

How to align security with your strategic business objectives*

Table of Contents

Introduction Pg. 04

As chief information security officer (CISO), you occupy the new seat at the executive table. In order to provide leadership in this position, you will need a clear vision for security, the ability to communicate its relevance and the managerial discipline to deliver its full value. This guidebook, based on our PricewaterhouseCoopers SecurityATLAS™ framework, explains how to achieve these goals.

Our Approach Pg. 08

We believe that in order to position yourself and your organization for success, you must be able to think, execute and deliver results along five strategic disciplines. This guidebook explains the five disciplines needed to help transform security's role in the organization and provides action steps for using them.

Assess: Understand where you are and where you want to be

Analyze: Conduct analyses that will give you actionable insight

Strategize: Build a strategic implementation roadmap

Align: Maintain strategy as a dynamic, continuous process

Communicate: Improve consensus-building, messaging and reporting

Appendix Pg. 61

The PricewaterhouseCoopers SecurityATLAS framework has been built based on our extensive client work. It is a comprehensive and flexible framework for the development, delivery, communication and maintenance of an enterprise-wide information security strategy. The components of the SecurityATLAS framework are explained in this appendix.

Get ready for some tough decision-making.

“It’s impossible to separate the concept of ‘security transformation’ from the pragmatic day-to-day discipline necessary to achieve it. In order to transform your security infrastructure, you must ensure that each security project clearly maps back to the organization’s strategic business objectives. You have to be ruthless when it comes to making tough decisions about the kind of information security investments you are willing to authorize and support. Ensuring that your security investments support your business strategy is a critical litmus test for any CISO. Every discrete security project must align with corporate strategy in order to make the cut. Otherwise, it is not going to drive your business forward.”

Ken Morris, CISO, Adecco

Introduction

With the mission of security expanding, the chief information security officer (CISO) faces a new test of leadership, one that requires essential disciplines in planning and communications.

As CISO, you are responsible for managing the crucial links between information security and operational performance, brand protection and shareholder value. It is a job that continues to change, and you are the executive most keenly aware of the extent to which security—including how your organization and others elect to align, harvest and sustain its value—is undergoing a transformation.

The nature of security is evolving.

Security is a crucial partner in helping manage large organizations.

As the scope and complexity of technology's contribution increases, so does the role of security. But a change to security's typically fragmented infrastructure is needed, one that promises to yield strategic cost savings for companies that address security from a comprehensive perspective.

Security is now critical for maintaining a competitive posture.

Once seen only as the first step in asset protection, today's security plays a critical role in enabling the exchange of sensitive information with other organizations.

Security is essential for compliance.

Heightened regulatory pressure to maintain better control over information means that information security must be incorporated early and comprehensively in the compliance planning and remediation process. When addressed as a whole, security can reduce the cost and increase the effectiveness of compliance.

New disciplines must lead the evolution.

These and other trends reinforce the importance of having ready access to a comprehensive set of managerial tools and disciplines in security management, along with a customizable means of communicating, to executive colleagues and other constituents, the value, status and impact of security.

As the role of security transforms from asset guardian to strategic business enabler, it will be up to you to determine the vision for security, refine your skills in communication and analysis, and undertake the disciplined approach required for effective executive leadership during this time of change.

Our Approach

We believe that in order to position yourself and your organization for success, you must be able to think, execute and deliver results along five strategic dimensions. This means the ability to assess, analyze, strategize, align with the business, and communicate the value of security. As shown in the graphic on the following pages, these are the disciplines needed to help transform security's role in the organization.

This guide explains the five disciplines and provides action steps for using them. It is based on thousands of hours of client service experience helping organizations of all sizes assess, develop and sustain an effective security program.

This guide is organized according to five disciplines.

The five CISO disciplines—assess, analyze, strategize, align and communicate—go to the heart of what it means to transform security and, through security, aspects of business performance, compliance and risk management.

Each discipline initiates a chapter within the guide and forms the basis for a set of actionable tips, suggestions and ideas intended to help you develop a security strategy that is repeatable, reportable and ultimately transforming.

Since these same insights, along with our knowledge and experience, form the basis of the PricewaterhouseCoopers SecurityATLAS, we will be drawing examples from this framework to illustrate key principles and actionable guidance.

SecurityATLAS is a comprehensive and flexible “concept-to-execution” planning, analysis and decision-support framework for the development, delivery, communication and maintenance of an enterprise-wide information security strategy. A full description of SecurityATLAS is included as an appendix.

The five disciplines of security transformation

Critical outputs of a structured security program

Assess

Assess, understand and define security's current and future role in your organization—where security capabilities in people, processes and technologies reside across the enterprise today, and what security needs to achieve for the organization in the future.

Security capability model

Analyze

Analyze the information collected to identify capability gaps in the context of regulatory considerations and industry benchmarks, check current project alignment, determine the appropriate size of a reasonable investment and identify precisely where the organization should be committing its scarce resources.

Project analysis tools

Strategize

Translate this information and analysis into an actionable, repeatable and reportable strategy that identifies the business case supporting project creation, project prioritization and investment optimization while also generating a strategic implementation roadmap.

Comprehensive roadmap

Align

Align this strategy and plan with the business on a continuous basis to accommodate continual change in the business, security and IT environments.

Security management framework

Communicate

Communicate security's current status, vision, strategic roadmap and progress to-date—at any point in the annual or quarterly business cycle and in a manner best suited to the different communication needs of a wide range of internal and external security constituents.

Customizable communication framework

Our Approach

Assess

How can you assess, understand and define security's current and future role in your organization? Where is money being spent on security personnel, processes and technologies across the enterprise today, and what does security need to achieve for your organization in the future?

A transformation for security should begin with a clear starting point, preferably, a base of fact. Gathering important security information from every corner of the enterprise, however, isn't always a straightforward task. Security capabilities today are often scattered across multiple business units and duplicated in different departments within the same operating division.

Overlapping responsibilities are likely to be shared by a host of personnel, including application developers, security staffers, system administrators and outside vendors. Understanding what each person does can be a task; aligning roles can be even more difficult, since these individuals often do not classify how much time they spend on security or which security tasks they are performing.

Complicating the challenge are the internal politics that are almost always present—if only because any effort to achieve transformation can be perceived, at some level, as a risk to jobs, responsibilities or personal career objectives. This may happen even when you and other senior executives are not planning such a level of impact.

Gather requirements in a controlled fashion.

When you begin to gather security requirements, you are not just putting out a request for information, you are also encouraging managers from all over the company to begin thinking and communicating about what they need or like about security—and what they don't. An example might be how security is currently being administered.

Expect conflict. Perhaps most of it will be a healthy exchange of views, but try to avoid creating an unstructured forum that doesn't result in meaningful input. Control the process by providing strong leadership. Establish clear starting and ending points for the requirements gathering process. Anticipate issues and take the time to finesse your approach. Document everything. And above all, work tirelessly to manage stakeholder expectations.

Ensure that those being asked to provide information understand the scope and purpose of the request and recognize that the effort is important to the broader goals of the business. Also, be prepared to enlist other executive leaders, including the CEO if necessary, in communicating the goals of the initiative.

