Boards, CISOs, COOs, etc.) this means recognising that cyber resilience must evolve in parallel with business strategy, regulatory change, and the shifting threat landscape. Success requires long-term commitment, not just from technology teams but across leadership and the wider enterprise.

New regulatory obligations, advances in digital services, and emerging attack vectors demand that firms continuously reassess their governance, risk and compliance capabilities. A static approach quickly becomes obsolete; a dynamic framework ensures controls, processes and reporting remain relevant and effective.

Collaboration is equally critical. Cybersecurity is a shared responsibility spanning business functions, third parties, and regulators. Investment managers who embed a culture of partnership between the Board, operational leaders, and external stakeholders are better positioned to manage risks proactively and demonstrate resilience to clients and investors.

By adopting an integrated GRC approach, UK investment management firms can strengthen protection of their assets and information, enhance trust and assurance for stakeholders, and meet regulatory expectations with confidence. Importantly, this does not mean sacrificing agility or innovation; rather, it ensures that digital transformation and business growth are underpinned by resilience, accountability, and strategic foresight.

CONCLUSION.

Start or enhance your Cybersecurity GRC journey by:

ESTABLISHING A CYBER GRC STEERING COMMITTEE.

PRIORITISING CYBER RISKS ALONGSIDE FINANCIAL AND OPERATIONAL RISKS.

CONDUCTING MATURITY ASSESSMENTS AND BENCHMARK AGAINST PEERS.

INVESTING IN EDUCATION AT ALL LEVELS, FROM BOARD TO FRONT-LINE STAFF.

Executive Call-to-Action: Questions for the Boardroom

To move from theory to practice, Boards and executives should challenge their organisations with the following questions:

1. GOVERNANCE

Do we have clear accountability for cybersecurity at Board and executive levels, with regular reporting that informs decision-making?

2. RISK MANAGEMENT

Is cyber risk fully integrated into our enterprise risk framework, and do we understand our most material exposures?

3. COMPLIANCE

Can we demonstrate that our control environment meets regulatory obligations in a defensible and efficient way?

4. CONTROLS & MONITORING

Do we receive timely, business-relevant metrics (KPIs and KRIs) that give assurance over our cyber resilience?

5. INCIDENT MANAGEMENT

Have we tested our response and recovery capabilities, and can we operate effectively under a real-world cyber crisis?

6. CULTURE

How are we embedding cybersecurity awareness and accountability into our organisational DNA, from the Boardroom to front-line teams?

By addressing these questions, leaders signal to regulators, investors, and clients that cybersecurity risk management is not siloed, and has the strategic visibility necessary to effective. Firms that act now position themselves to demonstrating resilience, trustworthiness, and operational excellence in a competitive marketplace.

TORAGUARD

ABOUT TORAGUARD.

ToraGuard is a boutique cybersecurity GRC consultancy dedicated to helping UK investment management firms align cybersecurity with enterprise goals. Through deep expertise, trusted partnerships and a commitment to measured value, we guide clients in building resilient and compliant businesses.

FOR ADDITIONAL GUIDANCE, CONTACT:

Gerrad Olisa-Ashar
Director Strategic Growth and Partnerships

gerrad.olisa-ashar@toraguard.com

George Wood
Director Cybersecurity Services

george.wood@toraguard.com