LevelBlue

PRODUCT BRIEF / MAY 2024

Align your Company Security with your Business Goals

The role of a security strategy is to align company security and business goals, provide a common security program framework to focus efforts and optimize compliance efforts, and ultimately use security as a business enabler.

The Strategy and Roadmap service delivers the expert resources, knowledge, and methodologies to assist you in building a complete unified information security program or individual elements within the existing security program (e.g., Incident Management Program or Threat and Vulnerability Management Program) to guide security efforts. This offering provides a solid foundation for a security program built upon risk management principles and achieving compliance with industry and governmental requirements.

Security Strategy

With technology rapidly evolving, organizational security requirements may not be integrated in your company's planning and design standards, resulting in technology and practices that are not aligned with existing efforts or future company initiatives. With the advent of wireless and mobile networking, Web 2.0, globalization, feature-rich applications, and much more data being collected, analyzed, and shared than ever before, security is sometimes an afterthought and can leave an enterprise vulnerable to attack from outside or from within. These attacks can compromise enterprise business processes, result in fraud and theft of trade secrets, and undermine a company's reputation with its customers.

In addition to pressures from possible attackers, regulatory pressures are expanding the requirements for information security and can impact different portions of the company in various ways. Legislation such

Potential Benefits

- Identify and prioritize strategic objectives
- Align security with business objectives
- Aid in effective implementation and operation of security processes and technologies
- Increase return on security investment

Features

- Needs Analysis and Framework Establishment
- Risk Assessment and Analysis
- Strategy Development
- Roadmap Development

as Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), and more recently, Health Information Technology for Economic and Clinical Health Act (HITECH), and various breach notification laws have impacted businesses large and small and frequently have left them in a reactive state. The breadth of legislation coming from governmental and industry regulatory agencies assures that almost every business is affected in some way. This reactive posture frequently leads to overlapping initiatives that can still leave gaps in the overall security program, while costing too much time and money to implement.

To make sense of all these threats and regulations, and to ensure that your company's information security program meets its requirements across the board, it is vital to have one enterprise security strategy and one information security framework. Putting in a solid foundational program is the first step in unifying your information security approach, proceeding with one clear plan, and implementing controls in a logical and efficient manner. Roadmaps can help focus efforts and plan budgets to ensure timelines are met with efficient expenditure of resources. An enterprise-wide security strategy and framework also has the effect of unifying the security efforts of multiple stakeholders in a large or highly distributed enterprise, across affiliate organizations, and between lines of business and IT. In addition, taking this type of structured, enterprise-wide approach also enables firms to undergo acquisition, and divestiture activities much more smoothly.

Solution

The first step in our Security Strategy engagements is determination of the specific requirements that must be addressed by the information security program in the organization; these requirements can be external (e.g., regulations) or internal (e.g., Enterprise Risk Management [ERM] mandates).

Subsequently, we will evaluate relevant information security frameworks in the context of the requirements previously determined. As frameworks themselves are not sufficient to create a practical strategy, LevelBlue Consulting will evaluate the current threats, exposures, and general IT controls in your organization. The general IT controls gap analysis will be conducted against the selected framework, relevant requirements, and identified threats and exposures. Subsequently, we will develop a strategy and an associated roadmap based on the current posture, requirements, current threat landscape, and the selected framework. The strategy and roadmap development work could lead to one or more subsequent LevelBlue certifications (see other product briefs for specific offerings).

The key activities of our Security Strategy and Roadmap services include:

- Needs Analysis and Framework Establishment
- Risk Assessment and Analysis
- Strategy Development
- Roadmap Development

Needs Analysis and Framework Establishment

LevelBlue Consulting will begin by understanding the client environment, gathering a comprehensive set of internal and external requirements for the information security program, and recommending an appropriate information security framework. LevelBlue Consulting recommends industry standard frameworks (such as ISO 27002, Health Information Trust Alliance [HITRUST] Common Security Framework [CSF], etc.) and will customize the framework to meet your specific requirements.

Risk Assessment and Analysis

A risk assessment, and subsequent analysis, are then used to augment the information security requirements gathered in the previous step by:

- Capturing the relevant threat landscape
- Determining quality and comprehensiveness of existing general IT controls

- Identifying general IT controls, gaps, and deficiencies in the context of the selected information security framework and relevant exposures

LevelBlue Consulting will begin by performing a Threat Assessment, followed by an Exposure Identification, and Risk Assessment of the entire enterprise or specific environment(s) in scope. Subsequently, a general IT controls gap analysis will be performed against the information security framework selected in the previous step and relevant exposures determined during the Exposure Identification step. Lastly, a comprehensive report outlining the overall findings and specific results will be provided to your organization.