Know what you're looking for.

Be certain that the people you've tasked with asking questions understand, at a technical, organizational and process level, the complex interdependencies that exist among security capabilities. Interviewers must be armed with insight into what they know will be happening in later stages of the strategy process.

You will want to anticipate this complexity and allocate information-gathering activities with different levels of sophistication to those most qualified for the task.

Know your team. Does your inner circle of direct reports understand the nature of your objective in developing a security strategy? Among them, how many have the communication and relationship-building skills to develop a rapport with business-unit managers in different operating theaters? Who are they? Do these individuals have the presence and the professional credibility to solicit the insights into business objectives, operating needs and resource constraints that will shape your later decisions? What is the cost to deploy them? Answering these questions will help you field the right fact-finding team for the job.

Capture the true spending on security.

Your strategy has to stand on a clear and accurate accounting of how much the entire organization is spending on security. Getting this information may require persistence. A difficulty in quantifying IT security spending is that almost every application developed or purchased requires a measure of security in order to operate properly. In the majority of cases, this component is independent of the strategic common components provided by the IT infrastructure.

Try to get to the bottom of the so-called “shadow” spending on security, i.e., dollars that are not budgeted, standardized or reported. Such hidden spending can occur within various business units, when divisions, departments and individuals decide to deploy security technologies, processes and services that aren’t centrally tracked or authorized. At least initially, be sure that your search parameters include all key security spending elements within both operational and capital expenditure categories.

It can be difficult, if not impossible, to identify the operational costs of other departments, in part because these departments do not always itemize expenditures on security. Under such circumstances, consider security costs embedded in the application portfolio’s budget as potential opportunities for cost savings that may be realized by expanding common security services.

In addition, be on the lookout for process or capability redundancies both inside and outside the formal boundaries of the security organization’s technologies, processes and budgets.

How to collect information.

In the process of gathering requirements, you'll be conducting interviews and surveys as well as gathering available documentation. Here are some ideas that may assist you:

- 1. Interviews:** Try to address key personnel at (a) the leadership level—to determine strategic objectives and assess senior executive perceptions; (b) the business-unit level—to identify line management's expectations and perceptions; and (c) different levels within your IT organization—to flush out the concerns, experiences and ideas among your technicians that can be invaluable but hard to uncover without a targeted effort.
- 2. Workshops:** While interviews are effective at surfacing detail, workshops generate a collaborative environment that supports the exchange of ideas and promotes the growth of productive working relationships between important stakeholders.
- 3. Surveys:** Because interviews can be expensive and time consuming, consider supplementing your findings with surveys that can be used to gather data quickly from a larger audience while establishing a baseline of management metrics that can be updated in later surveys.
- 4. Documentation:** Information is likely to be already documented and retrievable within your organization—assuming you know what to ask for and whom to ask. Accessing current documentation can be the quickest and most cost-effective means of collecting internally available information related to areas such as: (a) resourcing and head counts, (b) current security projects and investments, (c) hardware and software assets and their costs, and (d) operational statistics.

Think like a CFO.

“One of the most fundamental skills supporting a CISO’s fiscal and fiduciary responsibilities today is being proficient in translating the implications of security into financial terms with the appropriate level of transparency and clarity. You should be able to present your business case in a way that others on the executive management team will understand.

“In effect, you have to be able to ‘think like a CFO,’ because your ability to deliver results may depend on your ability to communicate what security costs and what it delivers.”

Elizabeth King, vp Information Management Services, Starbucks

Define business objectives.

Collectively, the organization's business objectives form the single most important driver of the security strategy. They are the basis of the arguments you will be using to communicate the business case for change and will help you prioritize initiatives based on business need. When determining your security strategy planning process, take care that it is explicitly mapped to the business objectives you have identified and carefully defined in terms of the benefits that will be used to measure project success.

Identify regulatory requirements.

Find out exactly what regulatory requirements must be taken into account. For example, your organization may be responding to regulatory requirements as they emerge, and reassessing its IT and security environment over and over on a regulation-specific basis.

If you have separate policies for compliance, privacy and security, you will likely have to address overlapping standards that are neither centralized, coordinated nor integrated.

Say, for instance, that your organization supports 25 different ways—many of them redundant—of managing user identities and privileges. In this case, proper security, compliance and risk management procedures would require that you document these 25 different procedures, test to ascertain whether they are operating effectively, manage changes to them and report on the status of their efficacy on a regular basis.

Unless you can consolidate these redundant processes, such a poorly coordinated system will result in significant costs to the organization. The good news is that your executive colleagues are now well apprised of their accountability for regulatory compliance—a situation that can help you attract support and funding for key security initiatives. But you must be able to impress upon them that regulatory compliance management should no longer be addressed as an event-driven activity. Rather, it has to be an ongoing component of your organization's day-to-day approach to overall security and risk management.

Having identified the regulatory requirements your organization has to comply with, you will need to determine—from across the spectrum of security activities—the precise security capabilities required to meet each regulation. Use this information to frame any resource communications with management.

Benchmark against competitors.

SecurityATLAS Regulatory Baseline

The SecurityATLAS Regulatory Baseline provides organizations with a clear picture of how and where specific regulations impact the security agenda. Please note that the information presented here is merely representative. Regulations depend in large measure on application-specific circumstances, and the data illustrated here is not applicable to all industries or operating environments. See page 67 of Appendix.

If possible, gain a thorough understanding of competitive security practices within your industry. This information can help you identify areas in which the organization needs to bring itself current with standard industry security practices and may offer insights to developing a competitive advantage.

Acquiring knowledge about what competitors are doing in security also changes the nature of your conversation with business-unit leaders. Armed with this insight, you can more readily discuss security's value from the perspective of enablement as well as prevention. This has the potential to trigger and maintain a more enthusiastic level of commitment and collaboration.

Define the future state of security in your organization.

SecurityATLAS Industry Benchmark

The SecurityATLAS Industry Benchmark presents a clear picture of how your industry is addressing key capabilities in the people, process and technology components of a security program.

We maintain this database with information gained through a global survey of security practices. See page 68 of Appendix.

Achieving security transformation depends in part on pointing the organization in the right direction. You will want to define a vision for security that is reasonably achievable, realistic in the context of industry peer activity and directly aligned with business objectives.

A future-state assessment should address the following six areas:

1. Guiding principles.
2. Services and technologies that support how security will function within your organization.
3. The high-level technological architecture necessary to maintain these services.
4. Emerging industry standards.
5. Identification of vendor technology trajectories.
6. Organizational roles and responsibilities and associated capabilities.

Addressing these areas will help you determine the extent to which the organization's future state is either divergent from, or convergent with, system components currently being recommended to you for purchase. Understanding these areas can also help you align common processes with key drivers of the business and identify skill sets required in the future that are not represented in the current security organization.

In security, it pays to look ahead.

“There is still a tendency within security organizations to focus on reactive security rather than taking a proactive approach. Reactive security appears, at first hand, to be less resource-consuming, with faster results and more flexibility, but this is a misconception. In the medium to long term, reactive security provides no scope for growth or adaptation and amounts to little more than expensive firefighting.

