Mastering the Risk/Reward Equation: Optimizing Information Risks while Maximizing Business Innovation Rewards

Report based on discussions with the "Security for Business Innovation Council"

1. Anish Bhimani, Managing Director, IT Risk Management, JP Morgan Chase
2. Bill Boni, Corporate Vice President, Information Security and Protection, Motorola
3. Dave Cullinane, Vice President and Chief Information Security Officer, eBay Marketplaces
4. Roland Cloutier, Vice President, Chief Security Officer, EMC Corporation
5. Dr. Paul Dorey, Vice President, Digital Security and Chief Information Security Officer, BP
6. Renee Guttmann, Vice President, Information Security & Privacy, Time Warner
7. David Kent, Vice President, Security, Genzyme
8. Dr. Claudia Natanson, Chief Information Security Officer, Diageo
9. Craig Shumard, Chief Information Security Officer, Cigna Corporation
10. Andreas Wuchner, Head IT Risk Management, Security & Compliance, Novartis

And guest contributor:
Julia Allen, Senior Researcher, CERT, Software Engineering Institute (SEI), Carnegie Mellon University

An industry initiative sponsored by RSA, the Security Division of EMC

Table of Contents

Executive Summary

For top-performing organizations, business innovation is not simply an event in time or a siloed laboratory project to generate a new product. It is an on-going, inter-disciplinary, cross-organizational effort to drive the business forward and create value. Forward-thinking security leaders have made tremendous progress in driving tighter linkages between business innovation goals and security actions. A critical element has been taking a more structured and strategic approach to organizational risk assessment.

The following report reflects the collective risk/reward lessons learned and best practices of 10 of the world's most accomplished information security leaders. It outlines a proposed methodology for making risk/reward calculations that drive optimum business value.

It starts with a shift in perspective for the security program from that of a technical specialty to a business advisory and consultancy. The goal then becomes to manage risks to an *acceptable level*, based on the enterprise's risk appetite with decision-making guided by a risk assumption model. A formal and repeatable process for making the risk/reward calculation helps to ensure that it is done consistently across the organization.

Making it sustainable requires a governance structure that integrates information risk management into overall enterprise risk management and has the support and involvement of executive leadership.

While many security teams are moving to build these competencies, they are doing so at varying speeds and levels of effectiveness. This report offers the first potential blueprint for achieving an information risk management program that enables business innovation and is offered in the spirit of advancing the interests of the industry.

II. Preface: The "Security for Business Innovation" Initiative

Business innovation has taken center stage in today's enterprises as the executive suite strives to harness the power of globalization and technology to create new value. Within the current environment, security strategies have a crucial role to play in achieving business innovation. Security can enable extremely efficient and competitive ways of sharing and processing information as well as managing mobile workforces, developing flexible collaborations and maximizing third-party relationships.

Yet for many new initiatives, the security team is brought in at the tail-end of the process to "bolt-on" the controls or is not even engaged in the process at all. At RSA, we believe that if security teams are true partners in the business innovation process, they can help their organizations achieve unprecedented results.

Most security professionals have also recognized that the goal is not to deploy the latest technology "du jour" or erect higher walls; it's about aligning security to business. The time is ripe for change; security must graduate from a technical specialty to a business strategy. But it is not an easy road.

Many security teams are still struggling to translate this understanding into concrete plans of action. They know where they need to go, but are unsure how to get there. This is why RSA is working with some of the top security leaders in the world to drive an industry conversation to identify a way forward.

RSA has convened a group of 10 highly successful security executives from Global 1000 enterprises in a variety of industries. The "Security for Business Innovation Council" is made up of some of the top minds in information security worldwide. We are conducting a series of in-depth interviews with the members of this Council, publishing their ideas in a series of reports and sponsoring independent research that explores this topic. RSA invites you to join the conversation. Come to www.rsa.com/securityforinnovation/ on RSA's web site to download primary research on this topic and view previous reports. Provide comments on these and contribute your own ideas. Together we can accelerate this critical industry transformation.

Business Innovation Defined

Enterprise strategies to enter new markets, launch new products or services, create new business models, establish new channels or partnerships, or achieve operational transformation.

"First and foremost, it is how you look at risk. Because I think the word, 'Risk,' has very negative connotations. 'Risk,' is not necessarily bad, because you have good risk and you have bad risk, and you have calculated risks. One of the things you must do from a security perspective is to look at risk from a very positive and balanced outlook. If you look at it from a negative outlook, it's going to lead you down a very risk-averse, very security-barrier sort of approach to coming up with solutions that don't enable the business to create value."

Dr. Claudia Natanson
Chief Information Security Officer
Diageo

III. Introduction to the Second Report

The first report in the Security for Business Innovation series, "The Time is Now: Making Information security Strategic to Business Innovation: Recommendations from Global 1000 Executives" defined a set of recommendations for how security professionals could make information security more strategic to business innovation. In particular, council members stressed the importance of one of the top recommendations: "Become a risk vs. reward expert." This second report explores this recommendation in more depth to help security and executive teams find the right balance between the level of risk versus the potential reward when it comes to business innovation.

This report specifically looks at *optimizing* rather than mitigating risks because optimizing is the right frame of mind when it comes to enabling business innovation. If you take away all risk, you take away all reward. Optimizing risks is about using risk-taking to its best advantage. As business innovation is about doing new things, like entering new markets, building new channels, creating new sourcing models and delivering new products, it inherently involves taking new risks. The enterprise must determine the magnitude of those risks and how much risk it is willing to take on, in order to maximize the rewards of a project.

Risks to information (confidentiality, integrity and availability) are just some of the risks an enterprise faces. As was evident from discussions with the Council for the first report, organizations worldwide are currently striving for a more consolidated view of all of the risks they face, including financial, legal, compliance, operational, market and strategic, etc. As enterprises attempt to look at risk management more holistically, processes for assessing information risks must be integrated into these overall risk assessment efforts. As such, this report also features contributions from Julia Allen, one of the leading researchers in the area of enterprise security and governance from CERT® at Carnegie Mellon University's Software Engineering Institute.

IV. What is the Risk/Reward Equation?

"So the reality is that at this point in the industry, it's not an overly scientific process. There is an assessment process by which you say 'Okay, what are the challenges this initiative poses? What are the risks it introduces?' You figure out the right level of controls that you need to put in place... You have to make security part of the cost of the initiative. And then if that changes, if it tips the balance, then you can generally go back and revisit it, the same way you would any other aspect of the initiative."

