LevelBlue

SERVICE BRIEF

LevelBlue Managed GRC: Transforming Risk and Compliance Into Strategic Advantage

GRC is a strategic framework that helps organizations align with relevant security regulations and frameworks.

Organizations now operate in an environment of rapidly proliferating regulations, expanding digital boundaries, and increased data sprawl. This evolution has fundamentally changed how businesses must approach cybersecurity governance, risk, and compliance (GRC).

Challenges

With the rapid pace of digital transformation and emerging threats backed by AI, organizations continue to struggle to effectively identify, assess, and mitigate cyber risks.

In addition, security and risk teams often have limited tools and personnel, making it difficult to allocate sufficient resources with the specialized knowledge required to manage comprehensive GRC frameworks effectively.

Disconnected processes and siloed departments can also lead to inefficiencies and errors, making it hard to maintain a cohesive approach to GRC. Without a streamlined GRC framework in place, organizations experience redundant processes and a lack of coordination and awareness between departments.

Non-compliance can be expensive, leading to substantial fines, legal consequences, and reputational harm. In fiscal year 2024, the U.S. Securities and Exchange Commission filed 583 enforcement actions and obtained orders totaling $8.2 billion, the highest in SEC history.

LevelBlue Managed GRC

LevelBlue Managed GRC services are designed to transform fragmented security and compliance processes into a unified, effective framework. This enables organizations to confidently navigate complex regulatory requirements while strengthening cyber resilience. Our services are supported by experienced risk and compliance specialists, delivering measurable outcomes.

Unified Governance Framework

Our security advisors develop strategies and governance frameworks tailored to your specific risks, threats, and compliance requirements, ensuring alignment with your goals and organizational culture.

In addition, we help our clients change outdated practices, bridge organizations silos, and drive operational scalability, transparency, and standardization by leveraging integrated GRC solutions.

Visibility Into Your Risk Landscape

LevelBlue supports clients with the evaluation, design, implemention, and ongoing management of their cyber risk management program. We provide a comprehensive view of risk and recommendations for improvement, with risk reduction measurement technology. This allows you to make more informed decisions and operate with accountability and transparency.

By adhering to formalized risk management standards, organizations ensure ongoing compliance and build stronger risk management cultures, improving the reliability of daily operations.

The LevelBlue platform is designed to support compliance efforts and risk visibility. Use of the platform does not guarantee compliance outcomes. Actual results may vary based on individual enterprise requirements and implementation. No part of this document constitutes a guarantee of performance or outcome.

Compliance Assurance
Updated laws and regulations require organizations to improve gaps in data privacy, cybersecurity, and corporate governance. LevelBlue evaluates your organization against relevant regulatory requirements (e.g., HIPAA, PCI-DSS, CMMC) and frameworks (e.g., ISO 27001, NIST), and then provides a prioritized roadmap for achieving and sustaining compliance. We can provide full lifecycle management through an integrated compliance management system that offers dashboards and evidence collection. We monitor compliance-related activity with real-time alerts, automated reporting, and proactive remediation of compliance issues.

Resource and Expertise
LevelBlue considers a client's business objectives, risk appetite, security culture, budget, industry, and internal security policies and then provides tailored guidance via LevelBlue consulting and professional services. We also provide virtual CISO and compliance specialist services to support strategic planning, risk management oversight, and compliance program development.

Service Tiers

LevelBlue offers flexibility through three Managed GRC service tiers: Essentials, Advanced, and Premium. Each tier gives clients a monthly allotment of hours with an experienced vCISO and a compliance specialist. Clients choose the service tier that best fits their needs, whether to establish or refresh an existing program, develop deeper, more proactive risk management and compliance oversight, or address complex risk management and documentation requirements.

The LevelBlue platform is designed to support compliance efforts and risk visibility. Use of the platform does not guarantee compliance outcomes. Actual results may vary based on individual enterprise requirements and implementation. No part of this document constitutes a guarantee of performance or outcome.

