IT GRC:
The Cornerstone of Operational Resilience in the Digital Era

Camms.

Software to Change Tomorrow.

Intro

No longer an onerous major overhaul of operations, digital transformation projects that would have taken years can now be completed in a matter of weeks thanks to modern technology. Amid expedited delivery timeframes, using a variety of integrated systems and applications to streamline processes has evolved into a core strategy for most organisations. This rapid adoption of digital technology has been further accelerated by a pandemic-induced change in working models, advanced technological innovations, and the development of AI.

At risk of being left in the dark ages, organisations have been forced to recalibrate their approach to the adoption of digital technology. Boards across a variety of industries have been implementing digital transformation projects at a rapid pace – a trend that isn't showing any signs of slowing. According to Gartner, 87% of senior business leaders say digitalisation is a priority – a forward-thinking mindset that's stoked forecasts for the global digital transformation market to double from $469.8 billion in 2020 to $1,009.8 billion by 2025.

While the opportunities and benefits of running operations through a variety of digital platforms, systems, and applications are unprecedented – such as improved efficiency, enhanced customer experience, and cost reduction – it also exposes them to potential challenges. The loss of a vital system, a data breach, or failure to get online can have an enormous impact on an organisation's ability to deliver its services and products.

This has brought the digital aspect of governance, risk, and compliance (GRC) – or 'IT GRC' – into sharp focus for organisations, making it a top board priority in a bid to embed operational resilience.

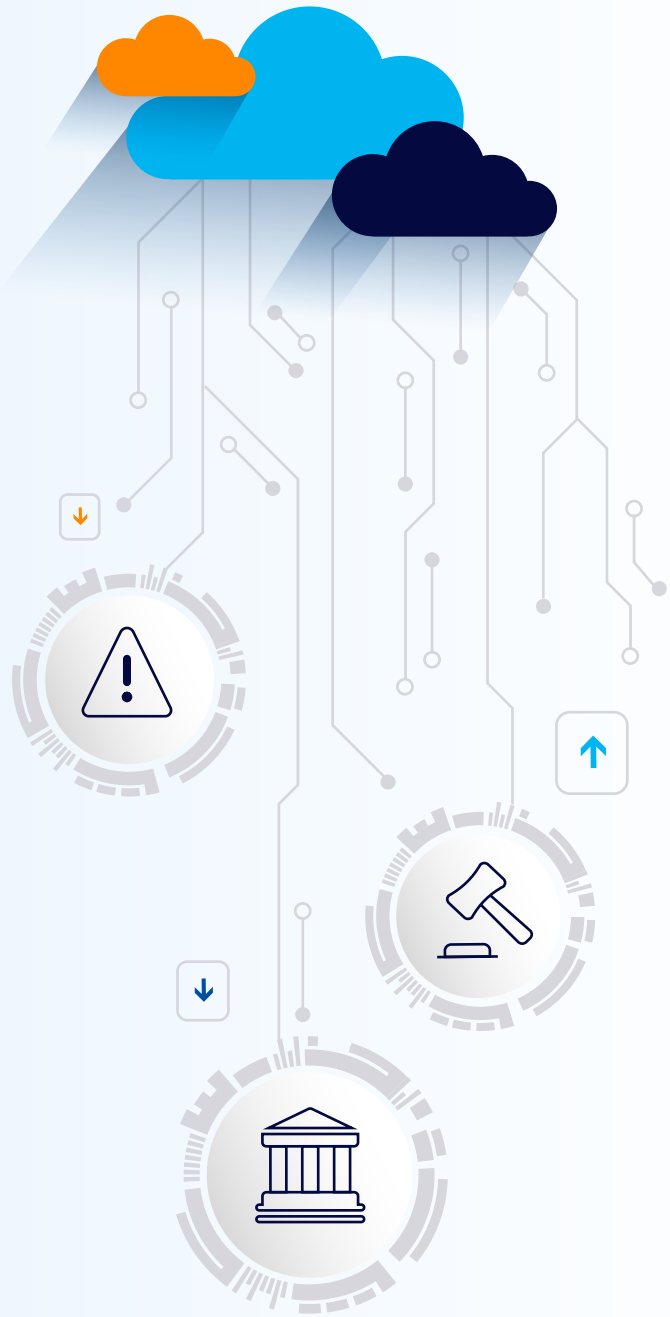
The Emergence of IT GRC

IT GRC is the term used to refer collectively to a whole host of processes that enable an organisation to ensure their company data is secure by managing IT related risks, threats, and vulnerabilities, and ensuring compliance with data privacy laws & regulations. It also involves implementing a strategy that ensures IT infrastructure is fit for the future – making sure systems, software licences & equipment are up to date, and implementing business continuity & disaster recovery plans.

Most organisations will have some kind of processes in place to manage aspects of IT GRC. They might have a risk register of IT related risks and a control library of processes to minimise these risks. They might have a list of data privacy regulations & IT policies to implement governance and monitor compliance. They may even have an asset management log or have business continuity plans and perform regular disaster recovery tests. They will likely have a process to log IT related tickets and incidents to ensure they are resolved quickly.