The risk/reward equation, like any equation, factors in many variables to arrive at a solution. When it comes to information security, it considers factors such as the type of information; its level of sensitivity and protection requirements; how it is being stored, processed or transmitted; the threats and vulnerabilities of the systems and applications; as well as the likelihood and impact of compromising events, etc. This will sound very familiar to anyone in information security, as it is the basis of a risk assessment to determine what security controls to implement. But the focus of a risk/reward equation is determining the right level of controls to put in place given an acceptable level of risk. And an acceptable level means that the owners of that risk are willing to take responsibility for that amount in order to maximize rewards.

Historically, information security has been singularly focused on the risks, but to truly enable business, you also have to keep your sights on the rewards.

Quantitative or Qualitative?

Ideally, the risk/reward equation would be based on hard numbers. As an illustration, in a perfect world an information security professional might be able to say something like, "This new business initiative is worth $100 million to the business (in savings or revenue, etc.) and there is a 10% chance that this particular detrimental event will happen; if it does, it will cost the business $250 million (in fines, direct incident costs, lost customers, etc.). The recommended security controls would cost $500,000, which would reduce the chance of that event occurring to 5% and the impact to $30 million, which is in line with the acceptable level of risk for this project."

Realistically, it may not always be possible to come up with hard numbers. Or they may not be as useful if the dollar values for information risks are on a completely different scale than other risks the enterprise faces (e.g. human safety or product liability issues). However making the calculation is still essential to making good business decisions. Even if the risk of a single event seems relatively small in terms of dollar value, organizations need a protocol for systemically calculating these risks because of the collective impact of all these risks across the organization.

Many organizations use well-defined "high, medium and low" risk definitions to describe probabilities and impact, or they use a numerical scale that assigns risk scores to qualitative measures (e.g. Risk scores of 1 to 9, with 1 representing higher risk events and 9 lower risk events; or scores for "CIA" risks of Confidentiality, Integrity and Availability). Others don't score risks, but rather make relative comparisons to identify the risks they believe to be relatively higher than others.

The key is ensuring that there is a clear and consistent understanding among security and business executives and personnel of what is meant by "high, medium, and low," the numbers on the scale or the relative ranking. One of the ways to approach this is to have very detailed, documented scenario descriptions of events that provide illustrative examples of different risk-level events such as a "low risk event", or a "Level 3 event."

Hard numbers may be easier to obtain over time as the discipline of information risk management matures. The "actuarial" data simply does not exist today. In other more mature disciplines such as physical security, the data and methods do exist to calculate, for example, that security will be 1.5% of capital costs for a particular type of building. It also depends on the organization itself; the management team may not have collected enough historical data but may be in the process of doing this, so they will eventually have hard numbers. At this point, many enterprises still have not identified critical information assets nor calculated the true value of these assets to the business. These are essential first steps.

"Risk/reward decisions are business decisions. Not security decisions. So the business has to be involved and there have to be baseline policies in place that follow a standardized way to make the determination. So it doesn't matter if I make it in June, July or August, against business unit one, two or three, the baseline assumptions and questions are the same, to have a standardized conversation with the business."

Roland Cloutier
Vice President, Chief Security Officer
EMC Corporation

However, there is considerable debate about whether the goal should be or could be to come up with hard numbers. Certain intangible variables, such as a decrease in customer satisfaction or loyalty, are extremely difficult to quantify. Some organizations, depending on their vertical industry and/or culture, have an expectation that information security must provide hard numbers for decision-making purposes. Others use a mix of quantitative and qualitative, quantifying what they realistically can and describing other variables qualitatively.

V. Moving from "Information Security" to "Information Risk Management"

A key component of building a security program that enables innovation is moving from "information security" to "information risk management (IRM)." The definition of IRM must incorporate the idea that information security is striving for an acceptable level of risk (see next page). The goal is to match risk exposure to risk appetite, not wipe out all risk. Having specific expertise in information security per se is still a crucial part of the program as it is essential for determining the optimum security controls. However, a risk-based approach shifts the security perspective from a technical IT specialty to a business advisory and consulting function. Managing information risks must be conducted in a way that is meaningful to the business and is based on how other categories of risk are discussed and calculated. So IRM must be integrated into the enterprise risk management framework.

Recently, there has been a growing recognition of the need to take a risk-based approach to security. Different organizations are at different stages along this progression, based not only on how they view information security and its importance to the business but also on the maturity of their enterprise risk management program.

There are some preconditions that are essential to the success of any security team's efforts. First, the organization must already be using the construct of "risk" in how they make investment and operational decisions. Some organizations may not have the culture for a risk-based approach as their strategy is still too tactical or "targeted opportunity" focused. The other key prerequisite is there has to be sustained attention from the top. If there is no attention for enterprise risk management or at least some notion of assessing risk at the board or senior leadership level, then trying to be effective in information risk management is likely beyond the organization's current capability.

"My experience in research tells me that there is a set of preconditions that must exist. Otherwise having security folks try to go down the path of information risk management, in the absence of some kind of key prerequisites, is not going to work."

Julia Allen, Senior Researcher, CERT
Software Engineering Institute
Carnegie Mellon University

"For us to effectively implement controls into the enterprise, my theory is that we have to have a risk- based approach, because we're fundamentally poor. I cannot spend all the money, even if I wanted to. So we have to take the most effective approach at identifying those potential risks to the business and protecting those things that need protecting."

Roland Cloutier
Vice President, Chief Security Officer
EMC Corporation

"My ultimate vision is that security and controls will be like a thermostat for maintaining an acceptable degree of comfort for the inhabitants of a particular building. If it's too hot, air conditioning kicks on. It gets too cold, heating kicks on. So how do I build a process control model for information protection? That's what we're heading towards."

Bill Boni, Corporate Vice President
Information Security and Protection
Motorola

Information risk management is…

"Identifying and measuring the risks to information* and ensuring that the security controls implemented keep those risks at an acceptable level to protect and enable the business"

Note: As information risk management is an emerging discipline, there is still no universally accepted definition. This definition is put forth to clarify the use of the term within this report. This definition is a compilation of concepts based on discussions with the Council and it should be duly noted that there was no one definition used. Definitions varied greatly and it was even thought by some that "information" risk management is perhaps too narrow and what should be defined is actually "operational" risk management, which is more broadly concerned with protecting the business as a whole and not just the information. However, the perspective varies with the type of organization, organizational structure and areas of responsibility.

*Includes the systems, applications, networks and infrastructure that processes, stores and transmits that information

VI. Determining Risk Appetite

Since the goal of information risk management is to manage risks to an acceptable level, you have to be able to figure out what acceptable looks like. E&Y defines risk appetite as: "A measure of the amount of total risk that a company is willing to accept in pursuit of its business objectives and goals."

While risk appetite is not a new concept in business, it is only during the past several years that many organizations worldwide have actually started to formalize risk decision-making. This shift has been prompted by government mandates such as Basel II or Sarbanes-Oxley, as well as shareholder and stakeholder demands for more transparency in how decisions are being made. Formalized structures for establishing and articulating risk appetite are just beginning to take shape.