Managed GRC Service Tiers

COMPONENT	ESSENTIALS	ADVANCED	PREMIUM
vCISO (Monthly Hours)	20	50	85
Compliance Specialist (Monthly Hours)	40	60	80

COMPONENT		ESSENTIALS	ADVANCED	PREMIUM
Security Strategy and Roadmap	Stakeholder interviews	**3**	**6**	**9**
	Review documents for strategy and roadmap creation	**6**	**12**	**15**
	Creation of 12-month strategy	Included	Included	Included
	Prioritized roadmap implementation timeline		Included	Included
Risk Management	Security Risk Assessment	Included	Included	Included
	Report on critical and high impact risks	Included		
	Risk Register		Included	Included
	Cyber Risk Management Plan			Included
Security Policy and Documentation	Development or maintenance of basic security policies and documentation	Included	Included	Included
	Strategic direction and tactical review of policies, standards and prioritized procedures		Included	Included
	Full management of compliance documentation			Included
Third-Party Risk Management	Advisory support for identifying third parties	Included	Included	Included
	Tracking basic risk information	Included		
	Vendor list with basic risk categorization	Included		
	Minimal automation for formal processes	Included		
	Advisory support on due diligence		Included	
	Build and implement strategy for identifying and prioritizing high risk vendors		Included	
	Strategic focus on vendors that matter most		Included	
	Full TPRM vendor program roll out			Included
	Ongoing oversight			Included
	Auditable program with continuous improvement cycles			Included

The LevelBlue platform is designed to support compliance efforts and risk visibility. Use of the platform does not guarantee compliance outcomes. Actual results may vary based on individual enterprise requirements and implementation. No part of this document constitutes a guarantee of performance or outcome.

COMPONENT		ESSENTIALS	ADVANCED	PREMIUM
Security Awareness and Training	Annual onboarding and refresher training for all employees	Included	Included	Included
	Quarterly lunch and learns		Included	Included
	Complete training program and roll out of content			Included
Audit Preparation	Reactive Guidance	Included		
	External Audit support		Included	
	Full Audit readiness			Included
Executive Reporting	Quarterly report included high-level summary	Included		
	Bi-Monthly reports include KPIs, project milestones, and new risks		Included	
	Monthly reports include trending risks, training completion, open findings			Included
Access to GRC Platform	Centralized platform with real-time visibility	Included	Included	Included

Managed GRC Service Components

- **Virtual CISO (vCISO) Support:** vCISO provides dedicated access to a senior security advisor who provides strategic leadership for an organization's cybersecurity program. LevelBlue's vCISO aligns security initiatives with business goals, delivers board-ready insights, oversees risk and compliance activities, and helps shape long-term security roadmaps.
- **Compliance Specialist:** Get a hands-on resource to support tactical compliance and documentation work, such as drafting policies, tracking audit items, and managing regulatory mappings. The compliance specialist manages the daily demands of compliance frameworks and supports audit readiness through structured documentation and follow-up.
- **Security Strategy and Roadmap:** LevelBlue provides a structured plan, aligned with recognized frameworks (e.g., NIST, ISO 27001) and business goals. The vCISO begins by assessing the current state of an organization's security program through stakeholder interviews and document reviews (depth varies by service tier). Based on these insights, the vCISO crafts a future-state vision and builds a strategy with a 12-month roadmap that includes prioritized initiatives, timelines, dependencies, and resource needs.
- **Risk Management:** LevelBlue starts with a comprehensive assessment of an organization's attack surface and cybersecurity risk posture that identifies, evaluates, and prioritizes exposures. We document and provide recommendations for risk reduction, using technology to help track, prioritize and remediate risk continuously.
    - **Risk Register:** The LevelBlue risk register is a structured document that captures and tracks organizational risks, including details such as description, impact likelihood, owner, mitigation strategies, and status. It supports risk prioritization, accountability, and ongoing monitoring, providing visibility for audits, leadership, and compliance reporting.
    - **Cyber Risk Management Plan:** Get a formal plan that outlines how your organization identifies, assesses, mitigates, monitors, and reports cyber risks over time. The plan establishes risk appetite and integrates into an organization's risk management strategy.

The LevelBlue platform is designed to support compliance efforts and risk visibility. Use of the platform does not guarantee compliance outcomes. Actual results may vary based on individual enterprise requirements and implementation. No part of this document constitutes a guarantee of performance or outcome.