Strategy Development

The Security Strategy will provide the guidance necessary for your organization to address the requirements previously identified, and mitigate risks to an acceptable level by implementing general IT controls, minimizing exposures, and other means. The Security Strategy will also allow for proper budgeting for security initiatives and a defendable prioritization model for implementation of these initiatives. Our Security Strategies are based on metrics computed by mapping control deficiencies and ineffectiveness to information asset groups, regulatory requirements, previous losses, and current exposures and threats.

Roadmap Development

LevelBlue Consulting assists your company with the development of a high-level roadmap to guide the transition to your desired information security program. Short-, medium-, and long-range goals and objectives are provided, along with priorities and approximate levels of difficulty and effort.

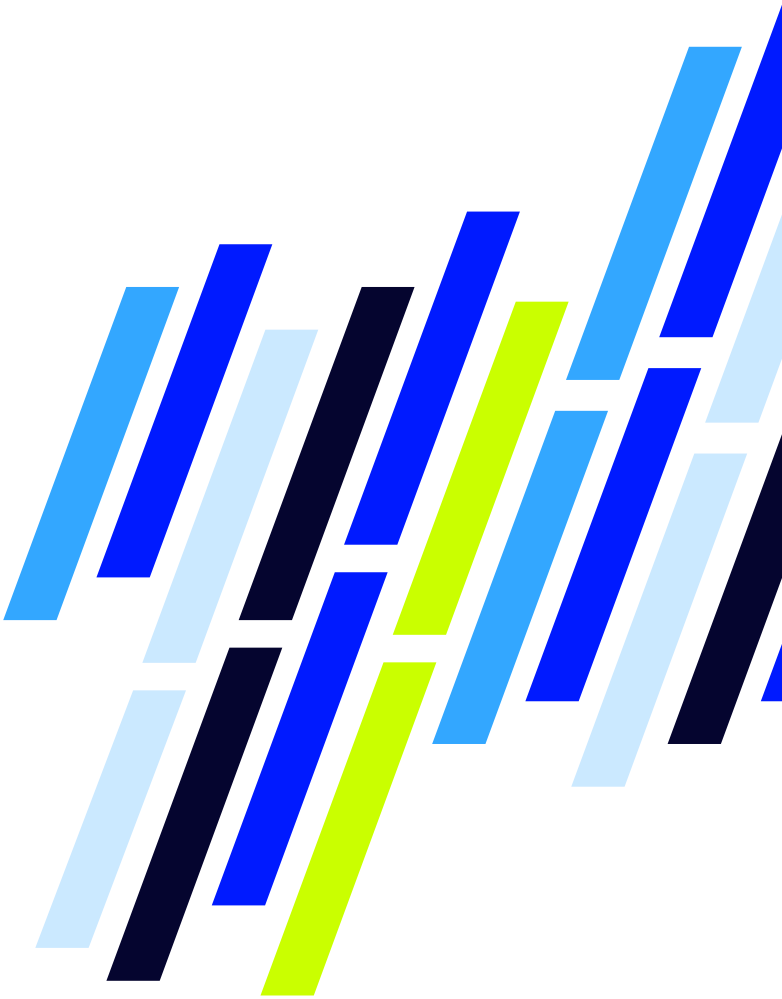
Key Benefits

LevelBlue Consulting takes a holistic approach to Information Security, addressing elements of people, technology, and processes. We combine in-depth knowledge and use of Information Security Standards of Good Practice (SOGP), applicable regulatory requirements and our experience in information security management practices within the industry.

Based on your needs, LevelBlue can develop a program charter, guiding principles, strategy and roadmap, that are not driven by compliance but rather partnered with compliance to enhance the security posture.

Security Solutions: Expertise from a Trusted Provider

LevelBlue provides a unique and world-class portfolio of assessment, compliance and related security services.



Our experience, expertise, and commitment to open standards have established us as a strategic and trusted advisor. By leveraging LevelBlue, you can expect best-in-breed solutions, a global network of proven technology, and a cost-effective, program-based approach to meet your security and compliance needs.

LevelBlue

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.

To learn more about Cybersecurity Consulting Services from LevelBlue, visit here or have us contact you.