GRC and Cybersecurity

Making the case
Don’t underestimate cybersecurity. In a world of raging cyber threat, a strong digital defense plays an invaluable role in business resilience

GRC: The Fundamentals

Today’s business climate is more challenging than ever before. Modern risks and requirements are myriad, evolving, and impactful to the business. For example, supply chain issues are new and hard to manage. The range, pace, and level of change can be demanding.

Governance, Risk, and Compliance (GRC) is a systematic way to align operations around business goals and objectives while at the same time addressing risk and compliance with standards and guidelines. It includes policy, process, accountability, and tools to integrate the running of the business and risk management with precision, automation, and accessibility.

GRC management is not new, but its visibility has been elevated as business deals with more sophisticated risks and rules. In today’s world, GRC underpins business efforts to deliver unique customer experiences, improve yield, and translate big data to enhance business decision-making.

GRC is a systematic way to align operations around business goals and objectives.

Business leaders must maintain a high degree of awareness of the ever-changing forces that impact the business daily to align resources and adapt the strategy preemptively. Intentional business requires up-to-date information and analysis, immediate data availability, and tools to ensure good decision-making.

GRC Drivers

Flexibility

Understanding what customers want and staying ahead of the competition while trying to interpret the applicability of laws and standards on the business is no small task. Staying in the game — let alone ahead of the game — is nearly impossible without an effective GRC program. Business leaders must maintain a high degree of awareness of the ever-changing forces that impact the business daily to align resources and adapt the strategy preemptively. Intentional business requires up-to-date information and analysis, immediate data availability, and tools to ensure good decision-making.

Regulations and Standards

Regulations on business seem to change and become more complex faster than they can be understood and implemented. Even when manual processes are in place to address new regulations and standards, the complex and changing nature of such rules requires integrated GRC programs to adjust and respond rapidly.

Risk Profile

Businesses have unique challenges when dealing with internal and external threats, opportunities, and risks and should be well-informed about their risk profile and threat landscape. GRC is paramount to effectively managing risk profiles.

GRC Benefits

Achieve Business Benefits

GRC applies frameworks to help teams achieve their objectives by managing risk, ensuring compliance with standards and laws, and maintaining ethical standards and good governance practices. This involves creating policies and procedures, investing in tools and technology, and conducting employee training and awareness programs to identify and prioritize potential threats and implement strategies to manage them effectively.

GRC also helps organizations comply with applicable rules and laws related to data protection, financial reporting, health, and safety to prevent legal penalties and reputational damage and build credibility with stakeholders. In addition, GRC helps organizations maintain good governance practices such as accountability, transparency, and adherence to moral principles. By doing so, GRC can improve organizational performance and increase stakeholder confidence.

Anatomy of the Security-Centric Organization

Build a GRC Culture

Creating an proactive, risk-aware culture within an organization is crucial for the success of any GRC program. Senior management must set a positive tone and communicate the importance of GRC throughout the organization. To establish a GRC culture, the organization should train employees on GRC principles, involve them in the culture, develop clear policies and procedures, and integrate GRC into business processes and decision-making.

Regular communication and transparency about GRC efforts and outcomes are essential, including reporting to stakeholders and open discussions about GRC issues. Regular review and updates of GRC processes and practices are also necessary to maintain a culture of GRC and ensure ongoing optimization. By building a GRC culture, organizations can improve their management, enhance their reputation, and achieve their business objectives.

Encourage Proper Conduct

GRC encourages proper conduct by establishing a comprehensive framework for organizations to effectively manage their business and comply with standards and laws. This includes developing clear policies and procedures, providing training and awareness programs, conducting regular risk assessments, monitoring and auditing activities, establishing reporting for potential violations, and taking prompt and effective action to remediate any identified violations.

Together, these measures create a compliance and ethical behavior culture that minimizes risks and ensures proper conduct.

The governance that enables organizations to meet their business objectives by mitigating threats, ensuring accountability, maintaining legal compliance, and aligning resources to achieve business objectives.

Risk Awareness

GRC provides a structured approach to identify, assess, and manage risks, helping organizations maintain awareness of potential threats to their operations, financial stability, and reputation. The risk management component of GRC involves conducting a risk assessment and developing a plan to mitigate or manage risks effectively. This includes implementing policies, procedures, and technical controls to reduce the likelihood of risks occurring, continuously monitoring operations and systems, and providing training and awareness programs to employees.