An enterprise's appetite for risk is very organization-specific and is driven by factors such as vertical industry, size, culture and regulatory regime. For example, a retail company is going to have a different risk appetite than a bank, utility or a high-tech start-up. And it will change over time, based on market position, business and brand objectives and leadership.

It may also vary from one business unit (BU) to the next. Some organizations operate in a decentralized model and allow BUs to have more latitude in determining risk appetite. Others demand a more consistent appetite across the organization. The ultimate objective is a consistent decision-making process and a consistent interpretation of risks across the organization. This approach also ensures that one particular BU's risk appetite and risk decisions don't impact other divisions or the whole enterprise.

Sources for determining enterprise risk appetite

Because Enterprise Risk Management (ERM) is a relatively new discipline, the risk appetite and especially the appetite for information risks are rarely spelled out for information security professionals. You have to go to several sources to figure it out.

An excellent source to start with is statements made by the Board of Directors (BOD) or senior leadership. They may have made statements about their risk appetite and communicated those to the organization. For example, the board may have outlined strategic directives and delineated the major risks to achieving business goals and what the organization is doing to address them. The security professional will have to seek out statements or references to risk from various documents such as annual reports, risk reports filed with the Securities and Exchange Commission or shareholder reports.

Another source is conversations and discussions with the BOD, senior leadership, business unit leaders and other business executives. Speak to the chief executives in disciplines including corporate responsibility, public policy, human resources, marketing and business development. Get input from the Enterprise Risk Committee (ERC). Depending on the maturity of the program, the ERC may determine the top strategic business protection requirements. (The ERC is discussed in detail in the "Making it Sustainable: Governance" section). Another important source is "situational analysis", gauging the market and your company's position in the market over time; knowing your organization's business objectives; and understanding what is happening in your vertical industry, etc.

"Take a look at documents like the mission statement and the shareholders report, because they will tell you right away what the business is focused on and what some of the key risks are. There's a good chance that whatever you're working on is in line with whatever they've broadcast out. And if you're talking risk, if it shows up in the shareholders report, then it's important to the business."

Making the translation to information risk appetite

In almost all cases, the information security officer will likely have to take general statements of risk appetite and translate or interpret them into specific statements of *information* risk appetite. You have to be smart enough about the business to be able to make the translation from statements related to business to statements of information risk. Try to figure out where security can add value to particular business objectives.

For example, take a BOD statement about the business objective of "preserving customer trust" and drill down to an equivalent information risk management statement. The risk to preserving customer trust would be unauthorized disclosure of personally-identifiable information (PII). For statements of information risk, find all the various ways in which PII is stored, processed, transferred and handled, and then explain the risks to that information and the controls which would help preserve customer trust. Map it back to the direct statements made by the board.

One suggested approach is to do a *failure mode effects analysis*. For example, take the macro level business goal of "Customers buy a certain level of product this year" and start going through questions that address how the company might fail. Would the company fail if it didn't identify customer needs or build the right solutions to meet customer needs or desired price points? Then look at the information risks that go with those. The company would fail to meet the objective if it doesn't collect, process and analyze information on a timely basis or if the information has been modified or misappropriated. A failure mode effects analysis can eventually lead down to, for example, "Windows systems are not being patched in seven days" or "The disaster recovery capability for the mission critical tier 1s don't meet our needs for our recovery time objectives" etc. As you decompose the elements involved in attaining a business goal, you eventually cross from business concerns into information technology concerns.

To understand exactly how much appetite the enterprise has for particular events, consider developing descriptive scenarios involving various information security events and then take these to the ERC, senior leadership and/or the BOD. Ask them to try to draw a line and say, "We'd accept this kind of risk, but not that." This will give you a feel for the general risk appetite for a given point in time. It needs to be regularly reviewed to reflect changing conditions. Risk appetite also varies depending on the initiative: how important is it to the company? Perhaps it is so important to attain a competitive advantage that the business is willing to take on a higher level of risk than for other projects.

"The senior leadership position should be established either as a policy or some kind of formalized statement of what the risk appetite for the organization is, so people have a sense of what the ground rules are."

Julia Allen, Senior Researcher, CERT
Software Engineering Institute
Carnegie Mellon University

VII. Building a Risk Assumption Model

> "Certain risk decisions must be made by more senior positions in the organization. If they are made by individual business units, they could have a negative impact elsewhere in the organization because of shared computing infrastructure. Business unit managers understandably are focused on their own localized activities and won't necessarily have as strong a holistic understanding of how their decision can impact the rest of a global organization."
>
> Craig Shumard
> Chief Information Security Officer
> Cigna Corporation

Conversations about risk invariably come down to who has the authority to make what level of risk decision. Having a formalized risk assumption model for information risks brings clarity and transparency to the process and delineates where and with whom risk-decision responsibilities lie. Depending on the maturity of the company's processes, it may still be relatively ad hoc, it may be well understood but informal, or it may be formalized and documented. Formalizing and documenting it may be undertaken by the Enterprise Risk Committee (ERC) (see "Making it Sustainable: Governance" section) or by the CSO/CISO in discussions with the BOD, senior leadership and the business.

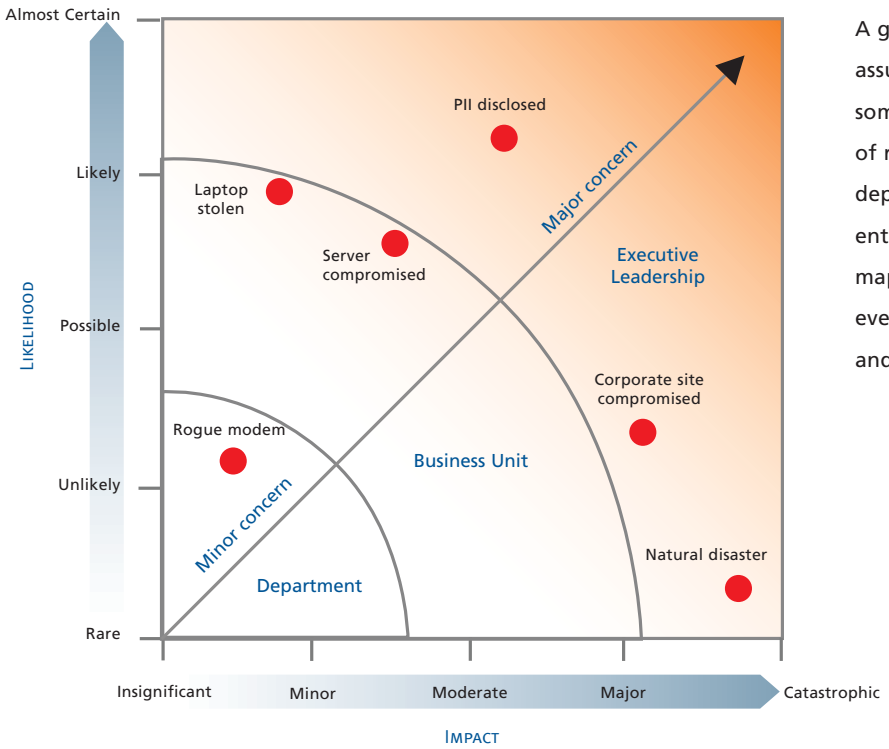
Understanding risk ownership is key. Although risk is owned by the business, business leadership may not yet completely understand all of the risks or recognize that they own the risks. A Risk Assumption Model formalizes risk ownership: "Ownership shifts from security being owned by those with technical expertise to security being owned by the business, which is the driver and ultimate benefactor. Ownership answers the questions 'Who has the authority to act?' and 'Who is accountable and responsible?'" (Governing for Security, Allen, 2005)