“Proactive security requires early identification of the business and technical requirements that can give a security chief the necessary edge to build an organization flexible and adaptable enough to provide holistic services, meeting both immediate need and providing structure for future growth. Taking the time to get it right in the early stages reaps huge benefits in the long term.”

Craig Thomas, Global CISO, PricewaterhouseCoopers LLP

Assess with care.

Definition of the future-state vision is an important technical requirement in a structured approach to security strategy—a first step in developing an actionable blueprint.

In a later step, you will be analyzing the gap between where your organization's security capabilities are today and where you would like them to be in the future. Clearly defining these two points will also help you develop, deploy and retain your team—a critical component of realizing the value of your strategy process.

How to identify your organization's current state and define a clear security vision for the future.

Here are suggestions to help develop an accurate assessment:

1. Use a standardized measurement framework for evaluating where you are today and where you want to be tomorrow. Without one, you may find yourself “comparing apples to oranges” and therefore unable to justify the results of your analysis.
2. Understand the major drivers of profitability and shareholder value for your organization. Become proficient at explaining the link between these business drivers and IT, and between IT and security. Don't be satisfied with a short list of high-level business drivers that shed no real light on security's mission. Press for a clear statement of how IT is driving toward the needs of the business. Be explicit in calling out the specific contributions that security can make in supporting key business initiatives.
3. Find out why and when executives have shied away from a proposed initiative due to technology-related risk factors. Use that information to build a better case for change.
4. Pick the right scope for the information-gathering process. Sometimes the scope of the strategy should be broader than the scope suggested by the most immediate security needs. A strategy can be constrained by capability interdependencies as well as the compromises necessary when scarce resources have to be unexpectedly redirected. There is nothing wrong with a roadmap that shows you several ways of reaching the same destination.
5. Initiate ways to cut through internal politics or bureaucratic obstacles that may crop up in the information-gathering process. Be sure that you have visible support from the CEO or CIO. Proactively counter any negative messages supporting fear, uncertainty and doubt with respect to IT security. Help your security constituents focus instead on security's enabling role—in the context of business enablement, regulatory compliance and the protection of assets. Communicate clearly and often.

Our Approach

Analyze

How can you analyze the information we have collected to identify capability gaps, check current project alignment, determine the appropriate size of a reasonable investment and identify where your organization should be committing its scarce resources?

Now that you have gathered everything relevant to your organization's security requirements, it is time to start making sense of the information. Doing this will be easier if your planning and analysis framework is well organized.

Start with a structured security capability model.

As one of the foundational steps in your strategy process, you will need to establish a comprehensive planning framework for security, one that defines a master set of core security capabilities and organizes them in a way that facilitates aligning security with the business.

Defining the right framework can be critical because it can determine (1) whether your strategy is effective, (2) whether it can be communicated easily to non-technical executives and (3) whether you will be able to sustain the strategy on an ongoing basis.

Questions arise: What should the taxonomy be for describing, naming and classifying security operations? How should you go about organizing this structure? What are you going to measure? What are the organizational units, key performance indicators (KPIs) and other building blocks that you should be using to structure your security program?

Some CISOs elect to organize security areas by function. Others define organizational parameters that conform to control frameworks such as CobiT¹ or standards such as ISO 17799² and COSO.³ These approaches, however, are not sufficient by themselves. They can help describe what information security must achieve, but they do not explain how security capabilities contribute value to the organization.

Consider what your selection criteria for a taxonomy might be. At a minimum, it should reflect logical relationships among security areas and include layers of detail that can be consolidated to create high-level reporting—from the lowest technical layer to the highest strategic presentation layer. The example on pages 32 and 33 shows what a taxonomy might look like.

¹ CobiT (or Control Objectives for Information and related Technology) is a framework for information security created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI).

² ISO 17799 is an internationally recognized generic information security standard published by the International Standards Organization.

³ This is framework for internal control provided by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

If you can't talk ROI, the boardroom isn't listening.

“There are two types of metrics used by the CISO: those based on security criteria and those based on business goals. Those based on security criteria are a useful intradepartmental tool for evaluating performance, but they do not translate to the boardroom. For example, knowing the number of attacks detected or thwarted may be useful in evaluating your incident response and detection processes, but they tell the executive nothing about the dollar return on his security investment.”

Lloyd Hession, CISO, Radianz

A sample taxonomy structure

Layer 01

To understand the first layer, suppose you elect to view security as comprising seven different functional areas. Think of each functional area as a distinct value chain, one that provides an identifiable value contribution to the organization and spans the entire security value chain. These seven functional areas are the basic categories into which your team groups all information security activities within your company.

Security functional areas

- Regulatory and policy compliance
- Architecture, consulting and development
- Awareness, education and communication
- Controls and identity management
- Threat and vulnerability management
- Physical security
- Program management and governance*



Layer 02

The second layer is comprised of the security activities necessary to deliver the primary value of the functional area.

Below is an example of the security activities necessary to deliver on “Program management and governance.”

Security activities

- Knowledge management
- Personnel management
- Enterprise security steering
- Third-party relationship management
- Third-party contract management
- Risk management
- Portfolio management*



Layer 03

The specific capabilities associated with each security activity make up the third layer. These represent the most fundamental building blocks for anything you are currently doing or that you intend to do in security. They form the lowest level of detail in your strategy and program management framework.

Below is an example of the security capabilities necessary to deliver on “Portfolio management.”

Security capabilities

- Business objectives
- Selection and prioritization
- Inventory and monitoring
- Portfolio management team
- Portfolio management technology

Why is this structure so important?

It allows you to catalog the current state of your security organization using these capabilities and a maturity scale (for example, one based on the Carnegie Mellon Capability Maturity Model®).⁴ It also provides you with a common framework that allows comparison of your current-state posture to (1) that of your industry peers, (2) the minimum regulatory baseline that you have defined and (3) the security services required by your most important business priorities. At the same time, it permits customizable multi-level reporting to different security stakeholder communities. Depending on the reporting audience, you will be able to consolidate capabilities in different ways to support various communication objectives.

To help companies achieve this level of planning control, PricewaterhouseCoopers has developed the Enterprise Security Capability Model™ (ESCM™), an industry-neutral, technology-independent capability framework that forms the basis for an organized approach to managing information security.

Based on the ESBM™, PricewaterhouseCoopers' view of the enterprise security value chain,⁵ the ESCM defines the full set of security capabilities that comprise any organization's security program—its people, business processes and technology infrastructure. The model details over 400 measurements of an organization's maturity across the security continuum and helps companies establish common benchmarks and control points across different control frameworks and standards.

⁴ Developed by Carnegie Mellon, the Capability Maturity Model® has been used by many organizations to identify best practices useful in helping them increase the maturity of their processes.

⁵ The Enterprise Security Business Model™ is an industry-leading model developed by PricewaterhouseCoopers that uses a value chain concept to explain how security adds value to an organization.

How to select a taxonomy system for an IT security program.