But in many organisations these IT GRC processes are often orchestrated using a variety of manual, outdated processes, spreadsheets, and clunky systems. Processes are often disjointed from overall business operations - and run solely by the IT team - making it hard for the organisation to get a consolidated view of IT related risks, potential compliance breaches, and the organisations overall cyber security posture.

However, it's not just business models that are undergoing digital transformation; organisations are realising that their IT GRC processes need a digital overhaul too. Many organisations have already embraced modern GRC technology for their non-digital governance, risk & compliance requirements, and they are quickly realising that these same technology capabilities can be used to streamline and automate a comprehensive IT GRC programme.



What are the key components of IT GRC... and how can technology help?

To deliver a comprehensive IT GRC programme, organisations must address a range of relevant factors across risk management, incident reporting, compliance with data privacy regulations, policies, and audits, and business continuity.

To establish an IT GRC framework that's free from human error and costly delays, organisations are embracing automated software tools that embed efficiency into their processes and procedures via a central point of oversight.

Here we explore 10 key areas that contribute to a best-practice IT GRC programme, and explore how they can be automated through the use of GRC technology.

1 Cyber & IT Risk Management

An unreserved reliance on digital data and IT systems has pushed cyber risk up the corporate agenda for most organisations amid the exponential growth of new and emerging digital threats. In its 12th Risk Barometer, Allianz ranked cyber incidents (34% of responses) as the most important organisation risk globally for 2023 – remaining at the top for a second consecutive year.

To manage this pervasive risk, boards must implement best practice risk management processes to ensure they have full visibility of cyber risks and that they are carefully managed. To build a comprehensive cyber risk management programme organisations will need:

A Cyber risk register: This document or database allows stakeholders to identify, assess, manage, and track cybersecurity risks. This process is essential for managing the organisation's cybersecurity posture and ensuring that potential threats and vulnerabilities are properly documented and addressed.

Cyber risk assessments: Carrying out regular risk assessments allow stakeholders to identify and evaluate potential cybersecurity risks that could impact IT systems, data, and operations. This understanding of the threats, vulnerabilities, and potential consequences of cyberattacks underpins the development of strategies for mitigating or managing these risks.

Cybersecurity controls: These proactive measures and safeguards are implemented to prevent an organisation's most critical risks from coming to fruition. These controls are put in place to protect digital assets and sensitive information from cyber threats and vulnerabilities – such as access control, cybersecurity awareness training, incident response plans, network security, and data encryption.

Control monitoring: Cyber risk management programmes should be reinforced by robust internal monitoring of the controls that oversee high-risk processes. Organisations that adopt an ad hoc approach to monitoring create gaps in their control environment that can lead to costly issues.

How can technology help?

A risk management tool provides the functionality needed for organisations to take responsibility for managing dynamic cyber and IT risks. These systems enable organisations to build a digital, searchable risk register - making it easy for teams across the business to log, rate, and categorise risk based on a predefined framework. Data from other sources can be pulled into the system via APIs making it easy to monitor risk levels based on live operational data in other systems.

Risk assessments can be rolled out using online forms with all data feeding directly into the platform. Workflows automate the distribution and chasing up of risk assessments - ensuring timely data is captured and problems can be resolved quickly.

Organisations can easily implement a control library to set controls to reduce the impact of the most critical risks. Controls can easily be linked to the relevant risk and teams can perform regular control testing and document the findings.

This comprehensive process provides risk managers and organisational leaders with a broader view of the impact of cyber risk on different areas of the organisation. This centralised process makes risk management more accessible, accountable, trackable, and resolvable. Risks can be logged, and treatments created, tracked, and linked to controls for ongoing monitoring in real-time.

This single-pane-of-glass view provides the foundation for a holistic approach to risk management that can grow and evolve with an organisation. It engages stakeholders by driving a transparent flow of risk-related information from the top down and the adoption of a proactive risk culture from the bottom up.

2 Controls & Control Monitoring

In a complex digital infrastructure, there is so much that can go wrong! As well as having an active risk register, organisations must also implement a series of 'controls' linked to each risk to keep the risk to a minimum or prevent it completely. Controls can come in a variety of different formats, they can be a series of regular checks to make sure systems, processes, and back-ups are working, they can involve implementing alternative solutions or back up providers that can be activated in case of a failure, they might be automated reports that are run to check email vulnerabilities & phishing attempts, or they might involve implementing a new policy or procedure to ensure things are done correctly to protect IT security & company data and ensure compliance with regulations.

A comprehensive Secure Controls Framework (SCF) typically includes a comprehensive list of security controls that address various aspects of information security, such as access control, encryption, incident response, and more. A SCF provides a standardised approach to security that organisations can adopt to mitigate risks and achieve compliance with industry-specific regulations.

All controls should be logged in your control register and linked to the corresponding risk. Once controls are logged and documented, regular checks should be made to ensure the control is effective. This rigorous testing allows for continuous improvement and enables organisations to ensure they are operating inline with established standards & frameworks, such as GDPR, ISO 27001, NIST Cybersecurity Framework, PCI DSS, and CIS Controls.

Controls should also be mapped to all associated frameworks and standards. This is particularly useful when an organisation needs to demonstrate compliance with multiple regulations or frameworks simultaneously.

How can technology help?