A framework for decision-making authority

Relatively mature programs will have established a framework that maps risk decision-making authority to levels of hierarchy or roles within the company. For example, scenario-based descriptions tie certain types of events to risk levels (which reflect the magnitude of the risk, taking into account reputational damage, financial loss, other impacts, etc.). A risk assumption model maps the different magnitudes of risk to different authority levels within a company, delineating who can make each kind of risk decision. For example, at what level can the business take on a particular risk? Department head? Business unit head? Group head? C-level executive? Board?

Some companies have risk-scoring systems based on, for example, a scale of 1 to 9, with 1 being the highest risk. If a risk is scored between 1 and 3, only the board or executive leadership can make a decision to accept this kind of risk; if it's 4 to 6, only a division head can make a decision; and if it's 6 to 9, the decision can be accepted at a local level.

In some companies where business units have radically different business objectives, risk appetite is business unit dependent. Also, BU leaders' personalities may differ; some may be gamblers, and others may be conservative. The risk assumption model establishes the level of risk that each leader *can* assume.



A graphic representation of a risk assumption model might look something like this: various grades of risk decision authority – from department to business unit to enterprise executive leadership – are mapped to several potential security events, which have certain likelihood and impact.

"I don't think it's appropriate for people who are not in senior positions to potentially make risk decisions that could sink the entire ship. You've got to have some kind of process for identifying high, medium or low risks, determining what the impact would be to a department, business unit, or the corporation and then figuring out what the right level of acceptance is."

VIII. Creating a Step-by-Step Process

"Try to push self-service enablement as far forward to the front or, as deep into the organization as you can so that more choices are being made with more informed insight than ever before. Over time you're basically creating less risk for the enterprise because better choices are being made in local environments. The benefit of self-service enablement to the security practitioners is that instead of dealing with the dreary, mundane, repetitious, monotonous, tedious, detailed daily hygiene of answering the same question a thousand times for a thousand different people, you're dealing with the new, the unique, the difficult, the dangerous, the exciting, the leading edge."

Bill Boni, Corporate Vice President
Information Security and Protection
Motorola

Although it varies from one organization to the next, there seems to be a common, emerging step-by-step process for making a risk/reward calculation for new business initiatives. Most companies do not yet have this entire process in place, but many are well on their way to formalizing a similar approach. While not all of the prescribed steps in this process are suitable for every company, they serve as a useful resource to consider.

The key to success in this step-by-step approach is transparency. In order for security leadership to make a proper assessment of the risk, there needs to be openness, dialogue and a high degree of trust with the business. This means security team members must be willing to openly justify their actions and decisions, and never just say to the business, "You can't do that because it's not secure," with no explanation. Otherwise, the business will discount security's role and opinion and will continue to view this key function as a barrier rather than an enabler.

The five general steps for making a risk/reward calculation are as follow:

1. New initiative proposed

A line of business or functional area initiates a new project. This could be any type of project from the routine to a "blue sky" initiative; and from a small initiative involving one department to a very large one that involves the entire business unit or even the whole enterprise. Some examples include: building a new customer web site, outsourcing customer service, automating the supply chain system, or conducting a major merger or acquisition.

2. Reward calculation

Depending on the company, the business executives who are proposing the initiative develop a business case or project proposal that lays out the opportunity. Most enterprises have a fairly rigorous business case process whereby the project must be described and documented, including goals, benefits, budgets, timeline, etc. Benefits include strategic benefits to the organization like increased market share; "hard" benefits like revenue, additional sales or cost savings; and "soft" benefits such as enhancements to the business operation, improved communications, and better education of consumers.

Typically, the business case or project proposal is augmented by discussions between the business and security teams. These discussions should allow the security team to determine the controls needed to achieve an acceptable level of risk. If the security team does not fully understand the reward side of the equation, they may misapply tools and create barriers that will be objectionable to the business and hinder the initiative. At this step, it's important that the security team demonstrates to the business that they "get" the value that this initiative offers the organization. This gives the

Who does what?

For any new initiative, the roles involved in determining the risk/reward calculation will be: those who actually make the calculation (the business together with the security team); those who govern the whole process (the Enterprise Risk Committee); and those who have set the risk parameters (the Board of Directors, Executives, and Business Leaders). The security team's role is to guide, advise and educate business leaders to a point where they not only have a solid understanding of the risks, but also recognize that they own those risks and can make decisions from a well-informed position. Information security also creates the tools to enable the business to do their own "first pass" risk calculations independently (in a self-service model). For projects that exceed a risk threshold, members of the security team work in collaboration with the business to make the calculations. Some security teams employ dedicated risk management specialists with focused knowledge while others demand that everyone on the team have at least a general risk assessment capability.

security team credibility and aligns their efforts with business objectives.

3A. Risk calculation: "first pass" is done by business in a "self-service" model

The business completes a short self-service risk questionnaire, which will provide an initial rating for the project. The questionnaire likely captures the type of information being collected or used by the project (such as personally identifiable information (PII), intellectual property or financial data, etc.), where that information resides (such as on laptops, in databases, in applications etc.), the confidentiality, integrity and availability requirements, and the architecture of the systems involved (internal network, remote office, third party location, etc.). This helps to identify and measure the potential risks based on the threats and vulnerabilities and the likelihood and impact of events (i.e. damage to reputation, revenue loss or non-compliance with regulations).

If the risk score or risk description resulting from the questionnaire is relatively low, then the business proceeds on its own to implement the controls as pre-determined by the security department (see Step 4). In developing a formalized risk management process, many organizations are moving towards this "self-service model" in which the business conducts its own first-pass risk assessment and implements a standard set of controls.

