Insight's Governance, Risk and Compliance (GRC) capabilities overview

Insight.

Introduction

In simple terms, GRC is about building trust - trust with your customers, trust with regulators, and trust within your own organisation that you are operating responsibly and resiliently.

Key Pillars of GRC:

1 Governance

Setting the tone from the top of the organisation, and turning this into clear policies. This is leadership's commitment to doing things the right way - from data ethics to corporate accountability. Strong governance means your teams have a compass for decision-making aligned with your business goals and values.

2 Risk Management

Identifying what could go wrong (from accidental data loss to ransomware attacks) and proactively mitigating it. It's about predicting what might happen and being prepared. Companies that manage risk well have fewer crises, and when issues arise, they handle them swiftly and effectively. You gain confidence to take strategic bets because you've hedged against the downside.

3 Compliance

Playing by the rules – whether laws like GDPR, industry standards like ISO, or internal codes of conduct. This isn't just to "make regulators happy"; it's to assure your customers and partners that you take security and privacy seriously. Compliance builds trust and opens doors – for example, being certified (e.g. ISO 27001) can be a ticket to do business with top clients who demand proof of good practices.

The business case for GRC

Neglecting governance, risk management, or compliance can expose an organisation to severe consequences:

- **Financial Loss:** Data breaches, fraud, or regulatory penalties can result in direct financial costs – fines, legal fees, breach remediation expenses – as well as lost revenue from business disruption. Notably, studies show non-compliance costs companies far more than the cost of compliance.
- **Operational Disruption:** Unmanaged risks (like cyberattacks or process failures) can halt operations and cause downtime, hurting productivity and service delivery. For example, a ransomware attack could lock up critical systems for days. GRC practices help identify and mitigate such risks before they materialize, preserving business continuity.
- **Reputational Damage:** Trust is hard to earn and easy to lose. Compliance failures or ethical lapses erode customer and stakeholder trust. A publicized data breach or compliance scandal can tarnish a brand for years, leading customers to flee. Strong governance and compliance demonstrate to the public, partners, and regulators that the organisation is responsible and trustworthy.
- **Regulatory Penalties:** Regulators are increasingly enforcing laws with heavy fines and even criminal penalties for non-compliance. For instance, under the EU's GDPR, fines can reach up to €20 million or 4% of global annual turnover for serious violations

In fact, regulators in Europe have handed out €5.88 billion in GDPR fines since 2018, including a record €1.2 billion fine against a single company GRC helps ensure all required controls and reporting are in place to avoid these penalties.

In summary, investing in GRC is far cheaper and safer than dealing with the fallout of compliance failures or major incidents. A cohesive GRC program protects the organisation's **financial health, operational continuity, and public reputation**, while also enabling better decision-making and strategic alignment. As one study succinctly put it, *"noncompliance costs nearly three times as much as compliance"*

On average, organisations spend $5.47M annually on compliance, but $14.82M when falling out of compliance – non-compliance cost is about 2.7 times higher. These losses include business downtime, incident response, and customer churn.

Key Frameworks and Regulations

In the GRC landscape, there are many standards, frameworks, and regulations that organisations may need to follow. Below is an overview of major ones – what they are, and how they apply to different organisations:

Framework / Regulation	Purpose	Applicability	Key GRC Implications
ISO/IEC 27001	Establishes an Information Security Management System (ISMS) to systematically secure information.	All industries globally (finance, tech, manufacturing, etc.).	Baseline for cybersecurity governance; often overlaps with NIS2 and other frameworks. Certification demonstrates strong security posture.
Cyber Essentials Plus	UK government-backed scheme for basic cyber hygiene via five key controls.	UK-based businesses, especially SMEs and suppliers to government.	Provides assurance of essential protections. Independent audit required for "Plus" level. Often an entry point into structured security.
CAF (Cyber Assessment Framework)	Developed by the UK's NCSC, CAF provides a structured approach to assess the cyber resilience of organisations operating critical functions.	UK organisations in critical national infrastructure (CNI) sectors and operators of essential services, particularly under UK NIS regulations.	Aligns technical controls with governance outcomes. Helps demonstrate maturity against NIS-aligned principles. Supports risk-based decisions and regulatory dialogue. Often used alongside ISO 27001 or internal assurance.
EU AI Act	EU legislation governing AI systems by risk category (e.g. high-risk systems like credit scoring).	Any organisation offering AI into the EU market.	High-risk AI requires documentation, risk management, and ongoing oversight. Strong AI governance helps ensure compliance and market access.
NIS2 Directive	EU-wide cybersecurity rules for critical and digital infrastructure.	Medium–large entities in key sectors (energy, telecoms, cloud, manufacturing, healthcare, etc.) including non-EU providers serving the EU.	Requires risk-based security, incident reporting, supply chain security. Penalties align with GDPR-level fines. Overlaps with ISO 27001 significantly.