GRC technology makes it easy to build a comprehensive control register and map controls back to the associated risks or to the relevant security standard, regulation, or framework.

Teams can build a comprehensive 'controls register' within the platform. Controls are logged via online forms which feed directly into the platform. The advanced mapping functionality ensures all controls are linked to the associated risks. Control checks and automated control monitoring on live IT data can be carried out within the platform. API integrations enable teams to pull in IT data from other systems and sources to set up automated control checks and automated alerts can be used to flag problems.

The system can be used to implement a secure controls framework to implement specific step-by-step workflows or compliance frameworks to comply with data privacy regulations such as GDPR, ISO 27001, NIST Cybersecurity Framework, PCI DSS, and CIS Controls.

Controls can easily be mapped to various compliance frameworks, enabling organisations to demonstrate compliance with a variety of different frameworks & regulations at the same time, minimising manual checks and duplicate controls.

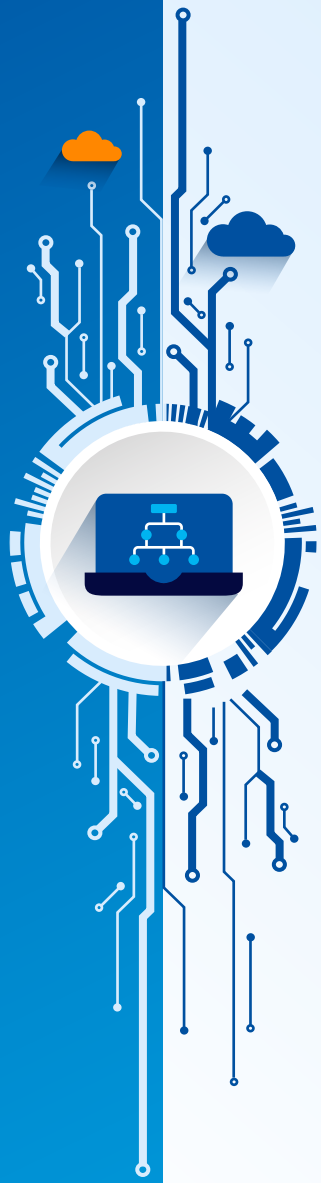
The system makes it easy to report on failed or ineffective controls and missed checks making it easy for teams to address problems quickly - ensuring an effective controls framework.

3 IT Vendor Risk Management

Around 70% of respondents in Deloitte's Global Third-Party Risk Management Survey 2022 indicated that they want to exploit synergies across third-party management processes to drive efficiency. While the benefits of engaging with third parties are compelling, this reliance on external partners exposes organisations to an additional layer of digital risk. For example, a total of 98% of organisations worldwide have integrations with at least one third-party vendor that has experienced a cyber breach in the last two years.

Organisations must build a centralised log of IT related vendors – capturing critical data around contracts, SLAs, KPI's, performance, key contacts, and cost. They must also roll out regular vendor risk assessments, questionnaires, and surveys to monitor performance against agreed metrics. They should also perform regular benchmarking & scorecards to compare current providers to other similar vendors in the market. This oversight allows vendors to be vetted and compared, the right one chosen, and facilitates continuous monitoring from a risk perspective. Onboarding & offboarding processes should also be documented and formalised.

Organisations should also ensure vendors are complying with any relevant policies or compliance requirements as part of their third-party risk management programme.



How can technology help?

IT GRC technology elevates IT vendor risk management by providing organisations with automated tools and processes that identify, assess, monitor, and mitigate the risks associated with IT vendors. Critical information, contracts, and performance data relating to each vendor are entered into the platform via customised online forms that feed into a single repository. The findings are displayed via a centralised dashboard, making it easier to manage and track vendor relationships.

Online vendor risk assessments with conditional workflows and transparent scoring methodologies automate vendor risk management. This streamlined process allows organisations to consistently evaluate and compare vendor risk profiles. The tool provides a framework for supplier onboarding & offboarding - ensuring teams have full visibility of supplier contract dates, costs, and SLAs.

Seamless due diligence processes are driven by integration with external risk intelligence sources to provide real-time information about critical factors like vendor financial stability and cybersecurity posture. The technology also automates compliance checks and provides real-time updates on changes in regulatory standards, helping organisations avoid potential penalties and legal issues due to supplier related non-compliance.

Real-time dashboards and reports ensure third-party threats are accessible at all levels of an organisation, allowing boards and senior executives to understand the dependencies and associated risks.

4 IT & Cyber Incident Management

In modern digital organisations, having a formalised process to capture & resolve cyber & IT incidents is essential. There are many types of cyber & IT related incidents. Employees need to be able to log problems with laptops, phones, and equipment, escalate problems with systems & applications, expired licencing, and internet downtime, and capture incidents relating to cyber threats & data breaches.

With so many different types of incidents to contend with, each incident must be logged consistently capturing essential data, images, and URLs. Each incident must then be categorised & rated according to severity and escalated to the relevant team or individual. All remediating actions should be carefully documented until the incident is resolved.

Capturing this data consistently enables teams to understand the source of incidents, allowing them to implement corrective actions to prevent recurrence.