Here are four criteria to consider when selecting a taxonomy for IT security:

1. Logical relationships. The taxonomy should group together technically similar functional areas, activities and capabilities.
2. Consolidation and detail. The taxonomy should support at least three layers of detail. These should readily consolidate to support reporting and communication to a senior executive audience. Detail must be available to support actionable technical communication across the IT and security organizations as well as to enable a tightly focused level of managerial planning, analysis and performance measurement.
3. Completeness. The taxonomy should be comprehensive in nature. It must be able to support, for example, the lexicon used to develop and describe both your current- and future-state definitions.
4. Value chain-driven and aligned. The taxonomy should support how the organization identifies and demonstrates value. Ensuring that the measurement and organization of information security maps clearly to the company's key value statements will help strengthen and retain the awareness and attention of senior executives.

Develop an effective weighting system.

Before you step into the gap-analysis phase, be sure that you have a system in place that can quantitatively measure differences between your current- and future-state capabilities.

Not all capability gaps are equivalent. You will be weighting, or prioritizing, some capability differences over others. In addition, you will need to have a means of measuring each gap in terms of the difficulty required to remediate it.⁶

⁶ Using a linear mathematical system (e.g., $4-2=2$) will not work well. For example, it may be more difficult to close the gap between two capabilities rated 3 and 4 than it is to close the gap between two capabilities rated 1 and 2. A linear rating system, however, would value the task equivalently.

Conduct a gap analysis.

At this point, you are ready to conduct the gap analysis. Using a variety of analytical methods and tools such as current- and future-state scorecards, examine and document the differences between your current and future states. Ask questions such as the following:

- **Where are the shortcomings in our capabilities now?**
- **What will it take to fulfill these requirements?**
- **Do we have the right organization to meet these capability needs?**
- **Where are the disconnects between our security technologies and practices? How should these be integrated, consolidated or coordinated?**
- **Which manual processes should we replace with automated ones?**
- **What and where are the technical interdependencies that will inform our later focus on prioritization, sequencing and dual-track avenues of implementation?**

Look for root causes.

Security organizations without strong analytical capabilities tend to adopt tactical or automatic reactions to negative security-related events—particularly to those events that are most apparent and urgent. While understandable, this approach is potentially costly. Capability gaps that are highly visible and urgent may be the result of weaknesses in other areas, and a reactive approach to applying a fix is not likely to yield desired results over the long term.

In most cases, a multi-dimensional analytical tool should be used to develop planning insight into the root causes that drive the organization's symptoms of need.

When selecting analytical techniques, take care that they allow you to view the information in your repository from various perspectives. For example, gaps that may not appear to be critical from a regulatory angle may be revealed as critically significant to the organization if viewed from a business requirements perspective.

Remember, if you limit your ability to assess security capabilities from different angles, you may miss or underestimate the magnitude of the capability gap most in need of redress.

Analyze your projects.

It can be challenging to get a comprehensive picture of all security projects being executed across the organization—and even more difficult to decide which projects to approve and support.

If you have conducted thorough and accurate assessments of your current and future state, you know exactly where security is, or should be, contributing value to the organization. But that does not mean you can afford every project that contributes incremental value to the organization's efforts. Here are some questions to ask:

- **How should our limited resources be optimally allocated?**
- **Where are the redundancies in project objectives, which, if eliminated, can reduce waste and free resources for other initiatives?**
- **How can we leverage our capability-specific gap analysis to identify and address the projects most important to supporting the organization's objectives?**
- **How can we focus our resources on the correct sequence of capabilities in order to achieve our vision while minimizing rework and completing the project on time and within budget?**
- **How can we optimize our product mix to demonstrate continuous value to the organization? Are projects taking too long to show demonstrable value?**

Prioritize and align your projects.

Now that your gap analysis has identified the organization's security needs and requirements, look at how best to prioritize these projects.

Adopting an effective capability framework will allow you to compare projects based on many more factors than just cost, resource availability and timing constraints. You will also be able to define project prioritization and sequencing based on (1) the relative importance of the gap the project is intended to redress, (2) the degree to which repairing or achieving a capability closes this gap and (3) whether the project should be addressed earlier in the strategy due to capability or implementation interdependencies.

This exercise would help you, for example, determine which project should be given higher priority: an initiative to bridge capability gaps essential for compliance with three different regulations, or an initiative to close a single large capability gap important to the business unit that generates 65% of the organization's profit.

Repeat this process to analyze various scenarios based on different funding requirement levels, shifting business and regulatory priorities and changes in project timelines. This should be an iterative process in order to clarify the full range of options available and to build the business case that will support your final recommendations as to which investments in security are most valuable to the organization.

How to improve the results of the analysis process.

This is an important stage: rigor in the analysis will determine the effectiveness of the strategy. Facilitate the process by taking the following steps:

1. Be sure to define the full set of assumptions that drive your strategy model. Whenever possible, secure from other executives feedback and buy-in on assumptions early in the strategy process. It will help you defend the results of the analysis later.
2. Have a clear understanding of how your various organizational capabilities relate to one another. This is essential. Many organizations overlook critical dependency relationships that dictate the need to address some capabilities before others—such as gaining comfort that the organization has an adequate data infrastructure before implementing an enterprise authorization solution.
3. Set aside preconceived notions about the outcome of the analysis. In some cases, the data and analysis will support conclusions you and others have anticipated. In other cases, the analysis will surface unexpected relationships between capabilities or needs that have not been previously identified.
4. Don't spend too much time on the assessment and analysis phases of the strategy development process. Some CISOs get stuck in this stage, as do security executives who are chronically reluctant to move forward because they know that the information supporting their analysis is not fully complete or accurate. Far better to focus on getting the best information possible and move forward into execution—assuming you continue to collect, refine and improve the information that informs your strategy on an ongoing basis.
5. Recognize that gaining acceptance of the results of your analysis depends on decision-makers understanding the framework supporting the analysis. Be ready to demonstrate to your executive colleagues that the analytical methods you have relied on can be used to derive a consistent and repeatable result.

Our Approach

Strategize

How can you translate this information and analysis into an actionable, repeatable and reportable strategy that identifies the business case supporting project creation, project prioritization and investment optimization while also generating a strategic implementation roadmap?

It is now time to shape your analysis into a comprehensive strategy. When complete, the strategic assessment should include a written in-depth analysis of your current security posture, as well as a recommended implementation roadmap.

Depending on the scope of the initiative, you will likely be using the strategy to identify where resources need to be focused to best align security with key business and regulatory compliance objectives. The analysis document has other uses as well, such as validating existing and future funding levels.

As your strategy begins to take shape, keep in mind a word of warning: with remarkable frequency—despite having developed a security vision and a roadmap—many CISOs and organizations either fail to act on the plan's guidelines and recommendations or, just as unfortunately, take concerted action in a manner inconsistent with the organization's business objectives. Deviation from the plan happens for many reasons; a common problem is that the security strategy is neither reasonable nor actionable.

Ground the strategy in realism,
and make it actionable.

The security strategy should be reasonable, achievable and explicit. Consider limiting the execution horizon to three years or less. Stress the identification and inclusion of metrics that give the detail necessary at any time to measure progress toward achievement and manage the benefits that achievement yields. Make sure the planning framework you adopt allows for maximum flexibility. And be ready to change the plan of attack in midstream whenever necessary.

