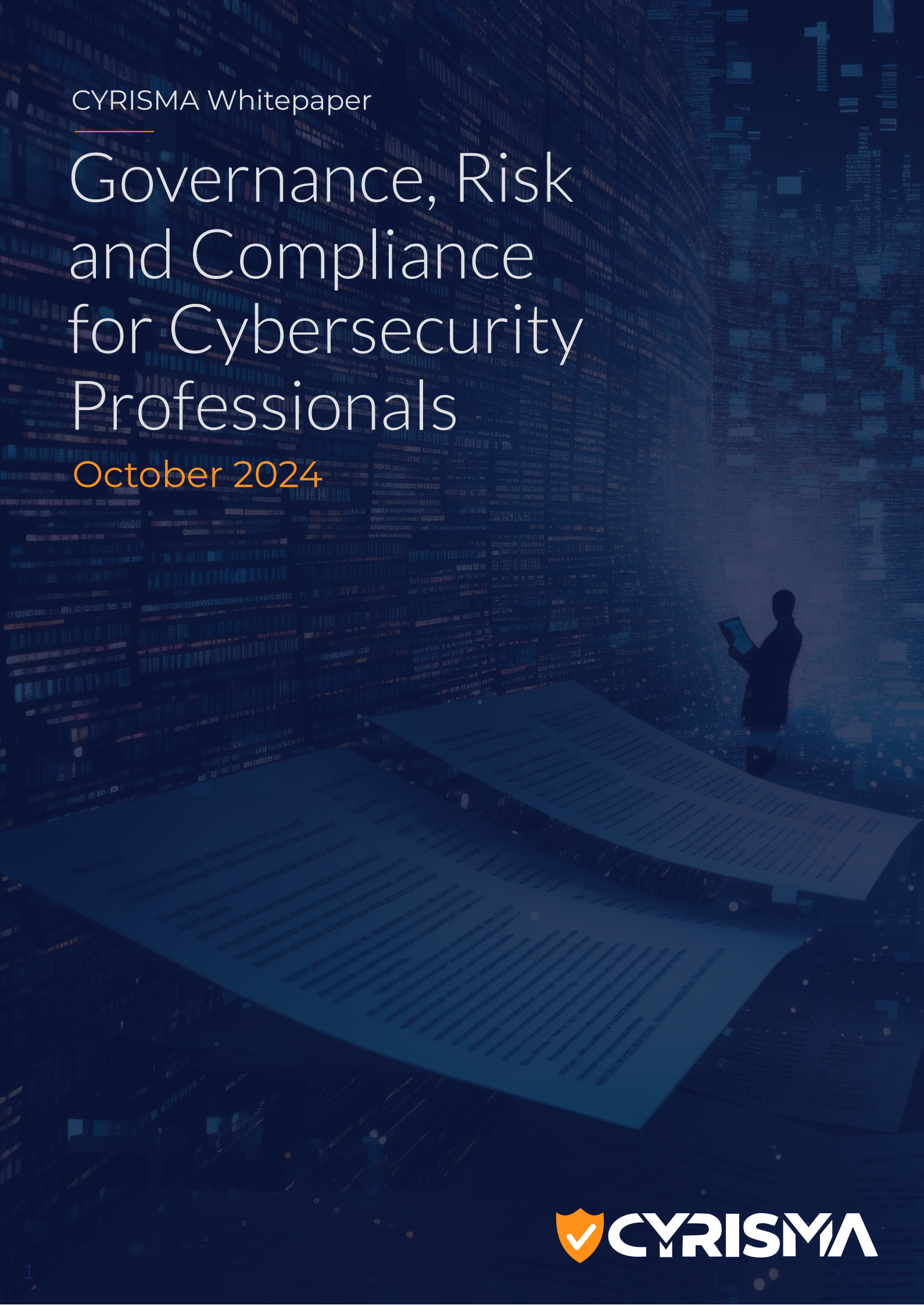
CYRISMA Whitepaper

Governance, Risk and Compliance for Cybersecurity Professionals

October 2024



CYRISMA

Table of Contents

1. Introduction

The convergence of escalating cyber threats, intensified regulatory scrutiny, and serious legal action following high-profile cyber incidents has propelled cybersecurity-focused Governance, Risk, and Compliance (GRC) to the forefront of organizational priorities. No longer just a compliance tick-box activity, GRC has evolved into a strategic necessity that underpins business resilience and sustainability.