In many organisations cyber incidents are logged in a variety of ways, there Is often an online ticketing system for employees to log problems with systems & hardware. Data breaches and phishing emails are often logged separately with IT, and major incidents like system downtime and internet outages are reported directly to IT leaders. These disjointed and often rely on manual processes and emails making it challenging for organisations to understand the full spectrum of cyber incidents that are happening across different sites.

How can technology help?

Software can support organisations to implement a comprehensive cyber & IT incident reporting process. During the system implementation IT teams will define how various cyber related incidents should be categorised and rated and who they should be escalated to.

Staff will use online forms to log cyber and IT related incidents. Forms can be customised depending on the type of incident logged - ensuring all critical information is captured consistently. Teams can upload photos, documents & URLs relating to the issue to ensure all information is documented - making incidents easier to resolve.

Workflows can be set up to automatically escalate incidents to the relevant team or departments depending on the incident type and rating. A step-by-step triage process allows for further escalations and enables teams to log remediating tasks & actions until cases are closed.

Leaders can easily report on types of incidents, typical resolution times, teams & departments affected by incidents, and incident causes, enabling them to understand the source of incidents & prevent reoccurrence. The same system can also be used to log other types of organisational incidents, like operational failures, accidents, hazards, and near misses - enabling teams to look at incidents holistically and break down silos.

Many GRC platforms also enable organisations to link incidents back to the originating risks or failed controls, enabling teams to understand control effectiveness and identify new risks to add to their risk registers.

5 Compliance with Data Privacy Laws & Regulations

An avalanche of new data privacy laws, regulations and standards have been introduced and tightened against a backdrop of escalating cyber-attacks targeting organisations both in terms of frequency and sophistication.

Compliance isn't just a fundamental element of IT GRC; it's a mandatory requirement as regulators and governments attempt to boost resilience against the damaging impact of cybercrime. To be successful, these efforts must be proactive, and organisations must keep a comprehensive library of all applicable data privacy regulations, policies, and procedures - and put steps in place to ensure teams are compliant.

Increasingly robust data privacy laws, regulations, and standards inform and drive IT GRC practices within different industries and regions – such as the General Data Protection Regulation (GDPR) in Europe, The NIST Cybersecurity Framework in the US, Cyber Essentials in the UK, and the ISO 27001 international information security standard used globally. These regulations require robust governance and strict procedures and policies to ensure compliance.

How can technology help?

Software can support organisations to streamline and automate IT related compliance. Organisations can use the tool to build an online obligations library. Teams log various regulations, policies, and process documents on the system, capturing key information around expiry dates, responsible personnel, and related business processes - and they can roll out regular checks to ensure compliance. Areas of non-compliance are highlighted via automated alerts so they can be quickly addressed.

Many GRC platforms offer integrations with third party content providers – this facilitates automated regulatory horizon scanning. By accessing current, up-to-date regulatory content and intelligence feeds, organisations benefit from a rich repository of information – ensuring they keep pace with new and amended rules and regulations. Notifications are sent when a regulation changes, enabling teams to quickly understand which business processes are affected and make the alterations. The technology offers a clear view of which regulations link to which internal policies and procedures – facilitating a full impact analysis and individual accountability and responsibility for corrective actions.

Access to a transparent audit trail of IT related compliance related activities enhances the efficiency of regulatory reporting and expedites the investigation of emerging issues.

6 Cyber Audits

Most organisations will be subject to a variety of cyber audits. These could be audits from external regulators, or audits to achieve various accreditations & certifications to cyber security standards. Many organisations even conduct their own internal audits that involve a comprehensive analysis and review of an organisation's IT infrastructure to ensure that appropriate policies and procedures have been implemented and are working effectively.

By assessing an organisation and its systems and services, auditors can detect vulnerabilities and threats, display weak links and high-risk practices, and determine whether practices comply with relevant laws and regulations.

Organisations should schedule regular audits upfront to ensure their policies and procedures are keeping pace with the dynamic cyber environment and to keep any accreditations & certification up to date.
Cyber audits are organisation-wide undertakings that can disrupt regular operational practices, particularly if they involve scanning networks, systems, or applications for vulnerabilities. Therefore, organisations must strike a balance that prevents them from scheduling audits too infrequently, resulting in gaps in security coverage, or scheduling them too frequently, straining resources and hindering remediation.

Scheduling and conducting audits are only the first steps; the heavy lifting is performed when analysing the results, prioritising vulnerabilities, and implementing remediation. Delays in these post-audit activities can impact an organisation's security posture.

How can technology help?

GRC technology enables teams to build a centralised register of all their IT audits online and schedule them upfront. The system automatically sends reminders to the relevant stakeholders when audits are due, ensuring the necessary steps can be taken - driving accountability. Findings of all audits are captured in the tool and automated workflows are used to implement recommendations and log actions to complete the audit cycle.

The data within GRC software can also contribute to successful IT audits. Many data privacy regulations and standards require robust risk management & strict governance practices, and compliance with data privacy laws. GRC software can support organisations to demonstrate they are successfully managing risk & maintaining compliance in order to meet audit requirements.