The security strategy is actionable if it meets the following criteria:

Clarity: Executives, managers and administrators at every level of the organization need to be able to understand which steps must be undertaken, and in which order, to implement the strategy from beginning to end.

Conciseness: Strategy stakeholders should be able to read the strategy publication quickly and easily.

Funding alignment: Strategy recommendations should be consistent with the level of investment and the scale of the resources that management is willing to commit to execute the plan.

Organization: Rather than defining large sets of overly complex activities, the strategy documents should organize all steps into small, simple groups of tasks logically arranged to result in discrete, measurable deliveries of value.

Adaptability: The strategy must be able to accommodate changes in key assumptions and requirements driven by shifts in the broader business and IT environments.

Executive leadership support: Management must be confident that the strategy has been created with the appropriate level of due diligence, insight, analysis and rigor. Organizational leaders must believe that, if enacted, the strategy would add value to the business relative to the size of the investment needed to implement it.

Define the project roadmap.

Focus now on building the project roadmap, a step-by-step plan that explains at the project level how the organization is going to achieve implementation.

Make the roadmap explicit with respect to milestones, deadlines, decision checkpoints and deliverables. Also, define resource usage and constraints, project dependencies, sequencing requirements and critical inputs required from either internal or external individuals or groups.

Be sure the project roadmap allows you to identify, revise and report on project resources. Where possible, structure activities in discrete, manageable segments that deliver benefit packages quickly, completely and in the right sequence.

Look for opportunities to quickly demonstrate value by ensuring that initial activities are focused on a few easily achievable and measurable goals. Early successes will help build the strong relationship between IT and the business units needed to drive more complex and difficult achievements later in the strategy implementation process. A project roadmap should include, at a minimum, the following core components:

Executive summary presentations: Necessary to demonstrate alignment with management's key business objectives and to build broad executive sponsorship and support.

Communication plan: Describes how the strategy will be communicated to various audiences, including developer communities, IT management and affected business communities.

Tactical maps: Identify short-term tactical steps as well as a vision for how these steps integrate with the longer-term plan.

Value realization plan: Describes the measurable value and benefits of the program or project.

Comprehensive planning framework: Helps executives re-evaluate strategic priorities as the needs of the business or technical assumptions change.

The project roadmap should also include a full complement of management tools, templates and scorecards that visually report progress toward program or project objectives.

How to put a strategy in place.

The process of pulling a comprehensive security strategy together and pushing it out into a working project roadmap can be rigorous and taxing. Here are three tips to help make it successful:

1. Recognize that the plan must be actionable at multiple levels. Apply discipline in shaping the solution components that make strategy actionable: (a) project roadmap, (b) dynamic communication framework and (c) structured security management framework.
2. Require that the security strategy be prepared in business, rather than technical, terms and that the content of the strategy be communicated in a manner that non-technical executives will find easy to understand. Substance, business relevance and insight into what is required to move the security organization ahead matter far more than technical detail.
3. Ensure that the strategy is developed by incorporating input from groups and individuals expected to be resistant to change. Involving them in the development of the strategy can present important opportunities to address opposition early in the process.

Impact on the bottom line speaks volumes.

“In the healthcare industry, our business leaders know that every dollar spent on security is a dollar not spent on caring for patients or improving the ability to attract patients and doctors. So as a CISO, whether we’re able to deliver concrete, measurable value to these leaders can rise or fall entirely on whether we’re able to explain security’s contribution to bottom-line business results.

“We have to be able to do this in a manner that links security with the business vision, communicates the real costs of security, and demonstrates a flexible, comprehensively structured approach that’s based on leading industry benchmarks and solid risk management practices. The steps for making the strategy actionable help avoid the common pitfalls that result in strategies being nicely printed and put into binders that sit on shelves gathering dust. Letting that happen can doom a security program and CISO to being on the outside looking in, in terms of integration as a critical component of business operations. This can be the difference between success and failure.”

Paul Connelly, CISO, Hospital Corporation of America (HCA)

Our Approach

Align

How can you align your strategy and plan with the business on a continuous basis to accommodate constant changes in the business, security and IT environments?

Strategy development is not an annual exercise. It is a continuous process that must evolve as the needs of the business change. In fact, one of the most common reasons that even carefully designed strategies are not implemented is that by the time the strategy has been approved, it is also out of date.

A rigid and inflexible methodology provides a poor foundation for a strategy blueprint, as does a design that resists standardization, systematization and transfer. The strategy you develop must embrace change.

Institutionalize agility.

Look for ways to make your strategy development process a continuously cycling set of activities. Count on change happening as a matter of course. Build a security planning platform that doesn't just tolerate a high level of uncertainty, but is designed to accommodate it.

Always press for advantage, because, until a dynamic security strategy becomes a management standard for CISOs, many of your business competitors will hang back—addressing security events from a reactive perspective, spending precious security dollars on point solutions and forgoing the stream of business benefits that flow from security strategies that are agile and aligned.

Keep your strategy up-to-date by modeling how you would carry out your implementation plan under different scenarios, such as amending it to accommodate a major last-minute shift in a key business driver. Embrace learning from initiatives that succeed as well as those that fail, and be prepared to change course quickly.

Be certain your strategy can be easily applied at every level of the organization. Emphasize the importance of using technologies and reusable planning and decision-support templates.

Apply principles of portfolio management.

Simultaneously assessing different strategy options and possibilities is not a simple process.

The variables are complex by themselves, and their combinations are even more so. At different stages, you need to know what outcomes to expect under various scenarios—ideally, you would like to have this information without having to retool your databases, spreadsheets and templates.

The most effective way of gaining this managerial insight is to engage a portfolio management approach. This allows the management of security technologies, capabilities and resources in order to dynamically review the impact of hypothetical changes to the business environment, quantify current spending and justify future increases or decreases in spending. There are several software tools on the market today designed to help automate the portfolio management process.

Portfolio management helps you optimize and manage the allocation of your security budget funds according to your organization's most important business objectives. It also provides the ability to demonstrate the basis of your security decisions and recommendations to other senior executives, as well as helping provide scope, context, options and direction to discussions that relate to security. This can be especially useful when, for example, unexpected occurrences (such as virus infections or hacker attacks) might otherwise compel senior business leaders to focus on events outside of the organization's control.

Security needs to move
in tandem with the business.

“Day in and day out, we’re competing for share in markets that reward agility. That need for agility is as true for security management as it is for any other critical facet of operations. In fact, we can’t justify a major security investment without also having the flexibility to continually manage this investment in the face of a constantly changing business environment. You’ve got to be able to reassign ‘committed’ budget resources, reprioritize investments and ultimately field a security strategy that inherently supports flexibility and change.”

Dave Cullinane, CISO, Washington Mutual

Use the right tools.

SecurityATLAS Portfolio Management Capabilities

Through a portfolio-based approach to managing project mixes and inputs, SecurityATLAS gives CISOs a pragmatic ability to optimize the allocation of security investments. This is a complex undertaking that requires a coordinated ability to identify, integrate and allow adaptations to the people, process and technology components that collectively drive any complex set of security initiatives. The approach also provides management with transparency into how resources and funding are being allocated and which trade-offs arise when unexpected issues surface that compel executives to reconsider security investment priorities. See page 69 of Appendix.