1.1 - What this Whitepaper Covers

- **What GRC is:** What GRC is; how the term came into use; and what it means in relation to cyber risk management and data privacy compliance.
- **The Current Context**: The reasons for an increased focus on cybersecurity-focused GRC in recent years
- **GRC Frameworks**: How security frameworks help with streamlining GRC initiatives
- **GRC Tools and Platforms**: GRC Tools and what next-gen GRC platforms are offering to help manage cyber risk and compliance more effectively.

1.2 - What is Governance, Risk and Compliance (GRC)?

Governance, Risk, and Compliance (GRC) is a strategic approach to managing an organization's operations while meeting compliance requirements and minimizing risk that can impact mission-critical activities. It involves a structured framework for defining policies and processes (Governance), identifying and mitigating risks (Risk Management), and ensuring adherence to laws, regulations, and internal policies (Compliance).

The term GRC was first used by Forrester Research analyst Michael Rasmussen in 2002. He defined it as a capability to reliably achieve objectives while addressing uncertainty and acting with integrity. The three components - Governance, Risk, and Compliance - are interconnected and should be approached with a big-picture view to achieve long-term strategic success.

Understanding the three components of GRC

Governance

Governance sets the direction for an organization. It involves defining policies, roles, responsibilities, and decision-making processes. Effective governance ensures alignment with strategic objectives and regulatory requirements.

Risk Management

Risk Management focuses on identifying, assessing, and mitigating risks. It involves understanding the likelihood and impact of risks, and developing strategies to address them.

Compliance

Compliance ensures adherence to laws, regulations, industry standards, and internal policies. It involves implementing processes and controls to prevent violations and mitigate potential consequences.

2. Cybersecurity-Focused GRC: The Current Context

Over the past several years, the business and risk landscape (particularly cyber risk) has changed significantly, making GRC and the need to incorporate cyber risk into enterprise risk more critical. Several factors have contributed to this:

Cybersecurity Threats: High-profile data breaches, such as those suffered by SolarWinds and Uber, and the legal action that followed, have highlighted the devastating consequences of inadequate risk management.

Heightened Regulatory Scrutiny: The Securities and Exchange Commision's (SEC's) recent actions, including stricter disclosure requirements for cyber incidents, have underscored the importance of robust GRC practices.

Legal Liability: CISOs and other cybersecurity leaders are increasingly held accountable for cybersecurity incidents, emphasizing the need for strong GRC frameworks that incorporate clearly defined cyber risk management processes.

2.1 - Legal Action against SolarWinds and Uber following Data Breaches

SolarWinds

- **SEC Charges**: In the aftermath of the massive "Sunburst" supply chain attack in 2020 that compromised numerous government and private organizations, the SEC filed charges against SolarWinds and its former CISO, Tim Brown (in 2023). The SEC alleged that the company deliberately downplayed or failed to disclose cyber risks while overstating its security practices.

- **Allegations of Misleading Investors**: The SEC contended that SolarWinds made incomplete disclosures about the cyberattack, depriving investors of crucial information about the company's cybersecurity posture.

- **Charges Dismissed**: While most of the charges the SEC brought against SolarWinds were dismissed in July 2024, the case signifies a critical change in the CISO's role and scope of responsibility. Security leaders must work closely with business-focused execs on reducing cybersecurity risk and meeting regulatory compliance.

Uber

- **Criminal Conviction of Former CSO**: Uber's former Chief Security Officer, Joseph Sullivan, was found guilty of obstruction of justice and misprision for covering up a massive data breach in 2016.

- **Cover-up of Data Theft**: It was alleged that Sullivan attempted to conceal the incident by disguising a ransom payment as a bug bounty.

- **Importance of Timely Disclosure:** The case highlighted the critical importance of promptly disclosing data breaches to affected individuals.