Framework / Regulation	Purpose	Applicability	Key GRC Implications
GDPR	EU regulation for handling personal data—consent, privacy rights, breach notification, etc.	Any organisation processing EU residents' personal data.	Data protection becomes a board-level issue. Requires strong governance, data inventories, DPOs, and rapid breach reporting. Significant fines for non-compliance.
SOC 2	US-developed framework to assess internal controls for data protection, especially in cloud/SaaS.	Technology and service providers, especially in B2B or SaaS.	Voluntary but often contractually required. Demonstrates strong operational security and builds trust.
PCI DSS	Global industry standard to protect cardholder data and reduce fraud.	Any entity that stores, processes, or transmits credit card data.	Mandatory for merchants and payment processors. Requires strict controls and regular audits by certified assessors.
DORA (Digital Operational Resilience Act)	EU regulation to ensure financial sector firms can withstand and recover from ICT-related disruptions.	Financial entities operating in the EU, including banks, insurers, investment firms, and critical third-party providers.	Requires robust ICT risk management, incident reporting, digital operational resilience testing, and oversight of third-party risk. Complements NIS2 and GDPR.

Compliance with multiple regulations / frameworks

Organisations today are rarely dealing with just one set of compliance requirements. More often, they face a patchwork of overlapping legislation, regulatory obligations, and industry frameworks. Whether it's GDPR, NIS2, ISO 27001, DORA, or sector-specific standards like PCI-DSS, the compliance landscape can quickly become complex and burdensome to manage.

What many organisations fail to realise, however, is just how much overlap exists between these various requirements. Core principles like risk assessment, access control, incident response, and governance are common threads that run through most cyber security and privacy regulations. As such, a smart, integrated approach to compliance can significantly reduce duplication of effort.

Rather than treating each regulation in isolation, leading organisations take a unified approach - mapping controls and processes across multiple standards, and building a security posture that satisfies them collectively. For example, an organisation certified to ISO 27001 is already well on its way to meeting the security requirements of NIS2 - perhaps 80% of the way there.

By building a centralised, control-based compliance framework, organisations can streamline audits, reduce costs, and ensure that security becomes a sustainable, business-aligned practice rather than a constant fire drill.

Compliance Automation tools

Keeping track of requirements across frameworks like ISO 27001, NIS2, GDPR, PCI-DSS, and others can quickly become overwhelming - especially when each brings its own set of controls, evidence demands, and audit requirements.

This is where compliance and GRC (Governance, Risk, and Compliance) automation tools come into play.

These platforms help organisations map, manage, and monitor controls across multiple frameworks, identifying overlaps and streamlining compliance efforts. Instead of duplicating work for every standard, automation tools allow you to implement a control once - say, for access control or incident response—and then map it to the relevant requirements across multiple regulations.

Key benefits include:

- **Reduced duplication and rework:** Implement controls once and reuse them across frameworks.
- **Continuous compliance:** Automated evidence collection, control monitoring, and workflow management help ensure you're always audit-ready.
- **Clear visibility:** Dashboards and reporting give stakeholders a real-time view of compliance status and risk exposure across the organisation.
- **Audit efficiency:** Centralised documentation and automated control mapping make internal and external audits faster and less disruptive.
- **Scalability:** As regulations evolve or new standards emerge, automation tools can adapt—so you're not constantly reinventing your compliance programme.

Compliance tools help you turn an annual rush to recertify into a robust process which operates all year round, so you always know your compliance position and have the time needed to address any gaps.

Facts and Figures

Cost of Non-Compliance vs Compliance: It is well documented that failing to comply is far more expensive than the investments to comply. One benchmark study found the average cost of compliance (implementing policies, training, audits, etc.) for large firms was ~$5.5 million annually, whereas the average cost of non-compliance (through fines, business disruption, lost productivity, and remediation) was ~$14.8 million – nearly 3 times higher

Reference: corporatecomplianceinsights.com

Regulatory Fine Trends: Regulatory bodies have been actively enforcing compliance. In data privacy, for example, GDPR fines have totalled **€5.88 billion** from 2018 through 2024 across Europe

Reference: dlapiper.com

On a positive note, companies with strong compliance programs often can negotiate lower fines or avoid violations altogether. As regulations like the EU AI Act and NIS2 come online, we expect an initial wave of high-profile enforcement to drive the point home – much like GDPR's early years – further reinforcing the need for mature GRC capabilities.

Adoption of GRC and Compliance Programs: Most organisations recognize the need for GRC. According to Accenture's global survey, **95% of companies have built or are building a "culture of compliance"** across their enterprise. This indicates near-universal awareness at leadership levels that compliance and ethics must be part of corporate culture. However, maturity varies: only **36% of organisations have a formal enterprise risk management (ERM) program** in place. This suggests that while most companies intend to be compliant, many are still developing the infrastructure and processes for comprehensive GRC. As industries face new risks (cyber threats, supply chain disruptions, pandemic impacts), boards are increasingly pushing for better risk oversight. In fact, **36% of organisations plan to increase investment in risk management and compliance in the next two years.**

Reference:procurementtactics.com

Volume of Regulatory Change: One of the biggest challenges in compliance is keeping up with the pace of new laws and updates. Globally, there are hundreds of regulatory agencies issuing updates daily. and this pace has only increased with privacy and financial regulations in recent years. This "tsunami" of regulations means organisations need mechanisms (often technology-driven, like regulatory feeds into GRC systems or subscription to compliance update services) to track relevant changes.