Managing cyber audits in a platform provides a complete history of all audits and their findings and any outstanding actions. Real time dashboards and reports make it easy to spot trends, identify problems, and conduct investigations. Many tools enable organisations to link audits to compliance obligations and risk management - adding another layer of depth to the process. This comprehensive mapping enables businesses to understand the risks relating to a failed audit or the impact of non-compliance. Data visualisation tools provide intuitive dashboards and reports for transparent oversight of audit-related findings and results.

7 Policy Management

The ever-widening cyber-attack surface has amplified the importance of robust IT security policies and procedures for business leaders. IT teams must implement a collection of policies that establish guidelines, best practices, and rules for managing and securing an organisation's technology infrastructure and data – such as acceptable usage policies, data protection & privacy procedures, and process documentation.

IT policies provide guidelines for how employees should interact with technology and handle company data and they provide governance for procedures that must be followed to comply with regulations, standards & IT certifications.

To ensure effective policy management, organisations must house a comprehensive library of all their active policies & procedures. They must capture critical details around policy owner, approvers, expiry date and who the policy applies to.

For this process to remain effective, policies must be checked against regulations and company guidelines and updated regularly using a stringent sign-off and approval process. Failure to implement these controls might result in necessary policy changes from a regulatory perspective slipping through the cracks, leaving existing policies outdated and making the risk of non-compliance a threat – exposing the organisation to legal liability.

How can technology help?

With multiple policies to manage concurrently and many stages involved in their lifecycle – from creation and implementation to management and updating – software automation can streamline the policy management process.

Organisations can create an online policy library within the platform. The functionality enables policies to be created consistently using pre-defined templates, capturing essential credentials like owner, approval date, and expiry date when policies are uploaded into the solution. Approval workflows can be set up to obtain policy sign off and ensure accountability, and the system provides a time stamped history of all revisions and changes.

Proactive policy insight and oversight empowers organisations to identify, analyse, manage, and monitor policies in the context of operations, processes, and roles – from harnessing a centralised policy register to transparent policy ownership, sign-off, and attestation.

KPMG further highlights the benefits of leveraging policy management through technology:

- Identifies triggering events for new policies and updates to existing policies – such as new regulatory mandates or changes to industry-leading frameworks.
- Streamlines and enhances policy development and establishes clear linkages to regulations and standards.
- Ensures necessary reviews are performed and approvals are documented and retained.
- Facilitates communication and training based on policy enhancements.
- Monitors ongoing policy compliance by impacted groups by linking policy attestations, control testing results, and issues to relevant policy requirements.
- Provides policy owners with meaningful insights into the entire policy management lifecycle: policy creation, maintenance, compliance, issues, and remediation.

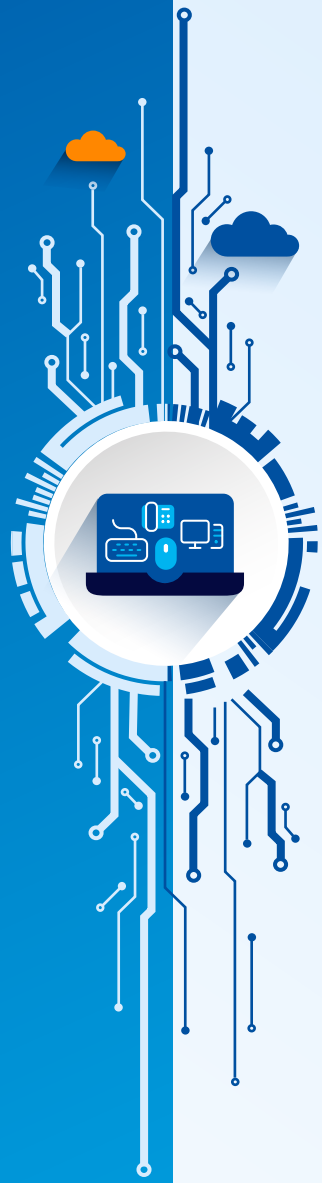
8 Asset Management

An IT asset is classified as any organisation-owned information, system or hardware used in its operations – from laptops, desktop computers, and smartphones to software licences for systems and apps. These assets permeate modern organisations, making them the cornerstone of operations.

IT assets have a finite period of use. Therefore, organisations should maximise the value they can generate from them by proactively managing the IT asset lifecycle to optimise strategic decision-making and budget allocation within the IT environment.

IT asset management involves managing an active inventory of all IT assets. It should include vital data including cost, expiry date, owner, make, model, and licence details. This will ensure an organisation's assets are accounted for, deployed, maintained, upgraded, and disposed of when the time comes.

Robust asset management collates and harnesses asset data to increase returns, minimise risk and fuel improved organisational value. By making informed decisions that avoid superfluous asset purchases and maximise current resources, organisations can reduce software licensing & support costs, eliminate waste, and improve efficiency.



How can technology help?

Technology can automate the asset management process and bring it online. Organisations can create an online asset library categorised by different asset types. Assets can be added to the register using simple online forms that can be easily customised to include the relevant fields for each category. Similar assets can easily be cloned to speed up the input process or uploaded from spreadsheets for large batches.

Critical data is captured about each asset, for hardware it will be details around owner, model, age, usage, and for software it will be things like contracts, expiry dates, and licence renewals. The critical process of collecting inventory data and tracking contract statuses throughout the IT asset lifecycle is centralised. This enables better IT asset management and tracking of hardware, software, licenses, and even non-IT assets.