The tools to complete this self-assessment are developed by the security team to empower the business to do the initial risk calculation. Many security programs have instituted a workflow system to monitor and track the business' calculations. This ensures the controls are implemented and the risks mitigated to the right level. Not all security programs have the "self-service" model in place yet, but many are working toward this vision. For the security programs that have already implemented some form of self-service, the objective is to continue to enhance it.

The self-service model helps to ensure coverage of risk assessments throughout the organization. In large, global enterprises, it is likely impractical for security team members to be able to have enough resources to do every single risk assessment themselves. Speed is another benefit; the tools can provide for fast self-assessments so that security reviews aren't choke points in the business innovation process. Self-service also allows the security team to focus on the less routine projects. It also can improve overall security posture because the business project managers are thinking about security risks.

3B. Risk calculation: if risk is relatively high, the security team does further analysis

Based on the self-service risk questionnaire, if the risk score or description categorizes the initiative as too high for a standard approach, the business will then "call in security" to further analyze risks and build a custom solution. The risk assessment methodology employed by the security team is typically developed in-house based on components of various standards such as ISO, NIST, ISF, OCTAVE, etc. It seems that most organizations don't conform to one particular standard, but rather take bits and pieces of multiple standards and then make it their own based on their organizational context.

Explaining the details of a risk assessment methodology is beyond the scope of this report. There are many publicly available resources which provide standards and guidance on security risk assessments (see a list of resources at the end of this document). For external data sources, the members of the Council use industry threat reports and data from analysts to some extent. For external benchmarking, vertical industry data is considered the most relevant, but it can also help to benchmark against companies with similar characteristics such as size, geography, culture and operations, and not necessarily from within the same industry.

The scope and level of effort involved in a risk assessment will vary greatly depending on the nature of the project being undertaken. Projects with high value or "blue sky" initiatives – which are entirely new and have never been undertaken by the organization – may require deeper analysis, and certain initiatives may have more urgent time frames. A broader risk assessment is required, for example, if a project involves setting up a location or a partnership in another country. For this type of initiative, the risk assessment would need to include an in-country threat analysis.

4. Security controls determined and implemented: either standard or custom solution

As determined in step 3 above, the project may be relatively standard (a new initiative that is very similar to ones undertaken in the past like building a customer web site). For standard projects, the security team has built a "solutions library" of templates to follow and the business "helps themselves" and selects the right set of controls to implement for their project. Some projects may require "facilitated" self-service, where the security team walks the business through the process.

For the higher-risk projects, information security develops a custom solution that reflects the rewards of the project, the general risk appetite, risk appetite for this particular initiative, risk assessment, as well as the cost, time and effort required and the resources available. Completely new "blue sky" projects will require some level of conjecture as to the appropriate controls because there won't be any significant historical data upon which to base strategies.

The security team works collaboratively with the business throughout the whole process and then presents its recommendations. This process is also typically a negotiation that involves back-and-forth deliberations to arrive at a solution. Depending on the organization, control implementation may be performed by IT operations with advisors from security or it may be performed by the security team.

5. Escalation and dispute resolution

If the security team and business executives can't arrive at an agreed solution (for example the security team believes that the business is taking on too much risk or the business believes that the controls are too onerous or expensive), there is an escalation process to resolve the dispute. Either the security team or the business executives can escalate the decision to a higher decision-making authority. Depending on the structure of the organization, the decision may be escalated to a single executive such as the COO or CFO or the Enterprise Risk Committee, who makes a final ruling.

In addition, if the information security officer believes that the risks being taken by the business are excessive, there may be a "sign here" process whereby the business literally signs an agreement documenting security's objections and formally assumes the risk and the associated responsibility for any consequences if risks are realized. All of the Council members stressed that it is extremely rare for initiatives to be escalated in this manner. For the most part, the business and security teams work cooperatively to negotiate a solution that all parties can accept.

"You have to be close enough to the business to understand their goals and objectives. You need a detailed understanding of why they're examining this course of action, and then you can align security to support that. If you don't have that detailed understanding, you're going to misapply the tools of security in a way that's going to create barriers."

David Kent
Vice President, Security
Genzyme

"Most people want to work with the security team to come up with a solution that brings the risk down to a level where it's in their ability to accept it, or it's been mitigated really low so everyone agrees it's immaterial. So most projects in organizations would likely never need to be escalated."

Dr. Paul Dorey
Vice President, Digital Security
Chief Information Security Officer
BP

IX. Making it Sustainable: Governance

Governance is...

Setting clear expectations for the conduct (behaviors and actions) of the entity being governed, and directing, controlling, and strongly influencing the entity to achieve these expectations. It includes specifying a framework for decision making, with assigned decision rights and accountabilities, intended to consistently produce desired behaviors and actions. (Allen, 2005)

To effectively manage information risks for business innovation on an ongoing basis, a governance structure must be in place. This ensures that the effort is sustainable. Information risk management should be built into business strategy and processes and into overall enterprise risk management. Risk decisions should be based on a well understood and defined methodology, which needs to be communicated throughout the organization. Everyone needs to understand and carry out their roles. Governance aims for clear expectations and consistent results (see definition in the sidebar).

The process must ensure that information security is always in the loop, and that security teams are consistently engaged early enough in new project initiatives to enable business innovation. Some organizations use very formal processes to ensure business leaders take every new project through a series of "gates" to obtain the necessary approvals. At each phase in the project, the business must engage security to some degree. In some organizations, the business must obtain security sign-off for funding approval.

The approach and level of formalization depends on the maturity of information risk management (IRM) and enterprise risk management within that enterprise. It is also dependent on the culture of the organization. Some organizations have a more conversational and relationship-based collaboration that doesn't require an overly formalized structure, but still offers well-defined processes for decision-making. Table 1, a "Maturity Framework," synthesizes Council member experiences as described in this report. It presents a progression towards an information risk management (IRM) process for enabling business innovation. Each category represents a related set of practices for the IRM process.

Enterprise Risk Committee

An "Enterprise Risk Committee (ERC)" governs the overall risk/reward calculation process. Formal names for these committees vary – Global Risk Council or Executive Risk Board are some examples – as do committee structures and levels of formality. But generally, they provide oversight to the management of risk within the enterprise. It is the team responsible for ensuring that the risk/reward calculations happen and that there is a consistent methodology for making those calculations that is used throughout the organization. The Committee members may occasionally get involved in making actual calculations for example, for very large initiatives with enterprise-wide implications or if an escalation process has been triggered.

Many companies have established some form of an ERC; some are in the process of building a more formalized structure, and others already have one in place. It depends on the industry, size of the company, maturity of the program and culture of the organization.