Market Growth and Future of GRC: The GRC technology market is rapidly growing as companies seek software to manage these complexities. By some estimates, the **global GRC software market** was about $5 billion in 2023 and is projected to nearly **double by 2029** (approaching $9-10 billion) as demand for integrated risk management tools escalates

Reference: verdantix.com

Cybersecurity Insurance and GRC: Insurers providing cyber insurance now scrutinize clients' GRC measures (like whether they follow frameworks such as ISO27001 or have certain compliance certifications) when underwriting policies. A strong GRC program can thus reduce insurance premiums and provide another financial incentive for companies to invest in compliance and risk management.

Are You Governance, Risk & Compliance Ready?

1. Governance – Leadership & Accountability

□ Do you have a formal governance framework that defines policies, roles, and responsibilities for risk and compliance?

□ Is your board/C-suite involved in risk and compliance decision-making?

□ Do you conduct regular reviews of governance policies to ensure they align with business goals and regulatory changes?

□ Do you have a documented code of ethics and conduct for employees and leadership?

□ Are third-party vendors and partners subject to governance and risk oversight?

If you answered "No" to any of these, you may have gaps in governance oversight.

2. Risk Management – Identifying & Mitigating Threats

□ Do you maintain a risk register that documents business, cybersecurity, financial, and operational risks?

□ Are risks assessed and prioritized based on impact and likelihood?

□ Do you conduct regular risk assessments (cybersecurity, operational, financial, reputational, supply chain, etc.)?

□ Do you have a formal risk mitigation strategy that assigns owners and timelines for corrective actions?

□ Is there a business continuity and disaster recovery plan in place for key systems and operations?

If you answered "No" to any of these, you may be exposed to unaddressed risks.

3. Compliance – Meeting Regulatory & Industry Standards

□ Are you aware of the key regulations and frameworks applicable to your industry (e.g., GDPR, ISO 27001, NIS2, PCI DSS, SOC 2, AI Governance, etc.)? Do you have formal compliance policies and controls in place for these regulations?

□ Is compliance regularly monitored and audited internally or externally?

□ Do you have automated compliance tracking or reporting tools in place?

□ Can you provide audit-ready documentation quickly in case of a regulatory review?

If you answered "No" to any of these, you may face regulatory or financial risk.

4. Cybersecurity & Data Protection – Secure Operations

□ Do you have a documented cybersecurity policy that aligns with compliance requirements?

□ Have you conducted a cyber risk assessment in the past 12 months?

□ Are employees trained on security awareness and compliance obligations?

□ Do you have incident response and breach reporting protocols in place?

□ Is sensitive data protected through encryption, access controls, and data classification?

If you answered "No" to any of these, your security posture may not be aligned with GRC best practices.

5. Continuous Monitoring & Improvement

□ Is GRC embedded into your organisation's culture rather than treated as a one-time project?

□ Do you have a GRC technology platform to manage governance, risk, and compliance in one place?

□ Are compliance and risk activities regularly reviewed, tested, and updated based on new threats or regulatory changes?

□ Do you engage in ongoing third-party assessments or audits to ensure compliance?

□ Is compliance reporting automated and integrated into your business operations?

If you answered "No" to any of these, your GRC efforts may lack sustainability and efficiency.

How We Help – Your Trusted GRC Partner

At Insight, we understand that Governance, Risk and Compliance (GRC) isn't just about ticking boxes. It's about protecting your reputation, enabling confident decision-making, and ensuring you can grow without fear of regulatory or operational blind spots.

We help you navigate this complexity with a holistic, practical and technology-led approach to GRC that delivers both resilience and agility.

Advisory & Audit Services:

Our experienced consultants help you understand your obligations, benchmark against leading standards, and chart a clear course forward.

Gap Assessments & Readiness Reviews – for ISO 27001, Cyber Essentials+, NIS2, CAF and more.

Policy & Framework Design – building scalable governance, risk and compliance programmes tailored to your business.

Board & Executive Reporting – translating GRC posture into meaningful business risk insight for leadership.

Internal Audit Support – including evidence preparation, remediation planning and continuous assurance.

Managed GRC Services

If you don't have the in-house bandwidth or expertise, our Managed GRC offering keeps your compliance programme running smoothly.

Ongoing Risk & Compliance Management – we manage your control testing, issue tracking, and reporting.

Virtual CISO or Virtual Information Security Officer – access expert support without the overhead of building a full internal team.

Why Clients Choose Insight

Trusted across industries – from financial services to healthcare, manufacturing to tech.

Certified to the standards we help you meet – including ISO 27001 and Cyber Essentials+.

Vendor-agnostic – we work with leading GRC platforms, but our advice starts with your goals, not a product pitch.

Business-aligned – we speak the language of both the boardroom and the back office.