Technology allows organisations to manage IT assets in real-time with a full understanding of how incidents, problems, changes, and releases impact them. This also makes it easier to track software licenses and warranties and avoid unnecessary repair charges or fines.

By establishing a consolidated and accurate database of all assets, organisations can oversee the cost associated with managing the devices, make informed decisions, properly allocate the right devices to users, and refresh older assets. Organisational risk is reduced as firms can be sure equipment is current, updated with the relevant security measures, and software licences and contracts are in date.

9 Business Continuity & Operational Resilience

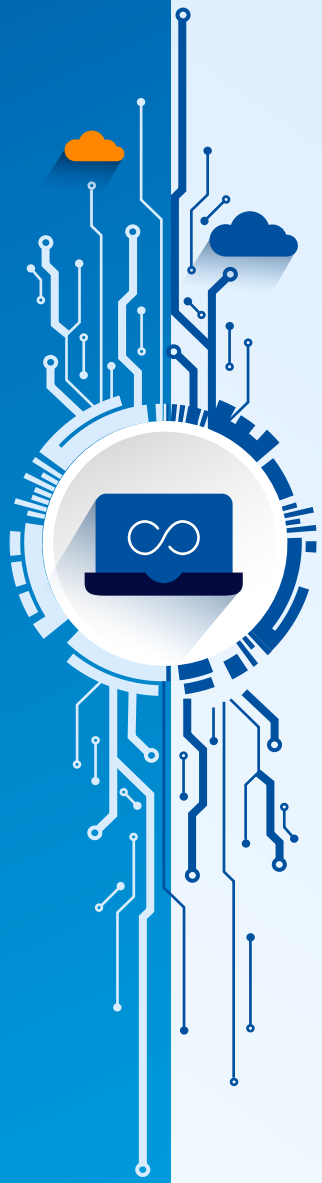
IT GRC isn't just about minimising immediate threats and achieving compliance with mandatory regulations; when done well it can support an organisation to achieve long-term operational resilience – a key component of which is business continuity.

IT systems are the backbone of modern organisations. Any disruption in IT services can result in significant downtime, which can be costly in terms of productivity, revenue, and customer satisfaction.

Business continuity in an IT context refers to an organisation's ability to maintain its critical operations and deliver its products and services when faced with technological failures or a data breach. To be resilient, they must implement robust strategies, procedures, and plans to provide essential functions with the durability needed for operations to be maintained or quickly resumed during and after incidents.

Without a prescribed plan to steer an organisation's holistic response to disruptive events, business continuity will lack the structure needed to deliver operational resilience. A comprehensive business continuity plan outlines potential business processes that could be affected by a disruption and delineates actions to mitigate the impact if they are interrupted – enabling an organisation to respond and recover expeditiously.

An IT GRC programme empowers boards to foster a culture of operational resilience from an IT perspective that's driven from the top down and implemented from the bottom up by nurturing their understanding and appreciation of digital risks – traditionally a blind spot for business leaders.



How can technology help?

GRC technology with business continuity capabilities allows organisations to create a business process register and a library of business continuity plans within the platform. Displayed in an intuitive and streamlined user interface with centralised personal views, this allows organisations to identify and log critical processes, systems, products, and sites that could impact operations if they fail.

Process review modelling functionality provides organisations with a detailed view of critical processes and allows them to formulate dependency mapping. It also captures vital details around key factors like cost, SLAs, KPIs, and industry benchmark standards for each process so organisations can quickly understand the impact of a failure in terms of cost, man hours, and potential lost revenue.

The best-practice business impact assessment templates within the tool help organisations to understand the importance of each business process based on things like increased expense, regulatory fines, and customer dissatisfaction. Forms are rolled out online with all data feeding directly into the platform.

In the event of a crisis software automates the activation of your recovery plan based on the incident logged. As you put the plan into action, leaders will get a live snapshot of the progress including the real time status of actions and tasks that are critical to the success of the recovery plan. Use the reports to identify gaps in your BCM and disaster recovery plans.

10 Strategy Planning & Execution

IT related processes & systems enable organisations to be more competitive, efficient, and adaptable in a rapidly changing business landscape. To exploit these benefits, IT infrastructure must be viewed as a critical component of the overall business strategy – not just a support function. Organisations must therefore, align their IT strategy with their overall organisational goals and continuously evaluate and adjust this comprehensive strategy to stay relevant and competitive in the market.

For each employee to understand the role they play in achieving the business's IT goals, senior IT leaders must break down their strategic programmes into actionable projects & tasks and allocate them out across the business. In conjunction with their strategic plan's, IT teams must also consider dependencies - including the associated risks & compliance obligations - and any key milestones that prevent the business from moving to the next phase of its strategy. Organisations must also adopt a collaborative approach and align the corporate strategic plan with broader IT business operations to achieve success.

Adopting a holistic approach to strategy planning will prevent outdated systems or technology from creating operational roadblocks and restricting growth. Therefore, long-term strategic plans should factor in new equipment, new IT-related regulations, and the modernisation of IT infrastructure.

How can technology help?