- **Security Policy and Documentation:** LevelBlue develops and implements security policies, standards, and guidelines tailored to an organization’s needs, ensuring alignment with business goals, regulatory requirements, and cybersecurity frameworks (e.g., NIST, ISO 27001). Our Essentials service tier starts with the development or maintenance of basic security policies, the Advanced tier expands on this by adding strategic guidance and a tactical review of policies, standards, and prioritized procedures, and the Premium tier includes all the above with full management of compliance documentation.
- **Third-Party Risk Management:** Reduce vendor-related risks by combining vCISO and compliance expertise with a cybersecurity scoring platform. This service streamlines compliance, automates workflows, and enables risk-based vendor categorization and monitoring.
  - **Advisory and Tracking:** Identify vendors and track basic risk details such as contract status, service type, and compliance posture. The Essentials tier offers lite guidance and a basic risk-categorization vendors list. Advanced adds support for reviewing critical vendors and applying targeted risk controls. Premium includes full program management of third-party risk, with shared execution and audit-ready governance.
  - **Strategy and Focus on High-Risk Vendors:** Create a focused strategy to identify and prioritize high-risk vendors. We define risk tiers, scoring logic, and establish review cadences, while supporting due diligence (e.g., SOC 2 and contract reviews). Execution is shared between the organization’s team and our vCISO or advisor.
  - **Full Vendor Program Roll Out and Ongoing Oversight:** A fully developed Third-Party Risk Management program covers the entire lifecycle, including vendor intake, onboarding, risk tiering, due diligence, contract review, and ongoing monitoring. LevelBlue works with clients to establish or improve policies and processes, stakeholder training, and executive-level reporting. The vCISO and compliance specialist, with internal stakeholders, provide shared ownership and oversight.

Security Awareness and Training: Take advantage of a behavioral training program with interactive modules on user awareness, role-specific topics, and compliance. Each module includes a quiz for reinforcement.

- **Onboarding and Training Content:** Develop or provide security awareness training for new hires and an annual refresher for all employees. Cover general topics: phishing, passwords, acceptable use, remote work. (Program does not include behavior testing or deep culture change.)
- **Quarterly Lunch and Learns:** Delivered live or recorded, these interactive sessions offer phishing deep dives, social engineering, secure collaboration guidance, and more.
- **Complete Training Program and Roll Out of Training Content:** Get comprehensive onboarding, user segmentation, gamified and measurable training, phishing simulations, automated reminders, dashboards, and role-based learning tailored to your workforce.

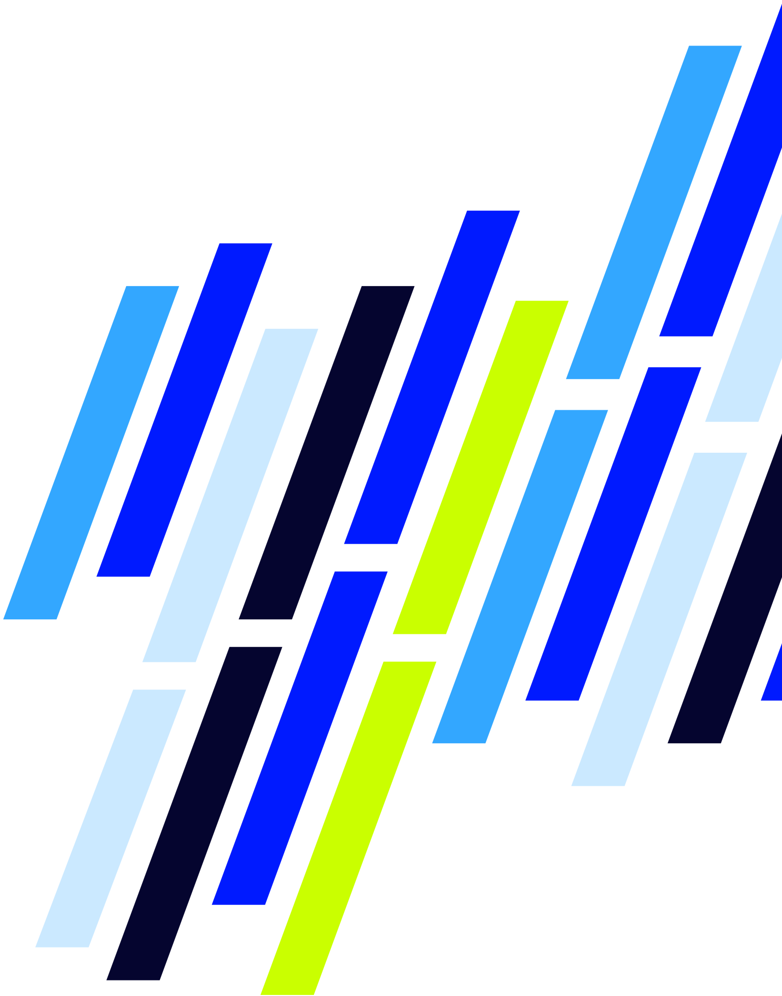
Audit Preparation: Get support preparing for audits by aligning documentation, controls, and evidence with industry and regulatory requirements. LevelBlue helps reduce audit fatigue and improve outcomes, with support for audit readiness.