Generally, the Committee is a cross-organizational and cross-functional team consisting of the most senior executives from such functions as security, information security, risk management, privacy, human resources, public relations, legal, as well as business unit executives. The Committee may be chaired by the CSO/CISO if he/she is in the best position to be chair. Subject matter expertise is typically not the major determining factor for selecting the chair, but rather connections and influence within the organization.

The Committee may report to the Board of Directors and/or a senior officer such as the Chief Operating or Financial Officer, or directly to the Chief Executive Officer. Or the committee may report to (or have a dotted line to) the Audit Committee. A common theme is that efforts towards establishing a formal ERC are often prompted by an audit finding and it is the audit executives or the Board Audit Committee that initially gets the ball rolling.

Often the ERC functions much like the UN Security Council in that it is comprised of several permanent members and rotating members are brought in based on current issues or risks. For example, a rotating member might be the VP of Customer Service because a particular project involves outsourcing customer service; or the VP of Engineering may be called to sit on the committee to assess the risks involved in building a collaborative product development platform; or the VP of Manufacturing for automating the supply chain, etc.

The ERC typically meets on a regular basis (e.g. monthly or quarterly) to review big picture enterprise risks (including information risks) and to gauge the overall security position as environments and circumstances change, such as system upgrades, new threats, new laws, etc.

Other structures include having an ERC for overall risks and having sub-committees for operational risks or information risks. Or each business unit may have their own localized risk committees that roll up into an overarching enterprise committee. Another example is an enterprise risk management process overseen by three risk co-committees: the Operational, Financial, and People Risk Committees.

If this type of overarching steering committee does not yet exist, this may be an opportunity for the information security officer to take the lead in creating one. This would expand the role of the CISO to include information risk management and allow him/her to be integral in establishing a formalized information risk management program.

Some organizations do not yet have a formalized risk committee, but use a process that is less structured and more based on relationships and conversations. A less formalized approach may be better suited to the size or culture of the organization. In this case, the information security leadership must have access to the executives when needed. This requires not only transparency and good communication, but also well-informed executives who are concerned with and engaged in information risk management.

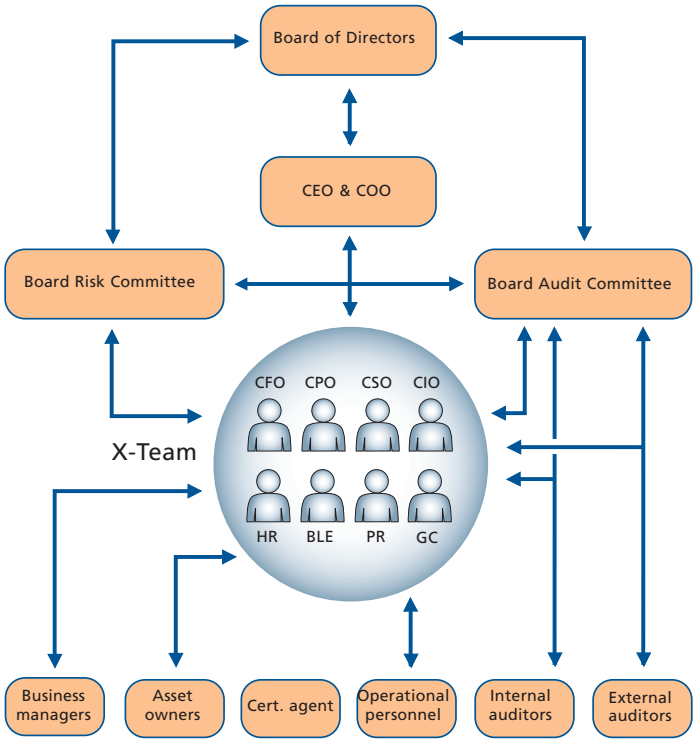
There seems to be no "most mature" or best Enterprise Risk Committee structure. The key is simply that there *is* a committee that oversees the information risk management process in a manner that best suits the organization and involves all key decision makers and stakeholders.

"To ensure that security is part of business innovation, you have to have a process in place. For example, for every credit request, there should be a stopping point - a mandate should be required. The mandate would be a business case. Then every credit request which is higher than a certain amount must go through a security review. The process methodology should include security sign-off points built-in to the project phases, mandatory stuff the business has to do."

Andreas Wuchner
Head IT Risk Management, Security & Compliance
Novartis

"Security is nothing special. It's not different than other business processes or risk management approaches. It integrates with and ties to and involves a lot of the same people that other types of risk management conversations involve. So information risk management should look like any other risk management conversations inside of the corporation."

Julia Allen, Senior Researcher, CERT
Software Engineering Institute
Carnegie Mellon University



Example of what an "Enterprise Risk Committee (ERC)" might look like is an "X-Team" (cross-organizational) comprised of the Chief Security Officer (CSO)/Chief Information Security Officer and/or Chief Risk Officer, Chief Privacy Officer (CPO), General Counsel (GC), the Vice President of Human Resources (HR), Business Line Executives (BLEs), Vice President of Communications or Public/Investor Relations (PR), Chief Financial Officer (CFO), and Chief Information Officer (CIO). The "X-Team" reports to the Chief Executive Officer (CEO) or Chief Operating Officer(COO) and Board of Directors; with oversight from the Board's Audit and Risk Committees. Several groups would execute on various aspects of the enterprise risk strategy such as the Asset owners, the Business managers, and the Operational personnel, including procurement personnel. Internal and external audit personnel are responsible for auditing the enterprise risk management program and the Certification agent is an independent agent who reviews all systems and assesses whether they follow prescribed best practices and standards.*

"An enterprise risk council consists of several members of the executive committee and the CISO. That's who makes the final decision and says , 'Now this is a risk that can't be accepted. We need to mitigate this risk by doing what the security team is saying,' or 'No, we as a business are willing to accept this risk. We recognize and appreciate security's recommendations, and the recommendations will be noted, but we've decided as a business decision we need to take this risk.' That's what regulators or auditors are looking for. They want to see your assessment of the risks and that you've made the decision as a business to accept those risks. You need to be able to prove to them that you have a good process."

Dave Cullinane
Vice President and Chief Information Security Officer
eBay Marketplaces

*NOTE: The above diagram is derived from "Figure 3: Roles Involved in an ESP," from the Technical Note "Governing for Enterprise Security (GES) Implementation Guide" by Jody Westby and Julia Allen, CMU/SEI-2007-TN-020, Copyright 2007 by Carnegie Mellon University and is used with special permission from the Software Engineering Institute.