These cases underscore the severe legal consequences for companies that fall victim to cyber-attacks and are unable to manage risk in a transparent and structured manner – before and after the breach. CISOs and other security leaders face increasing personal liability for security inadequacies and failures.

2.2 - Implications of these Cases for the Cybersecurity Industry

The SolarWinds and Uber cases and other high-profile data breaches have had profound implications for the cybersecurity industry, leading to significant shifts in regulatory, organizational, and technological landscapes.

The biggest lesson for cybersecurity professionals is to create strong connections between governance, risk management and compliance activities, so that each of the three components informs the other two. Some of the language in the legal action that followed these breaches referred to inconsistent communication and messaging internally and externally, with SEC filings going out without being vetted by cyber leaders.

It is absolutely essential for business and cyber leaders to communicate and get visibility into the others' domains. The organization's business objectives need to inform risk management, and cyber risks and compliance requirements in turn need to inform strategic business planning. Without creating strong links between the three, businesses run the risk of non-compliance and legal action following breaches.

Regulatory Changes

- **Increased Scrutiny**: Regulatory bodies worldwide are intensifying their oversight of cybersecurity practices. This includes more stringent reporting requirements, stricter penalties for non-compliance, and increased focus on supply chain security.
- **Data Privacy Laws**: The importance of robust data protection measures has been highlighted, leading to the strengthening of data privacy laws and regulations like GDPR and CCPA.
- **Cybersecurity Frameworks**: The adoption of cybersecurity frameworks like NIST Cybersecurity Framework and CIS Controls has become more prevalent across verticals. This year, both Frameworks were updated to include a cross-cutting Govern function to the five core functions included in earlier versions (Identify, Protect, Detect, Respond, Recover.)

Organizational Shifts

- **CISO Role Elevation**: The role of the Chief Information Security Officer (CISO) has become more strategic and influential. CISOs are now expected to be deeply involved in business decision-making and risk management.
- **Increased Security Investments:** Organizations are allocating more budget to cybersecurity initiatives, including advanced threat detection, incident response, and employee training.
- **Supply Chain Risk Management**: Companies are focusing on assessing and managing risks associated with their supply chain to prevent incidents like the SolarWinds attack.

Technological Advancements

- **Threat Detection and Response**: Investments in advanced threat detection technologies, powered by artificial intelligence and machine learning, have accelerated to improve incident response capabilities.
- **Zero Trust Architecture**: The adoption of zero-trust security models has gained momentum as organizations seek to strengthen their security posture.
- **Identity and Access Management**: Improved identity and access management practices are being implemented to protect sensitive data and systems.

2.3 - The 2023 SEC Ruling on Cyber Incident Disclosure

On July 26, 2023, the SEC adopted rules that required registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance. The rules became effective starting December 2023.

The incident disclosure is due four days after the registrant determines that the incident is material.
The new rules also require registrants to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents. These disclosures will be required in a registrant's annual report on Form 10-K.

Assessing the Materiality of Cyber Incidents

On a high-level, organizations can consider the following questions to assess material impact of an incident.

Financial Impact

- **Revenue Loss**: How much revenue will be lost due to the incident? This can include lost sales, decreased productivity, and increased costs.
- **Cost of Response**: What will be the costs associated with responding to the incident? This can include forensic investigations, legal fees, public relations efforts, and system restoration.
- **Market Valuation Impact**: How will the incident affect the organization's stock price and overall market valuation? This can include investor confidence, customer trust, and regulatory fines.

Operational Disruption

- **Business Continuity**: How will the incident impact the organization's ability to continue its operations? This can include disruptions to critical services, data loss, and supply chain disruptions.
- **Data Integrity**: Has the incident compromised the integrity of the organization's data? This can include data breaches, unauthorized access, and data corruption.

- **Service Delivery**: How will the incident affect the organization's ability to deliver its products or services to customers? This can include delays, disruptions, and quality issues.