Technology can support an organisation to successfully plan and implement an effective strategy to achieve strategic goals & objectives. This includes IT or technology related infrastructure goals.

The framework within the tool enables organisations to map out their strategy by breaking down their goals & objectives into smaller, programmes, projects, tasks, and actions. Each key deliverable is allocated a timeline, budget, and KPI's. As tasks and actions are completed, progress is indicated at each level of the strategic plan. Leaders can easily view the strategy map and its status using simple tree views and dashboards & reports. Automated control monitoring can be set up to flag missed deadlines and budget overspends - ensuring problems are addressed quickly. Workflows can be used to add structure to the process, for example when a task or action is completed, the relevant stakeholders are notified enabling them to move on to the next step in the strategic plan.

The ability to monitor and report on key performance metrics provides organisations with oversight of the effectiveness of their strategic plan execution – allowing prompt course correction if required. Comprehensive scorecards also provide a clear view of IT infrastructure performance.

Strategy mapping provides a holistic view of the strategic plan and its performance at each level of the plan structure. Comprehensive reporting capabilities power the compilation of detailed reports, actions, and metrics for stakeholders & executives.

Empowering the Board: Strategic Decisions Informed by IT GRC

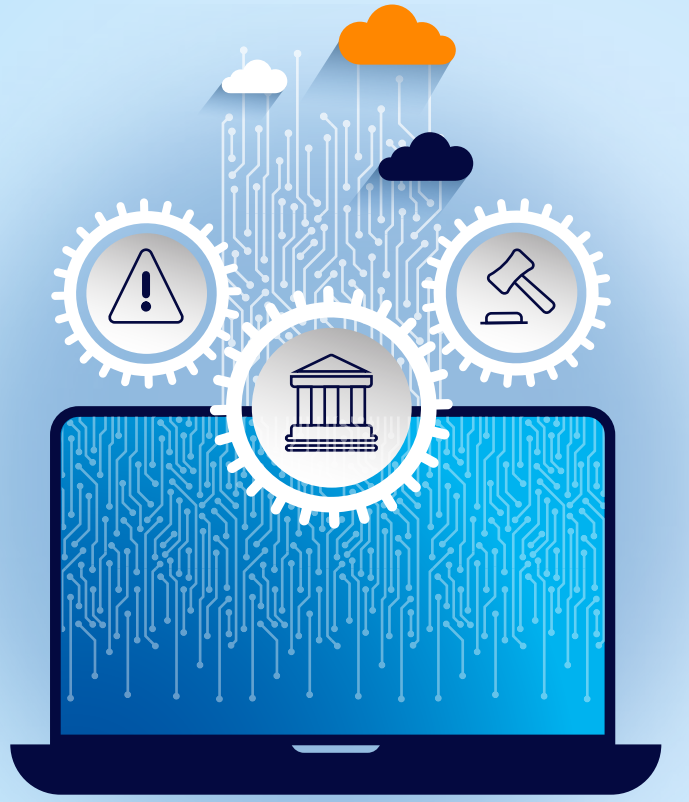
Boards are undergoing their own digital transformation to be effective in the digital age. Turning a blind eye to IT value creation and IT performance because they lack the awareness, knowledge, or skills is no longer sustainable. Nor is viewing digital requirements as 'operational issues they should avoid', rather than strategic imperatives.

Robust IT GRC frameworks can bridge the gap between boards and their digital responsibilities by providing clarity, insights, and actionable data that addresses their opaque view of this contemporary requirement.

IT GRC provides actionable data for the board by integrating associated processes, tools, and frameworks to help them manage and mitigate IT-related risks and ensure compliance with regulations and standards. They can leverage the data to inform decision-making around purchasing new equipment, upgrading IT infrastructure, introducing modernised systems & platforms, and allocating budget & resources to implement controls to reduce critical digital risks.

Merging IT GRC with Broader GRC Considerations

As organisations adopt digital technology to streamline & automate processes, understanding and addressing new risks & compliance requirements linked to digital transformation will help them to optimise the value gained from these technologies.



However, organisations must not overlook non-digital risks in the process. Instead, they should integrate digital risk & data privacy compliance with their existing enterprise risk framework. The ability to understand digital risk in isolation and compare it to standard operational & enterprise risk in a unified framework provides enriching benefits, including:

Holistic Risk Management: By managing digital and operational risks in unison, organisations can ensure that resources & budget are allocated effectively to address all potential threats.

Risk Impact: Digital risks often have dependencies & connections to non-digital risks and vice versa. Understanding these interdependencies helps organisations develop more effective mitigation strategies.

Decision-Making & Reporting: Cohesive reporting helps executives & boards to make more informed strategic decisions when they understand the potential impact of all types of risks –including operational, strategic, and digital risks.

Regulatory Compliance: A consolidated view of both digital & operational compliance obligations allows organisations to achieve detailed oversight of their compliance efforts and ensure they meet their legal and regulatory requirements – now and in the future.

Stakeholder Engagement: Transparency in risk management across all risk areas fosters a risk aware and demonstrates a proactive approach to risk management.

IT GRC should be integrated into the wider corporate strategy to ensure that an organisation's IT infrastructure is futureproof and aligns with its broader objectives. This will empower an organisation to leverage technology as a strategic asset to achieve its goals and meet modern requirements.