X. Conclusion

Any new business innovation inherently carries its own unique risk/reward equation. If security teams look only at "mitigating risk," without enough focus on the reward, they can end up erecting barriers to innovation. There is a need to fundamentally shift perspectives. Security teams must mobilize to develop the practices, tools and relationships necessary to effectively define and assess the level of acceptable risk required for each new innovation to yield maximum business reward. By defining and implementing a process and putting in place a governance structure, organizations will ensure that the risk/reward calculations are executed and governed for enterprise success.

Developing these competencies in the risk/reward equation will help security teams go a long way on the road to enabling business innovation. Many security teams have already embraced the idea that security must align with business. One of the key aspects for realizing a program that aligns with business is mastering the risk/reward equation.

Next Steps

RSA is honored to be working with the some of the brightest minds in security; we hope you can learn from the Council's experience and apply it to your own programs. Watch for our next reports which will continue to look at other important topics regarding security's role in the business innovation process.

We invite you to be part of this initiative. Go to www.rsa.com/securityforinnovation to access all of the reports as well as other research. Sign up to receive notices when reports are released or research published. Contribute your own ideas. We've built a platform for collecting and promoting the best ideas. Here you'll also find tools to evaluate your own security programs to determine how far you've come and how far you have to go. Join the conversation. Help define a new approach to security that enables business innovation.

Appendix 1. Security for Business Innovation Council Members' Biographies

Anish Bhimani, CISSP
Managing Director,
Risk and Security Management,
JP Morgan Chase

Anish has global responsibility for ensuring the security and resiliency of JP Morgan Chase's IT infrastructure and supports the firm's Corporate Risk Management program. He oversees security architecture and participates in the firm-wide technology governance board. Previous roles include being a senior member of the Enterprise Resilience practice in Booz Allen Hamilton and Senior VP and CTO of Global Integrity Corporation and Predictive Systems. Anish authored "Internet Security for Business" and is a graduate of Brown and Carnegie-Mellon Universities.

Bill Boni
Corporate Vice President,
Information Security and Protection,
Motorola

Bill has spent his professional career as an information protection specialist and has assisted major organizations in both the public and private sectors. Bill has helped a variety of organizations design and implement cost-effective programs to protect both tangible and intangible assets. He has pioneered the innovative application of emerging technologies including computer forensics and intrusion detection to deal with incidents directed against electronic business systems.

Dave Cullinane, CPP, CISSP
Chief Information Security Officer
and Vice President,
eBay Marketplaces

Dave has more than 20 years of security experience. Prior to joining eBay, Dave was the CISO for Washington Mutual, and held leadership positions in security at nCipher, Sun Life and Digital Equipment Corporation. Dave is involved with many industry associations including as current Past International President of ISSA. He has numerous awards including SC Magazine's Global Award as CSO of the Year for 2005 and CSO Magazine's 2006 Compass Award as a "Visionary Leader of the Security Profession."

Roland Cloutier
Vice President,
Chief Security Officer,
EMC Corporation

Roland has functional and operational responsibility for EMC's information, risk, crisis management, and investigative security operations worldwide. Previously, he held executive positions with several consulting and managed security services firms, specializing in critical infrastructure protection. He is experienced in law enforcement, having served in the Gulf War and working with the DoD. Roland is a member of the High Tech Crime Investigations Association, the State Department Partnership for Critical Infrastructure Security, and the FBI's Infraguard Program.

Dr. Paul Dorey
Vice President Digital Security and Chief Information Security Officer,
BP

Paul has responsibility for IT Security and Information and Records Management Standards & Services globally across BP, including the digital security of process control systems. He has 20 years management experience in information security and established one of the first dedicated operational risk management functions in Europe. Prior to BP, he set up strategy, security and risk management functions at Morgan Grenfell and Barclays Bank. Paul has consulted to numerous governments, was a founder of the Jericho Forum, is the Chairman of the Institute of Information Security Professionals and currently sits on the Permanent Stakeholders Group of the European Network Information Security Agency.

Renee Guttmann
Vice President, Information Security and Privacy Officer,
Time Warner Inc.

Renee is responsible for establishing an information risk-management program that advances Time Warner's business strategies for data protection. She has been an information security practitioner since 1996. Previously, she led the Information Security Team at Time Inc., was a security analyst for Gartner, and worked in information security at Capital One and Glaxo Wellcome. Renee received the 2008 Compass Award from CSO Magazine and in 2007 was named a "Woman of Influence" by the Executive Women's Forum.

David Kent
Vice President, Security,
Genzyme

David is responsible for the design and management of Genzyme's business-aligned global security program. His unified team provides Physical, Information, IT, and Product Security along with Business Continuity and Crisis Management. He specializes in developing and managing security programs for innovative and controversial products, services and businesses. Previously, he was with Bolt Beranek and Newman Inc. David has 25 years of experience aligning security with business goals. He consults, develops and coordinates security plans for international biotechnology trade meetings and serves as a pro-bono security consultant to start-up and small biotech companies. David received CSO Magazine's 2006 Compass Award for visionary leadership in the Security Field. He holds a Master's degree in Management and a Bachelor of Science in Criminal Justice.

Dr. Claudia Natanson
Chief Information Security Officer,
Diageo

Claudia sets the strategy, policy, and processes for information security across Diageo's global and divergent markets. Previously, she was Head of Secure Business Service at British Telecom, where she founded the UK's first commercial globally accredited Computer Emergency Response Team. She has served as Board and Steering Committee member of the world Forum of Incident Response and Security Teams and is currently Chair of its Corporate Executive Programme. She is active in a number of European Initiatives involving areas such as privacy, e-government and network and system security for the ambient population. Claudia holds an MSc. in Computer Science and a Ph.D. in Computers and Education.

Craig Shumard
Chief Information Security Officer,
Cigna Corporation

Craig is responsible for corporate-wide information protection at CIGNA. He received the 2005 Information Security Executive of the Year Tri-State Award and under his leadership, CIGNA was ranked first in IT Security in the 2006 Information Week 500. A recognized thought leader, he has been featured in The Wall Street Journal and InformationWeek. Previously, Craig held many positions at CIGNA including Assistant VP of International Systems and Year 2000 Audit Director. He is a graduate of Bethany College.

Andreas Wuchner, CISO, CISA, CISSP
Head IT Risk Management,
Security & Compliance,
Novartis

Andreas leads IT Risk Management, Security & Compliance right across this global corporation. He and his team control the strategic planning and effective IT risk management of Novartis' worldwide IT environment. Andreas has more than 13 years' experience managing all aspects of information technology, with extensive expertise in dynamic, demanding, large-scale environments. He participates on Gartner's Best Practice Security Council and represents Novartis on strategic executive advisory boards of numerous security organizations including Cisco and Qualys. Andreas was listed in the Premier 100 IT Leaders 2007 by ComputerWorld Magazine.