Legal and Regulatory Compliance

- **Regulatory Penalties**: What fines or penalties could the organization face due to the incident? This can include violations of data privacy laws, industry regulations, and contractual obligations.
- **Litigation Risk**: What is the potential for lawsuits or other legal actions against the organization? This can include claims from customers, employees, or other stakeholders.
- **Breach Notification Requirements**: Does the organization have a legal obligation to notify customers or other stakeholders about the incident? This can include requirements for disclosure, remediation, and compensation.

Reputation and Trust

- **Brand Damage**: How will the incident affect the organization's reputation and brand image? This can include negative publicity, loss of customer trust, and damage to stakeholder relationships.
- **Customer Trust**: How will the incident impact customer trust and loyalty? This can include decreased customer satisfaction, increased churn, and difficulty acquiring new customers.
- **Stakeholder Confidence**: How will the incident affect the confidence of investors, employees, and other stakeholders? This can include decreased morale, difficulty attracting talent, and challenges in fundraising.

Strategic Impact

- **Competitive Advantage**: How will the incident affect the organization's competitive position in the market? This can include lost market share, increased costs, and decreased innovation.
- **Mergers and Acquisitions**: How will the incident impact the organization's ability to engage in mergers or acquisitions? This can include decreased attractiveness to potential partners, increased due diligence requirements, and challenges in integrating acquired businesses.

Scope and Scale

- **Scope of Impact**: What is the extent of the damage caused by the incident? This can include the number of affected systems, the amount of data compromised, and the geographic reach of the incident.
- **Scale of Breach**: How large and significant is the breach? This can include the number of records compromised, the sensitivity of the data, and the potential for widespread harm.

2.4 - The “Govern” Function in the NIST CSF and the CIS Controls

The importance of an integrated approach to GRC activities in the cybersecurity domain is reflected in changes to the NIST Cybersecurity Framework v2.0 and the CIS Critical Controls v8.1 this year. Both cybersecurity frameworks have now added a “Govern” function to their core functions (which previously included Identify, Protect, Detect, Respond and Recover).

NIST Cybersecurity Framework 2.0

In version 1.1 of the NIST CSF, governance-related activities were included under the “Identify” function. By placing these activities under a new, cross-cutting Govern function in version 2.0, NIST elevates the importance of aligning Cybersecurity Risk with Enterprise Risk.

The Govern function includes action categories for establishing and monitoring cyber risk strategy, expectations, and policy. The strategy direction set under it will inform the implementation of the five other functions. Within the Govern function, NIST lists the following main categories: Organizational Context; Risk Management Strategy; Cybersecurity Supply Chain Risk Management; Roles, Responsibilities, and Authorities; Policies, Processes, and Procedures; Oversight.

CIS Critical Controls 8.1

The latest version 8.1 of the CIS Controls, too, added a Govern function to the other five. The addition of Governance as a core component will enable users to identify the essential policies, procedures, and processes needed to safeguard their assets.

To support the Govern function, CIS added the asset type “Documentation” which includes Plans, Policies, Processes and Procedures. This will provide organizations with the evidence required to demonstrate compliance with industry standards.

3. Cybersecurity Frameworks and Data Privacy Regulations

Implementing GRC initiatives in a streamlined manner can be difficult because of the multiple interoperating domains and the specialized nature of some of the activities. Cybersecurity initiatives and legal operations are all specialized functions that need domain expertise. Furthermore, tying everything together in a way that ensures every activity is designed with the end goal of meeting business objectives is complex.

To make this process smoother, organizations can leverage readymade frameworks like the NIST Cybersecurity Framework or the CIS Critical Controls discussed above. These frameworks provide a structured approach to managing GRC activities, with a cyber-focused perspective, and can be customized based on specific business needs.

3.1 - Key Benefits of Using GRC Frameworks

- **Structured Approach**: Frameworks offer a clear roadmap for identifying, assessing, and mitigating cybersecurity risks.
- **Industry Best Practices**: They incorporate proven industry standards and best practices, ensuring alignment with established guidelines.
- **Compliance Support**: Frameworks assist in meeting regulatory requirements, such as PCI DSS, HIPAA, and GDPR.
- **Risk Management**: They provide a systematic way to identify and prioritize risks, enabling organizations to allocate resources effectively.