Predicting & Adapting to Future Challenges

Rigid GRC frameworks that lack the agility to scale with an organisation and incorporate digital risk & compliance requirements will become stagnant and perpetuate risks rather than mitigate them. By establishing a framework that can grow as the business evolves, the organisation can adapt to future challenges that arise within the ever-evolving digital risk landscape and maximise the strategic opportunities that technology offers.

The dynamic nature of risk and compliance will expose the IT GRC sphere to several compelling future trends, including: increased regulatory complexity, integration with AI and automation, cloud and hybrid environments, and digital supply chain risks.

To keep pace with this evolution and make informed strategic decisions, boards must engage with emerging IT risks, technological advancements, and changing IT/digital regulatory requirements. This will give them the scope needed to provide robust governance, transparent strategic direction, and ongoing risk oversight.

Conclusion

Digitally focused, data-driven, and cyber-savvy IT GRC frameworks are a prerequisite for success against a backdrop of seismic change in the modern business landscape. Organisations that persevere with outdated, siloed, spreadsheet based approaches to IT GRC are hamstrung by static functions, outdated processes and disjointed departments & data sets that fail to consider and address a new wave of digital risks and responsibilities.

The integration of IT into GRC represents an inflection point in the holistic management of risk and compliance in the digital era– and it's being enabled by powerful, agile, scalable, and modern GRC software. Empowered by the ability to adapt swiftly to changing digital regulations, risks, and market conditions, boards can make informed strategic decisions that ensure operational resilience now and in the future.

About Camms.

Camms offers a cloud-based SaaS solution that enables organisations to drive risk, incident, and compliance management across all IT systems & processes. The solution uses a modular approach, allowing organisations to scale and mature their risk management processes at their own pace without the need to purchase disparate systems to cater to different requirements.

The platform offers all the functionality you need to build a comprehensive IT GRC programme:

Risk Management & Controls

Set up a comprehensive cyber risk register, track progress, and define KPIs & tolerances based on your risk appetite. Use the structured framework to define ownership and set key risk indicators. Use automatic workflows & alerts to flag problems and implement approval processes.

Compliance Management

House a comprehensive obligations library of applicable IT & Data Privacy regulations, legislation, policies, and internal procedures. Set a structured process for version control, approval, ownership, and regulatory change. The solution integrates with third-party regulatory content providers to offer regulatory horizon scanning.

Business Continuity

Create a business process register with best-practice BCM plans. Perform business impact assessments (BIAs) to understand the impact of unforeseen events. Execute your BCM plan to get your organisation back up and running in line with RTOs.

Strategic Planning & Execution

Map out your top line goals & objectives relating to IT infrastructure & data privacy and break them down into smaller projects, tasks & actions and allocate them out across the business for completion. Track progress via live dashboards & reports.

Incident Management

Facilitates IT & cyber incident reporting in real-time and triggers the investigation process post-event. Enables teams to link incidents back to the originating risks.

Asset Management

Maintain a digital, searchable register of all IT assets, software, and licenses. Run reports on outdated equipment & license expiry dates to ensure IT infrastructure is modern & fit for purpose.

Audit Management

Schedule & manage internal & external cyber & IT related audits and formalise the results & required actions. Provides a complete history of all your audits and their findings and any outstanding actions.

IT Vendor Risk Management

Create an online vendor register capturing details around contracts, performance, and SLA's. Manage vendor onboarding & offboarding, carry out online vendor risk assessments, and conduct vendor benchmarking & scorecards.

Stakeholder Dashboarding

Intuitive functionality provides executives and the board with key risk, compliance, and strategic progress information when required.

Analytics & Reporting

Built-in dashboards & reports provide critical insights and executive reporting that satisfies requirements from auditors & regulators.

API Integrations

Transfer data from other systems in and out of the Camms solution via API connections, enabling you to base KPIs and risk monitoring on live data.

Adopting a comprehensive approach to managing IT GRC will facilitate the transparent flow of relevant information from the top-down, and the creation of a proactive cybersecurity culture from the bottom-up – empowering the right people to make the right decisions at the right time. Never has this been more important to a business's current and future success. As cyber-attacks become more sophisticated & prevalent and the consequences cause increasing financial, operational, and reputational damage, boards must engage with and extend their superintendence of cybersecurity. The Camms platform provides them – and the business as a whole – with the right level of oversight and action on cyber risks by integrating it into enterprise risk processes, making the business more resilient.

Discover How Camms is Helping Organisations to Implement a Comprehensive IT GRC Programme

Camms provides a cloud-based SaaS solution that offers all the functionality needed to set up a comprehensive IT GRC programme that aligns with an organisations' strategic goals & objectives.

Set up IT risk registers, manage cyber incidents, monitor compliance with data privacy regulations, administer IT policies, implement business continuity plans, and deliver your strategic goals & objectives - all within one platform.

Streamline your IT GRC processes with digital, registers, online forms, automated workflows & alerts, and state of the art analytics & reporting to deliver a cyber savvy organisation that is future ready.

Visit Website **Request Demo**

Camms.

Software to Change Tomorrow.