Portfolio management tools should support the ability to manipulate data inputs. You should be able to change the assumptions and inputs relatively easily in order to model annual plans and “what if” scenarios that will help you develop forward visibility into how, when and in what combinations and sequences you should be focusing on new security capabilities. In this regard, software is a critical asset because it standardizes analysis models and can forecast impacts to the organization resulting from changes in the business or technology environments.

Under the best circumstances, this is a high-level, dashboard-driven discipline that allows you to manage and categorize total security spending in the organization as a mix of investments whose balance and make-up you can reconfigure whenever necessary.

How to maintain the strategy as a continuous process.

Managing the strategy in response to changing conditions is as important as putting the strategy on the ground in the first place. Here are five insights to help you manage in a changing environment:

1. Understand how each security initiative advances both the security and business strategy. Define this understanding in terms of the benefits the initiative will help realize. If this alignment is not fully apparent, be prepared to withhold approval of the initiative in question.
2. Do not sign off on the security strategy unless the security initiatives are examined, assessed and presented as a full portfolio of investments—including total costs, quantitative and qualitative benefits and key business risks.
3. Take care that the CIO, CFO and, in some cases, the CEO understand your standard of approval. This can be a wise tactic, particularly if you are still working to build credibility for the CISO position among your executive colleagues.
4. Recognize that the security strategy is a dynamic, continuous process—not a static event conducted on a quarterly or annual basis—and that security is affected by market forces and other external events as well as by changes in the internal corporate environment.
5. Suggest to the CIO that you collaborate in preparing a report for presentation to the CEO and the executive management team, highlighting how the security strategy and program are structured to handle change in a flexible, adaptable and continuously cycling manner.

Our Approach

Communicate

How can you communicate security's current status, vision, strategic road map and progress-to-date at any point in the business cycle and in a manner best suited to the different communication needs of a wide range of internal and external security constituents?

At the executive level, the corporate world provides a framework for individual performance. Organizations assign titles and responsibilities; leaders bring credibility and impact—if they can. The role of CISO is no exception. To build your position, earn credibility and create an impact, we believe it is essential to have a:

- **Solid understanding of how to communicate the value of security activities to a wide range of security consumers**
- **Security management framework with communication tools and reporting capabilities versatile enough to support your communication objectives**

If you do not define the key issues and challenges for your organization's security program, chances are that others will. Unfortunately, remarks made about security are often critical, inaccurate or both. Why? Because security tends to attract the most attention when things go wrong or when other executives start wondering aloud if the investment is actually producing a return.

As the CISO, you need to get out in front of how security is perceived, understood and supported at every level of your organization. This part of the CISO mission requires good communication, clear reporting and an ability to craft crisp messages that can help your audiences internalize and quickly accept your information.

Tailor your communication approach to different audiences.

What, where and how you communicate about security within your organization need to take very different forms depending on which security constituent you are trying to reach.

Are you addressing senior corporate executives at the C-suite level, business-unit leadership or IT managers and administrators? Are you reaching out through email, hand delivering a comprehensive report or conducting weekly planning meetings at satellite IT offices? Are you communicating in action and behavior, as well as through written and electronic means? Are you training, coaching and mentoring your security staff to extend, support and explain the communications objectives you have defined?

Work to understand how each security constituent looks at job objectives. From this perspective, imagine how each views security's effectiveness in supporting his or her role in driving the organization's agenda. For example:

If you are looking to raise the CEO's security awareness, remember that the CEO is primarily focused on the drivers behind earnings, profitability and shareholder value. This person may be more receptive if you can explicitly link security with a role in supporting these key objectives.

If you are addressing the CFO, be prepared to discuss security in the language and context of financial issues, such as security's current and future impact to the corporation's assets, liabilities, income and expenses. How does the security strategy address risk management, mitigation and transfer issues? How does it address short- and long-term effects on the corporation's share price?

If you are working with the COO, expect to discuss how security should support new product or service strategies. Or how security will impact operational availability, business process integrity or continuous operational improvement.

Take the time to develop good skills in listening, conversing and exchanging information with other business and IT leaders. Take an interest in their points of view and build rapport at a personal level.

Be certain the strategy framework supports customized reporting.

In order to communicate with others at every level of the organization, you must be supported by a strategy framework or methodology that provides a broad number of reporting choices in how you sift, filter, roll up and summarize security information in a manner customizable for different audiences.

Become a business leader with
the soul of a technologist.

“The most effective CISOs today aren’t just experts in technology; they’re experts in how technology must be positioned and implemented to support the business. That represents a quantum shift in the balance and breadth of skills that a CISO must be able to bring to the organization, because now rather than being just a ‘technology guru,’ a CISO must also be at home with the skills necessary for leadership, business management, executive communications, fiscal planning and risk management.”

Gary Eppinger, CISO, Rockwell Automation

Tie metrics to specific audience needs.

As a forward-looking CISO, you should be the person in your organization who actively defines the quantitative measures and metrics that will be used by the CIO as well as the executive management team to measure and assess security's performance.

This means having the ability to prepare reports that include different sets of metrics for security information consumers with different needs. Of course, this first requires that you define, embed and track metrics in key areas such as strategic alignment and business value, security management and control, and security operational performance.

What kinds of metrics should you be using? They should be value focused, performance based and improvement oriented. They should be placed throughout the security infrastructure and business unit operations, as well as at the most illuminating points of friction, integration and support that exist between the two. They should be positioned at touch points that give you and your operations staff the best opportunity for assessment, intervention and correction.

How to make communication a critical success factor.

Here are four concrete steps you can take to help create and sustain executive security awareness and support:

1. Recognize that effective relationship management is an important driver of your long-term success with the organization and your ability to be recognized and welcomed as a peer by other senior executives on the leadership team.
2. If you have a strong background in business, but are less experienced with how technology impacts business performance, start with the CIO. Consider spending some time shadowing an IT implementation team, or observing how internal service calls are handled. This will help you understand how the organization's business users interact with the technology that the CIO is managing, and what kinds of expectations for service, support and accountability they place on the CIO whether or not they are directly related to security.
3. If you have a predominantly technical background, find ways to live and walk in the shoes of your business executive peers. Spend some time with business-unit managers—on their terms, in their offices, addressing their challenges. You will understand much more about how to define, design and communicate your security strategy to support their efforts. And you'll begin building a working platform for trust, communication and collaborative success.
4. Develop crisp reporting capabilities that support roll-up activity summaries. Use features that allow you to screen, drill down or manipulate views into your security strategy to support your team's ability to customize communications for different security information audiences.

Arm everyone with the knowledge
to save your company.

“It’s hard to overstate the importance of effective security awareness and communication. As one of the largest power generators, transmitters and distributors in the United States, we’re acutely aware that the weakest link in the information security effort that protects our data, our control systems and our generating fleet can be something we don’t know, leaving our networks or data exposed to attack.