3.2 - Difference Between Security Frameworks and Privacy Standards & Regulations

The key difference between a cybersecurity framework and a regulatory standard is that a framework is a voluntary set of best practices while a regulation needs to be complied with as a legal obligation or requirement.

Cybersecurity Framework

A Cybersecurity Framework is a set of best practices designed to help organizations manage and reduce cybersecurity risks. Frameworks are often voluntary and provide flexible approaches that can be tailored to an organization's specific needs. They offer a systematic way to assess and improve security posture. Examples include the NIST Cybersecurity Framework (CSF), ISO 27001, COBIT.

Data Privacy Regulation or Standard

A data privacy regulation is a legal requirement that organizations must comply with to meet industry-specific or governmental regulations related to data protection. Compliance with regulatory standards is mandatory, and organizations face legal consequences for non-compliance. Examples include GDPR, HIPAA, PCI DSS, CCPA.

3.3 - Popular Cybersecurity-focused GRC Frameworks

NIST Cybersecurity Framework

Developed by the National Institute of Standards and Technology, the NIST Cybersecurity Framework provides a flexible and adaptable framework for managing cybersecurity risks. It is divided into six core functions: Govern, Identify, Protect, Detect, Respond, and Recover.

CIS Critical Security Controls

Developed by the Center for Internet Security, the CIS Control offers a prioritized list of 18 controls that address the most critical security risks. The controls are applicable to a wide range of organizations, and are divided into Implementation Groups for easier prioritization based on maturity level, size and specific requirements.

ISO 27001

The ISO 27001 is an international standard for information security management and provides a comprehensive framework for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). ISO 27001 is based on a risk-based approach and requires organizations to identify and assess their risks, implement appropriate controls, and monitor their effectiveness.

COBIT 5

A framework for governance and management of enterprise IT, COBIT 5 provides a comprehensive set of principles, practices, and tools for IT governance. COBIT 5 is based on five principles: relevance, efficiency, effectiveness, reliability, and conformance.

NIST Special Publication 800-171

NIST 800-171 outlines security requirements for protecting Controlled Unclassified Information (CUI) in non-federal systems. It provides 14 families of security controls, covering areas like access control, encryption, incident response, and risk assessment. The framework helps contractors and organizations working with the government secure sensitive data and ensure compliance with regulations such as DFARS.

The ACSC's Essential Eight and the UK NCSC's Cyber Essentials

The ACSC Essential Eight is an Australian cybersecurity framework focusing on eight key mitigation strategies to protect systems, including patching, backups, and access management. The NCSC Cyber Essentials, from the UK, outlines five basic security controls like firewalls and malware protection. Both frameworks aim to help organizations defend against common cyber threats and reduce risks effectively.

3.4 - Data Privacy Regulations

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a set of security standards designed to protect cardholder data. It requires organizations that handle credit card transactions to implement specific security measures to prevent data breaches. These measures include protecting cardholder data, maintaining secure networks, and regularly monitoring and testing networks.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a U.S. federal law that sets standards for the privacy and security of protected health information (PHI). It applies to healthcare providers, health plans, and their business associates. HIPAA requires covered entities to implement safeguards to protect PHI from unauthorized access, use, disclosure, or modification.

General Data Protection Regulation (GDPR)

The GDPR is a European Union regulation that governs how organizations collect, store, and use personal data. It emphasizes individual rights, requiring consent for data processing and ensuring data subjects can access, correct, or delete their information.

California Consumer Privacy Act (CCPA)

The CCPA is a U.S. regulation providing California residents with the right to know what personal data is collected, request its deletion, and opt-out of its sale. It holds businesses accountable for data protection and transparency.

3.5 - Implementing a Cybersecurity Framework

- **Framework Selection**: Choose a framework that aligns with your organization's size, industry, and specific requirements.
- **Mapping to Organizational Processes**: Identify existing processes and procedures that can be mapped to the framework's components.
- **Customization**: Tailor the framework to fit your organization's unique needs and risk profile. This may involve adding or removing controls, mapping controls to regulatory needs, or modifying methodology, etc.
- **Implementation**: Implement the framework's components, including risk assessment, control implementation, and monitoring.
- **Continuous Monitoring and Improvement**: Regularly review and update the framework to ensure it remains effective and aligns with evolving threats and regulatory requirements.