Regular review and updates of risk management processes are also necessary to ensure their effectiveness and efficiency. By adopting GRC practices, organizations can stay ahead of potential risks and achieve their business objectives.

Boost Stakeholder Confidence

GRC helps organizations build stakeholder confidence by demonstrating compliance with regulations and standards, implementing good governance practices, managing threats effectively, and committing to continuous improvement. Compliance with guidelines and laws is crucial in maintaining stakeholder confidence, as it shows that the organization operates within a legal and ethical framework.

Regular review and updates of risk management processes are necessary.

Good governance practices, such as accountability, transparency, and ethical behavior, are essential in building stakeholder confidence, improving organizational performance, and avoiding reputational damage.

Effective threat management is another critical aspect of GRC that can boost stakeholder confidence. Organizations can reduce the likelihood of adverse events by implementing a structured management approach and maintaining operational stability. Regular review and updates of threat management processes and governance practices demonstrate a commitment to continuous improvement and responsible decision-making, further enhancing stakeholder confidence. Organizations can maintain stakeholder confidence over the long term by consistently committing to responsible risk management and regular progress.

Increase Efficiency

GRC establishes a structured approach to governance, risk management, and compliance, improving organizational efficiency and reducing the time and resources required for compliance. By streamlining processes, reducing effort duplication, and providing a comprehensive view of threats and requirements, GRC enhances decision-making and enables organizations to allocate resources more effectively.

Automating manual processes such as risk assessments, monitoring, and reporting increases efficiency, resulting in more accurate and consistent results. GRC also helps organizations identify and address potential compliance and ethical violations early on, leading to a more efficient resolution of issues.

Manage Business Consciously

GRC helps organizations manage their business consciously and responsibly by providing a framework for establishing clear policies and procedures, identifying and managing risks, ensuring compliance, promoting transparency, and continuously improving business practices. Compliance with standards, policies, and laws is an essential aspect of GRC that helps reduce the possibility of legal and financial penalties.

GRC promotes transparency in business practices by providing a mechanism for reporting potential violations and investigating incidents, promoting accountability and conscious behavior by employees. Regular monitoring and auditing of policies, procedures, and controls help organizations identify areas for improvement and promote a more mindful and sustainable business.

Optimize Profit

GRC helps organizations optimize profit by increasing operational efficiency, improving decision-making, ensuring compliance, and promoting a positive reputation and strong customer trust. By proactively identifying and managing potential risks, GRC reduces the likelihood of adverse events impacting profitability. Streamlining processes and automating manual tasks also increase efficiency and reduce costs, freeing up resources for other business areas. GRC provides a comprehensive view of compliance requirements, enabling informed and effective decision-making.

Maintaining a trustworthy reputation through GRC promotes ethical behavior, increases transparency, and builds customer trust, leading to long-term profitability.

Cybersecurity: The fundamentals

A proactive cybersecurity strategy is dynamic and provides a flexible approach to securing assets and minimizing risk. It should be developed with a three-to-five-year horizon and revisited frequently. A comprehensive cybersecurity strategy helps stakeholders:

- Align cybersecurity with the business
- Promote a security-aware culture
- Understand high-risk areas
- Identify risk, threat, and vulnerability quickly
- Enable business growth
- Make smart cybersecurity investments

Cybersecurity Benefits Secures Sensitive Asset

User authentication is a crucial aspect of cybersecurity, achieved through passwords, smart cards, or biometric authentication, and ensures that only authorized individuals access sensitive assets. Access control systems, such as role-based, rule-based, and discretionary control, provide an additional layer of security to prevent unauthorized access. Encryption converts data into a coded format, while data classification categorizes data based on sensitivity, ensuring that only those who need access can view it.

Network segmentation is another critical measure that limits the exposure of sensitive assets to potential threats by dividing a network into smaller segments to contain a breach.

The Emerging Threat Economy

The financial impact of cybercrime is staggering, with estimates suggesting losses in the trillions of dollars and increasing. Cybercriminals are skilled at stealing sensitive information through various methods, and security breaches affecting individuals and businesses are a frequent news topic. In 2016, the "Hackerpocalypse" report by Cybersecurity Ventures predicted that cybercrime would cost the world $6 trillion annually by 2021.*

Statistics from DataProt.net reveal that in 2020, the global cost of cybercrime reached $1 trillion, with an average cost of $3.86 million.** The increasing financial toll of cybercrime and the growing threat to personal privacy highlight the urgency for organizations and individuals to prioritize cybersecurity.

Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Read More

More Than 70 Cybercrime Statistics - A $6 Trillion Problem

Read More

Enhances Productivity

Cybersecurity protects sensitive information, reducing costs and time associated with recovering from a security breach. It also ensures reliable information systems and networks, reducing downtime and data loss. With the increasing use of cloud-based technologies and collaboration tools, cybersecurity ensures that information is securely shared and stored, enhancing collaboration and mobility.

Adequate cybersecurity controls streamline processes, increasing efficiency by automating and standardizing processes. Organizations can improve their productivity and overall efficiency by implementing a comprehensive cybersecurity program, ensuring a secure and reliable technology infrastructure.

Maintains Trust and Credibility

Compliance with data privacy and security guidelines demonstrates an organization's commitment to security and privacy, which is crucial in building and maintaining trust with customers and stakeholders. Transparency about measures to secure financial and personal data can build trust and increase customer confidence. Including information about established security controls, reporting security incidents, and preventive steps can further build trust with customers and shareholders alike.

In the event of a security breach, a prompt and effective response, including notifying customers promptly, can help minimize damage and restore confidence. A robust cybersecurity plan demonstrates a commitment to security, further enhancing trust and credibility with customers and stakeholders.

Improves Risk Profile

Cybersecurity measures can strengthen an organization's risk profile by reducing the likelihood and impact of cyberattacks and data breaches. Regular risk assessments and incident response planning are essential to identify and mitigate security weaknesses. Keeping software and systems current with security patches and updates is fundamental to preventing cyberattacks, and employee training can reduce the risk of unintentional exposure to sensitive information.

Encryption is critical in protecting sensitive information and improving an organization's risk profile, reducing the possibility of data breaches and cyber-attacks. Organizations can protect their brand reputation, maintain customer confidence, and avoid costly, time-consuming data breaches and recovery efforts with effective cybersecurity measures.

Positive Impact on the Bottom Line

Adequate cybersecurity controls can result in significant cost savings for organizations by reducing the likelihood and impact of security incidents. This can minimize expenses associated with such events and free up resources.

Strong cybersecurity measures can also build customer confidence and attract new customers as more consumers prioritize data privacy and security, helping organizations differentiate themselves from competitors. Adherence to data privacy and security directives can help organizations avoid costly fines and legal liabilities, protecting their brand reputation and improving their bottom line.

Protects Personal Data

Protecting personal data is a critical aspect of cybersecurity. Encryption is an effective tool to prevent unauthorized access to personal data, even if it is intercepted or stolen. Access controls, such as password policies, multi-factor authentication, and role-based access, help to ensure that only authorized individuals can access this information. Compliance with data privacy and security regulations is vital for protecting personal data.

These standards establish guidelines for collecting, storing, and processing personal information, and organizations must adhere to them to handle data appropriately. Robust security measures, such as regular security audits and incident response plans can help prevent and mitigate security incidents that may compromise personal data. Keeping software and systems up-to-date with the latest security patches and updates is also essential to reduce the risk of cyber-attacks and data breaches exposing personal data.

By prioritizing cybersecurity, organizations can protect personal data and maintain individuals' privacy and security, enhancing their reputation in the market.

Supports Remote Workforce

Cybersecurity is essential for supporting a remote workforce and protecting sensitive data. Secure remote access solutions, such as virtual private networks (VPNs) and encrypted connections, ensure remote workers can access company systems safely. Endpoint protection, including antivirus and anti-malware software and Mobile Device Management solutions (eg. SOTI, Airwatch, and MaaS360), helps secure and manage remote devices such as laptops, smartphones, and tablets.

Summary

GRC and cybersecurity work together to protect an organization's sensitive assets. GRC provides a framework for organizations to manage risks and ensure compliance with regulatory requirements, while cybersecurity focuses on safeguarding an organization's systems, networks, and data from potential cyber threats.

IntraSystems Advisory Division's guiding principle of "Driving Change by Empowering People" puts people first in an integrated approach to application modernization, cybersecurity, cloud, enterprise, and organizational change. With expertise across multiple industries and business functions, IntraSystems Advisory Division helps bring harmony to the delicate balance of people and digital.