Guest Contributor

Julia Allen
Senior Researcher, CERT,
Software Engineering Institute (SEI)
Carnegie Mellon University

Julia is engaged in developing and transitioning executive outreach programs in enterprise security and governance as well as conducting research in software security and assurance. Prior to this technical assignment, she served as acting Director of the SEI as well as Deputy Director/Chief Operating Officer. Her degrees include a B. Sci. in Computer Science (University of Michigan) and an MS in Electrical Engineering (University of Southern California). She is the author of *The CERT Guide to System and Network Security Practices, Governing for Enterprise Security* and a co-author of *Software Security Engineering: A Guide for Project Managers.*

Sources for Report

- Governing for Enterprise Security; Julia Allen, Carnegie Mellon University, 2005. Available at http://www.cert.org/archive/pdf/05tn023.pdf.
- Governing for Enterprise Security Implementation Guide: Jody Westby and Julia Allen, Carnegie Mellon University, 2007. Available at http://www.cert.org/archive/pdf/07tn020.pdf.

Resources for Information Security Risk Assessments

National Institute of Standards and Technology (NIST)

- *Managing Risk from Information Systems: An Organizational Perspective*; Second Public Draft. National Institute of Standards and Technology Special Publication 800-39, April 2008. Ross, Ron; Katzke, Stu; Johnson, Arnold; Swanson, Marianne; Stoneburner, Gary. [Ross 2008] http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf.
- *Risk Management Guide for Information Technology Systems*. National Institute of Standards and Technology Special Publication 800-30, July 2002. Stoneburner, Gary; Goguen, Alice; Feringa, Alexis. [Stoneburner 2002] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

International Standards Organization (ISO)

- *ISO/IEC 27005 Information technology – Security techniques – Information security risk management.* ISO/IEC, 15 June 2008. ISO/IEC 27005:2005 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107
- *ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.* ISO/IEC, 15 October 2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103
- *ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management.* ISO/IEC, 15 June 2005. (Also known as ISO/IEC 17799.) http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

Information Security Forum. (ISF)

- *The Standard of Good Practice for Information Security* Information Security Forum [ISF 2007] https://www.isfsecuritystandard.com/SOGP07/index.htm.

Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE)

- Carnegie Mellon University, Software Engineering Institute, CERT® Program. OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation℠). [CMU] http://www.cert.org/octave.

Appendix 2. Maturity Framework: a Progression Towards an Information Risk Management (IRM) Process

Categories	Absent / Ad hoc	Initial	Effective	Integrated	Optimal
Importance of Risk/Reward Equation to Business Innovation Strategy	Tone at the top is not supportive and engagement absent or ad hoc/ event-driven. BOD and leadership do not consider assessment of information risks as relevant but rather consider security a technical IT concern	Information security is viewed as a compliance issue BOD and leadership have considered risks to information as part of enterprise risk discussions when addressing compliance IRM is not integrated into strategic decision-making processes	Information risks are regularly reviewed by BOD and leadership IRM is integrated into strategic decision-making processes CSO/CISO has full access to the BOD and leadership to discuss information risks Leadership recognizes that information security is a business issue	IRM is integrated into relevant business processes IRM is now "mainstream" and part of how business is conducted day-to-day Information risks are routinely examined as part of new business/project proposals Business leadership may still circumvent IRM processes due to limited enforcement	Corporate policy requires information risk reviews as part of the approval process for every project Information risk reviews are standardized, consistent and pervasive across the enterprise IRM is a key cultural norm reflected in performance expectations for the business
Formalization of Risk Appetite	BOD and leadership discuss risk in "localized" exchanges during closed-door meetings Communication about risk out to the organization is absent	BOD and leadership have communicated general statements of risk to their direct reports at a minimum	BOD and leadership have communicated statements of risk to the organization BOD and leadership have scenario-based risk discussions with the CSO/CISO Statement of risk are not documented	Statements and policies regarding acceptable levels of enterprise risks are documented and communicated	Scenario-based descriptions of acceptable/unacceptable information risks are documented and communicated Risk appetite is reviewed and updated on on-going basis as conditions and business strategies change
Formalization of Risk Assumption Model	Decisions about information risk are made in an ad hoc fashion, on a case-by-case basis with no consistency across the enterprise Lower levels in the hierarchy often take on inappropriate risk decisions	Leadership is starting to understand that they own the risks to information but they still do not understand the full extent of the information risks they are facing nor do they take full ownership There is no clear assignment of authority to make risk decisions based on risk magnitude	Leadership has a clear understanding that business owns all information risks There is a general understanding in the organization regarding who has what level of risk decision-making authority Most risk decisions are based on conversations in real-time Decision making guidelines are not documented	Documented risk assumption model clearly delineates who has the authority to make what level of risk decision Escalation process/dispute settlement exists but not formalized	Escalation process/dispute settlement are clearly delineated, formalized, and documented

Categories	Absent/Ad hoc	Initial	Effective	Integrated	Optimal
Formalization of Risk Roles and Responsibilities	No risk roles and responsibilities have been assigned and communicated	Leadership supports expanding the scope and role of information security to IRM Beyond this expansion, no other business leadership roles or responsibilities are assigned	Leadership has created a cross-enterprise group to assess/review enterprise risks holistically Initial efforts are often driven by Audit or Compliance CSO/CISO provides input	Enterprise Risk Committee* is established to govern risk management for all enterprise risks including information risks CSO/CISO has representation (e.g., CIO) or is a permanent member and possibly chair ERC meets regularly to review and update the enterprise risk posture	ERC's risk management plan is aligned with the organization's strategic goals
Formalization of Risk/Reward Assessment Process	Information security is treated as a technical concern within the IT department, addressed by implementing technical controls Risks to information, if considered, are discussed only by IT security function; not considered as a business issue	CSO/CISO is asked to perform risk assessments for some new initiatives but often late in the process CSO/CISO is not privy to business discussions regarding business objectives and rewards of initiatives	CSO/CISO is a member of the team evaluating new initiatives, working with the business to do risk assessments CSO/CISO is a full partner with the business and participates in discussions on business objectives and rewards of initiatives	CSO/CISO creates tools for business units to conduct their own risk assessments. Security team is called in only when risk reaches/exceeds a certain threshold (realization of self-service model) Risk assessment workflow is tracked and monitored Data collection in support of risk assessments is conducted in accordance with a defined process	Self-service model is pervasive (thorough coverage across the enterprise; used by all business units) Extensive solutions library is available to business leaders Risk assessment workflow is automated Data collection in support of risk assessments is automated

* Includes the following roles or equivalent, either as standing or rotating members based on the issues at hand: CSO/CISO, CIO, Chief Financial Officer, Chief Privacy Officer, Business Unit Leaders, General Counsel, Human Resources, and Public Relations

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

CISO RPT 0708