4. GRC Tools for IT and Cybersecurity Professionals

GRC tools are software solutions that streamline and automate various aspects of governance, risk management, and compliance. These tools enable organizations to centralize their GRC activities, making it easier to track compliance requirements, assess risks, and implement controls. They also provide dashboards and reporting features that offer real-time visibility into your organization's GRC status, allowing for quicker decision-making and proactive risk management.

4.1 - The Benefits of GRC Tools

Choosing the right GRC tool is crucial because it directly impacts how effectively you can manage risks and ensure compliance. The right tool not only streamlines GRC processes but also provides the insights and capabilities necessary to protect your organization in an increasingly complex and regulated digital landscape.

Risk Management Effectiveness

The right GRC tool allows your organization to accurately identify, assess, and mitigate risks. It helps prioritize risks based on their potential impact, ensuring that critical vulnerabilities are addressed promptly. An inadequate tool may leave gaps in your risk management process, exposing your organization to potential threats.

Regulatory Compliance

Compliance with industry regulations and standards is essential to avoid legal penalties, protect your reputation, and maintain customer trust. A robust GRC tool ensures that your organization stays compliant by automating the tracking of regulatory requirements, generating necessary reports, and providing alerts for any compliance issues.

Operational Efficiency

Managing GRC activities manually or with disparate tools can be time-consuming and prone to errors. The right GRC tool centralizes and automates these activities, improving operational efficiency, reducing redundancy, and freeing up resources for more strategic tasks.

Data Centralization and Visibility

A comprehensive GRC tool offers a unified platform where all GRC-related data is stored and accessible. This centralization provides a clear, real-time view of your organization's risk and compliance posture, enabling better decision-making and faster responses to emerging threats and noncompliance issues.

Scalability and Flexibility

As your organization grows or faces new challenges, your GRC tool should scale and adapt accordingly. Choosing the right tool ensures that it can evolve with your needs, supporting additional users, processes, and regulatory requirements without significant reconfiguration or replacement.

4.2 - Key Features to Consider When Choosing a Cybersecurity GRC Tool

Get a deep understanding of existing compliance processes and requirements, and research options carefully before making a final decision on the best GRC tool or platform for your organization.

Compliance Coverage

Ensure the tool covers all relevant regulatory standards applicable to your industry, such as GDPR, HIPAA, PCI DSS, etc. It should be able to track changes in regulations and automatically update requirements.

Risk Assessment and Management

Look for robust risk assessment capabilities that allow you to identify, evaluate, and prioritize risks. Ideally, the tool you choose should not just help with gap assessments but also help you reduce risk and close the gaps.

Integration Capabilities

The tool should seamlessly integrate with your existing IT infrastructure, including security, IT, and business applications. Integration with other tools like SIEM systems, and identity management solutions would be ideal.

Reporting and Analytics

The ability to generate detailedreports is critical. Look for a tool that offers advanced analytics, dashboards, and reporting features to monitor your GRC activities, assess performance, and make data-driven decisions.

Automation and Workflow Management

Automation is key to reducing manual effort and improving accuracy. The tool should automate routine tasks such as policy management, control assessments. Workflow management features should enable collaboration, task delegation, and deadline tracking across teams.

User-Friendliness and Accessibility

A GRC tool should be intuitive and easy to use, with a user-friendly interface that requires minimal training. Consider tools that offer the ability to provide control to multiple stakeholders for easy collaboration.

Vendor Support and Updates

Reliable vendor support is crucial for addressing issues, deploying updates, and ensuring the tool evolves with new threats and regulations. Consider the vendor's reputation, the frequency of updates, and customer support.

Cost and Total Value

Evaluate the total value the tool provides. Assess whether the features, support, and scalability justify the investment. Consider the potential savings in time, reduced risk exposure, and improved compliance.