- **Reactive Guidance:** Use limited support in answering audit-related questions and recommending templates or controls aligned with relevant compliance regulations.
- **External Audit Support:** Take advantage of hands-on assistance throughout the external audit process. LevelBlue can organize and present relevant evidence, write audit response documentation, support your team during audit events, and join auditor meetings.
- **Full Audit Readiness:** Receive end-to-end support that includes proactive planning and a dry run to simulate the audit, an internal gap analysis to identify compliance deficiencies, the preparation of necessary documentation, and tracking remediation efforts to ensure timely resolution.

The LevelBlue platform is designed to support compliance efforts and risk visibility. Use of the platform does not guarantee compliance outcomes. Actual results may vary based on individual enterprise requirements and implementation. No part of this document constitutes a guarantee of performance or outcome.

Executive Reporting: LevelBlue summarizes an organization's key risks, ongoing initiatives, and audit or compliance updates with relevant metrics.

- **Quarterly Reports:** A high-level summary of key risks, initiatives, and audit or compliance highlights, the report is delivered as an executive summary via email.
- **Bi-Monthly Executive Reports:** More frequent, moderately detailed updates, bi-monthly reports include key performance indicators, project milestones, and new risks, delivered in a PowerPoint format for active oversight.
- **Monthly Executive Reports:** More detailed insights on trending risks, training completion, and open findings, these reports are delivered via email with an attached dashboard in PowerPoint.
- **GRC Platform:** LevelBlue's centralized platform offers real-time visibility into an organization's risk, compliance, and governance activities. It streamlines processes, improves decision-making, and ensures alignment between security efforts and business goals. The platform simplifies audits, reporting, and regulatory compliance. All three service tiers include access to this GRC platform.



Managed GRC with LevelBlue

LevelBlue stands as your premier security partner, delivering transformative GRC solutions through unmatched expertise and flexible engagement models. Our team of highly certified consultants bring 30+ years of industry experience, global recognition, and specialized credentials as a PCI QSA Company, HITRUST External Assessor organization, and a CMMC Registered Provider Organization (RPO). Through strategic technology partnerships and our adaptable service delivery approach, we seamlessly integrate with your existing infrastructure while providing the specialized knowledge necessary to navigate complex regulatory requirements. By partnering with LevelBlue, you gain a trusted advisor committed to enhancing your cybersecurity posture, ensuring operational efficiency, and protecting your organization's reputation in today's increasingly challenging threat landscape.

The LevelBlue platform is designed to support compliance efforts and risk visibility. Use of the platform does not guarantee compliance outcomes. Actual results may vary based on individual enterprise requirements and implementation. No part of this document constitutes a guarantee of performance or outcome.

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Contact us to learn more, or speak with your LevelBlue sales representative.

The LevelBlue platform is designed to support compliance efforts and risk visibility. Use of the platform does not guarantee compliance outcomes. Actual results may vary based on individual enterprise requirements and implementation. No part of this document constitutes a guarantee of performance or outcome.