“That is why we expect our managers—at every level of our organization—to understand how security supports and impacts our processes, assets, efficiency and our operating objectives. At AEP, communication about security isn’t just an administrative function—it’s an integral component of how we provide tangible value to our customers, our employees and our shareholders.”

Michael Assante, VP and CISO, American Electric Power

Appendix

PricewaterhouseCoopers' SecurityATLAS is a comprehensive and flexible "concept-to-execution" planning, analysis and decision-support framework for the development, delivery, communication and maintenance of an enterprise-wide information security strategy.

The same insights, knowledge and experience that inform this publication also represent the core of PricewaterhouseCoopers' comprehensive strategy development and support approach.

This integrated and customizable set of tools, templates, software and business processes is based on PricewaterhouseCoopers' experience in helping companies throughout the world align security with their business and regulatory objectives.

Built upon a multi-layered planning approach, the SecurityATLAS framework helps CISOs develop a current-state assessment, define a security vision, develop and execute an actionable strategy roadmap, sustain the resulting security strategy over time and use the tool sets to create and sustain executive security awareness and sponsorship.

As a comprehensive and customizable planning framework, SecurityATLAS integrates the critical processes that link security strategy development, execution and maintenance.

Features and outputs include the following:

A comprehensive capability model

Based in part on PwC's Enterprise Security Business Model, this model helps clients visualize, summarize, communicate, and execute against complex information security objectives.

SecurityATLAS Regulatory Baseline

Designed to provide visibility across regulations, this tool helps CISOs understand how and where specific regulations impact their security agendas.

SecurityATLAS Industry Benchmark

Updated by PwC's global surveys of security practices as well as by experience collected over hundreds of client engagements, this industry-specific database of security practices offers insight into how comparable companies are addressing security.

SecurityATLAS Capability Analysis

Designed as a rich visual planning aid, this tool helps CISOs analyze and communicate information along multiple dimensions.

SecurityATLAS Portfolio Management Capabilities

Portfolio-based analyses give CISOs a pragmatic ability to optimize the allocation of security investments.

SecurityATLAS Security Roadmap

This is an actionable plan that helps CISOs implement the appropriate project mix in sequences that minimize rework and maximize value creation.

Analytical tools and templates

These help CISOs conduct graphically enhanced, multi-dimensional analyses focused on identifying capability gaps and optimizing project portfolios. In addition, current- and future-state scorecards provide a disciplined framework for setting goals and measuring progress.

A dynamic communication framework

A robust, multilayered reporting structure provides CISOs with a lens-based approach to tailoring communications for different executive and technical audiences.

SecurityATLAS Strategy Delivery Framework



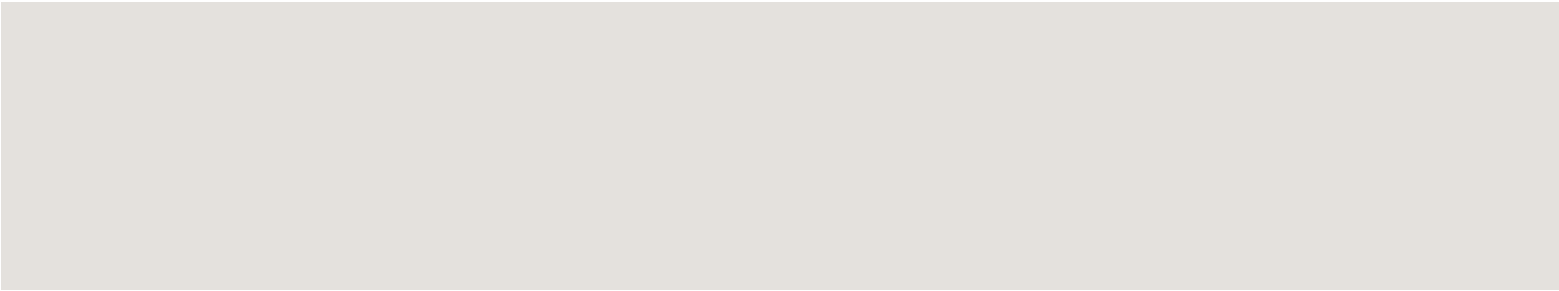
continued

SecurityATLAS Strategy Delivery Framework (continued)