4.3 - The Next Generation of GRC Tools

What's the future of Governance, Risk and Compliance (GRC) tools? We believe that in the cybersecurity domain, GRC tools will increasingly bring together the tactical and strategic components of compliance and cyber risk management. This means that unlike traditional GRC tools that are primarily compliance and policy-focused – new and emerging solutions will allow organizations to:

- View, track and assess compliance requirements across frameworks and standards
- Discover, assess and reduce cyber risk (system vulnerabilities, threats to data, and more)
- Measure the financial impact of cyber risk
- Map risk to compliance requirements
- Close both cybersecurity and compliance gaps in a holistic manner

Bridging the Gap Between Policy and Execution

Next-generation GRC tools are designed to bridge the gap between policy and execution by providing capabilities that extend beyond traditional checklists and static reports. These tools enable organizations to:

- **Track and Manage Compliance**: Monitor both existing controls and any new controls required to meet evolving compliance needs.

- **Directly Implement Tactical Controls**: Move from merely identifying compliance requirements to actively executing controls that ensure compliance, all within the same platform.

- **Develop a Unified Approach**: Integrate gap assessments, mitigation plans, and proof of control implementation into a single workflow, making the entire GRC process seamless and efficient.

Consider the Following Questions in Addition to the Features Listed on the Previous Page

To build and implement a truly effective GRC strategy, consider a few key questions that tie together Governance, Risk and Compliance. Addressing the following questions will help your organization visualize and build a continuous flow between the different components of GRC.

- What are your key business goals? How can cyber attacks hurt your business's bottomline (revenue)?

- What regulations apply to your industry and your specific business? What are the costs of non-compliance?

- Do you use a cybersecurity framework? Does this framework map to the regulations and standards your organization must adhere to?

- How are you currently managing and documenting cyber risk and compliance? Do you quantify cyber risk (Do you know what a data breach would cost your company?)

The GRC tool you acquire should function as a single source of truth for the cyber risk and compliance status of your organization and also help you address the questions listed above.

4.4 - CYRISMA Cyber Risk Management and Compliance Platform

CYRISMA brings together essential risk management and compliance assessment capabilities in a unified platform. Developed for organizations looking to reduce risk in a holistic, measurable and cost-effective manner, CYRISMA makes GRC simpler by providing all-round visibility into both cyber risk and evolving compliance needs.

What makes CYRISMA truly effective as a GRC tool is that in addition to assessment capabilities, it also includes the ability to implement controls to shrink compliance gaps.

Platform features include internal, external, agentless and agent-based vulnerability scans, patching for Windows-based third-party apps, sensitive data discovery in both on-prem and cloud environments, dark web monitoring, financial impact estimates, secure configuration scanning, compliance tracking and assessment, and much more. Run scans to discover, assess and mitigate risk, and assess compliance with multiple frameworks (CIS Critical Controls, NIST CSF, HIPAA, PCI DSS, Essential Eight, Cyber Essentials, Microsoft Copilot Readiness, and more.)

Core Cybersecurity Compliance Features

- Review full list of controls and requirements in one dashboard
- Get an overview of progress status on the main compliance dashboard
- Auto-track tactical controls implemented using CYRISMA
- Provide control and assign tasks to other teams, upload docs as evidence
- Review and resolve blocks, close compliance gaps
- Generate comprehensive report with tailored recommendations

Virtual CISO Action Plans: Leverage ready-to-use policy and program templates based on cybersecurity maturity.

Frameworks and Standards Covered (more frameworks to be added soon)

- NIST Cybersecurity Framework
- CIS Critical Security Controls
- HIPAA (for healthcare data)
- PCI DSS (payment card data)
- The Essential 8 (Australia)
- CyberSecure Canada
- Microsoft Copilot Readiness Assessment
- The Cyber Essentials (UK)

For more information on CYRISMA's GRC module and complete feature-set, go to our Cybersecurity Compliance Software page.

All of CYRISMA's features and future updates are included in the standard pricing. CYRISMA is priced per endpoint (where endpoints include desktops, laptops and servers.) All other IP-connected devices are included and can be scanned AT NO ADDITIONAL COST.

Email us at info@cyrisma.com for more information.

+1 585-620-2496
www.cyrisma.com
info@cyrisma.com