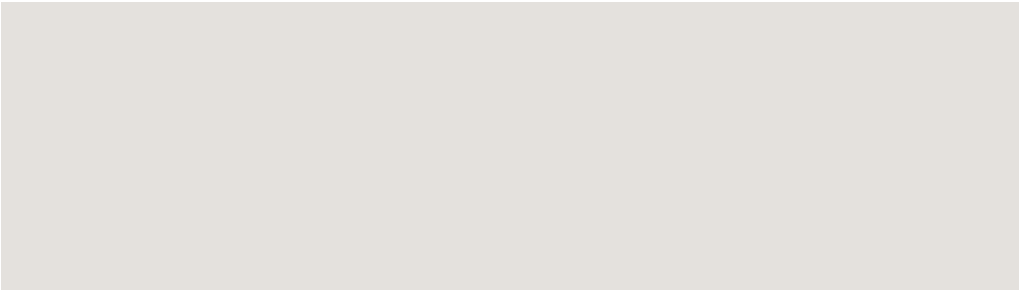
Analyze

Strategize

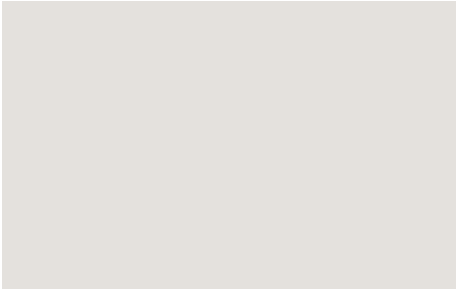
Align



Capability gap analysis
Current project alignment analysis



Project creation
Project prioritization



Investment optimization

Dynamic communication
Ongoing management

**Capability analysis
Project analysis**

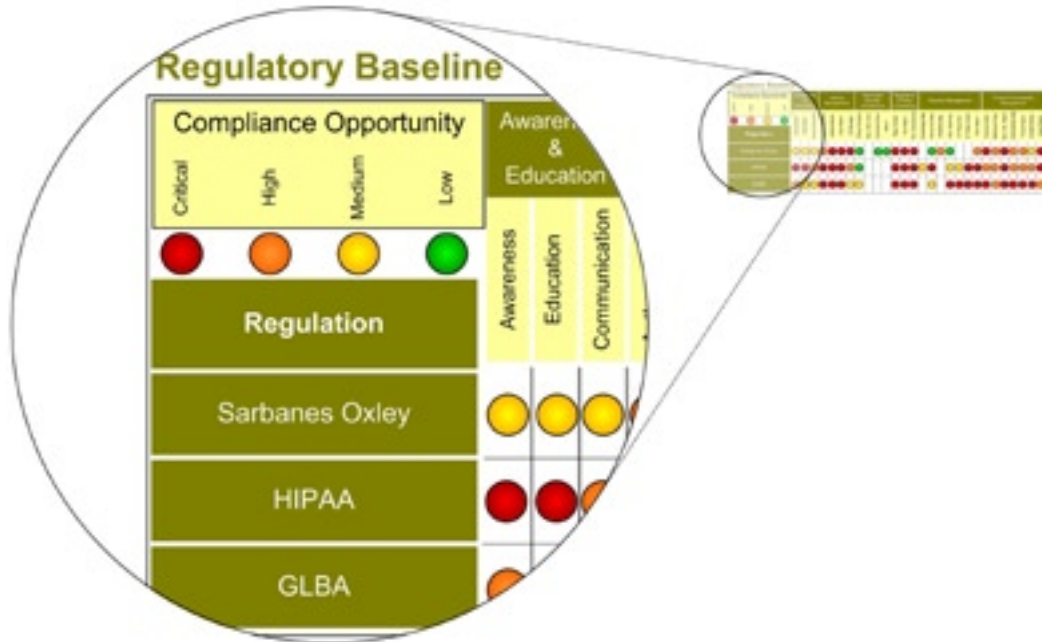
Project roadmap

**Dynamic communication framework
Security management framework**

SecurityATLAS Regulatory Baseline

See Page 21

The SecurityATLAS Regulatory Baseline provides organizations with a clear picture of how and where specific regulations impact the security agenda. Please note that the information presented here is merely representative. Regulations depend in large measure on application-specific circumstances, and the data illustrated here is not applicable to all industries or operating environments.



**SecurityATLAS
Industry Benchmark**

See Page 22

The SecurityATLAS Industry Benchmark presents a clear picture of how your industry is addressing key capabilities in the people, process and technology components of a security program.

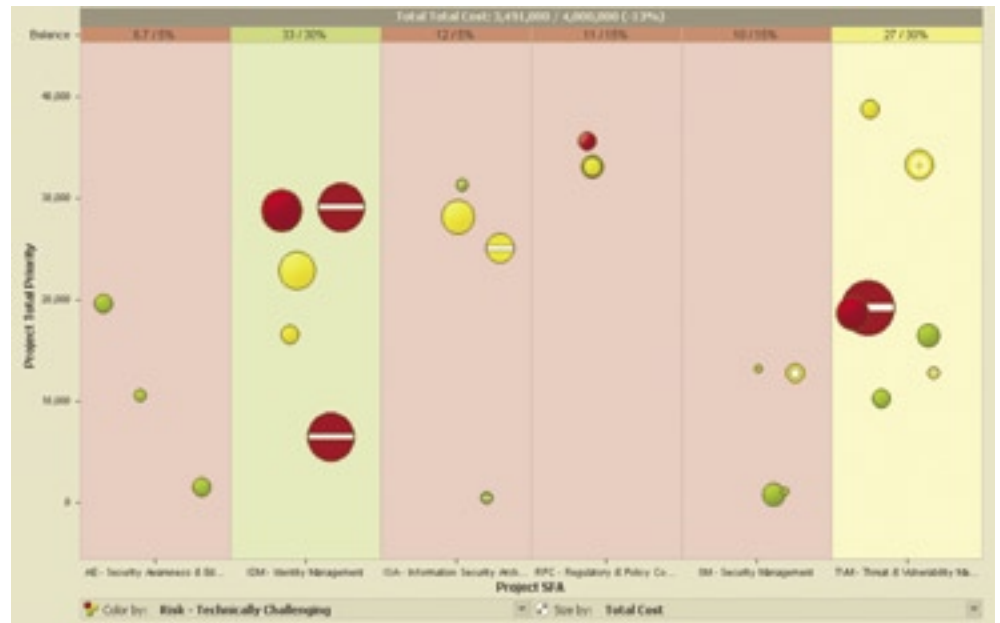
We maintain this database with information gained through a global survey of security practices around the world, as well as through thousands of hours of service to our clients in the context of security, governance, risk and compliance management engagements. Please note that the information presented here is provided on a sample basis only, and is not meant to be representative of any particular industry.

| Portfolios | BA01 - Business Gap | BA01 - Current State vs. Industry | BA01 - Regulatory Gap | BA01 - Weighted Composite Gap | Priority Score |
|---|---------------------|-----------------------------------|-----------------------|-------------------------------|----------------|
| By Dimensions | | | | | |
| 1 AI.1 - Awareness | ● | ● | ● | ● | ● |
| 2 AI.2 - Education | ● | ● | ● | ● | ● |
| 3 AI.3 - Communication | ● | ● | ● | ● | ● |
| 4 IDP.1 - Authentication | ● | ● | ● | ● | ● |
| 5 IDP.2 - Authorization | ● | ● | ● | ● | ● |
| 6 IDP.3 - User Management and Provisioning | ● | ● | ● | ● | ● |
| 7 IDP.4 - Identity Storage / Data Integration | ● | ● | ● | ● | ● |
| 8 ISA.1 - Enterprise Requirements Analysis & P | ● | ● | ● | ● | ● |
| 9 ISA.2 - IT Security Reference Architecture | ● | ● | ● | ● | ● |
| 10 ISA.3 - Common Security Services Infrastruct | ● | ● | ● | ● | ● |
| 11 ISA.4 - Security Implementation Methodology | ● | ● | ● | ● | ● |
| 12 RPC.1 - Regulatory Compliance | ● | ● | ● | ● | ● |
| 13 RPC.2 - Policies & Standards Management | ● | ● | ● | ● | ● |
| 14 RPC.3 - Policy & Standards Compliance | ● | ● | ● | ● | ● |
| 15 SPL.1 - Knowledge Management | ● | ● | ● | ● | ● |
| 16 SPL.2 - Personnel Management | ● | ● | ● | ● | ● |
| 17 SPL.3 - Portfolio Management | ● | ● | ● | ● | ● |
| 18 SPL.4 Enterprise Security Steering | ● | ● | ● | ● | ● |
| 19 SPL.5 - 3rd Party Relationship Management | ● | ● | ● | ● | ● |
| 20 SPL.6 - 3rd Party Contract Management | ● | ● | ● | ● | ● |
| 21 SPL.7 - Risk Management | ● | ● | ● | ● | ● |
| 22 TPL.1 - Intrusion Monitoring | ● | ● | ● | ● | ● |
| 23 TPL.2 - Malicious Program Detection | ● | ● | ● | ● | ● |
| 24 TPL.3 - Security Information Management | ● | ● | ● | ● | ● |
| 25 TPL.4 - Vulnerability Management | ● | ● | ● | ● | ● |
| 26 TPL.5 - Threat Management | ● | ● | ● | ● | ● |

SecurityATLAS Portfolio Management Capabilities

See Page 51

Through a portfolio-based approach to managing project mixes and inputs, SecurityATLAS gives CISOs a pragmatic ability to optimize the allocation of security investments. This is a complex undertaking that requires a coordinated ability to identify, integrate and allow adaptations to the people, process and technology components that collectively drive any complex set of security initiatives. The approach also provides management with transparency into how resources and funding are being allocated and which trade-offs arise when unexpected issues surface that compel executives to reconsider security investment priorities.



For more information, please contact:

James Quinnild, Partner
PwC Advisory
612.596.4486
james.quinnild@us.pwc.com

