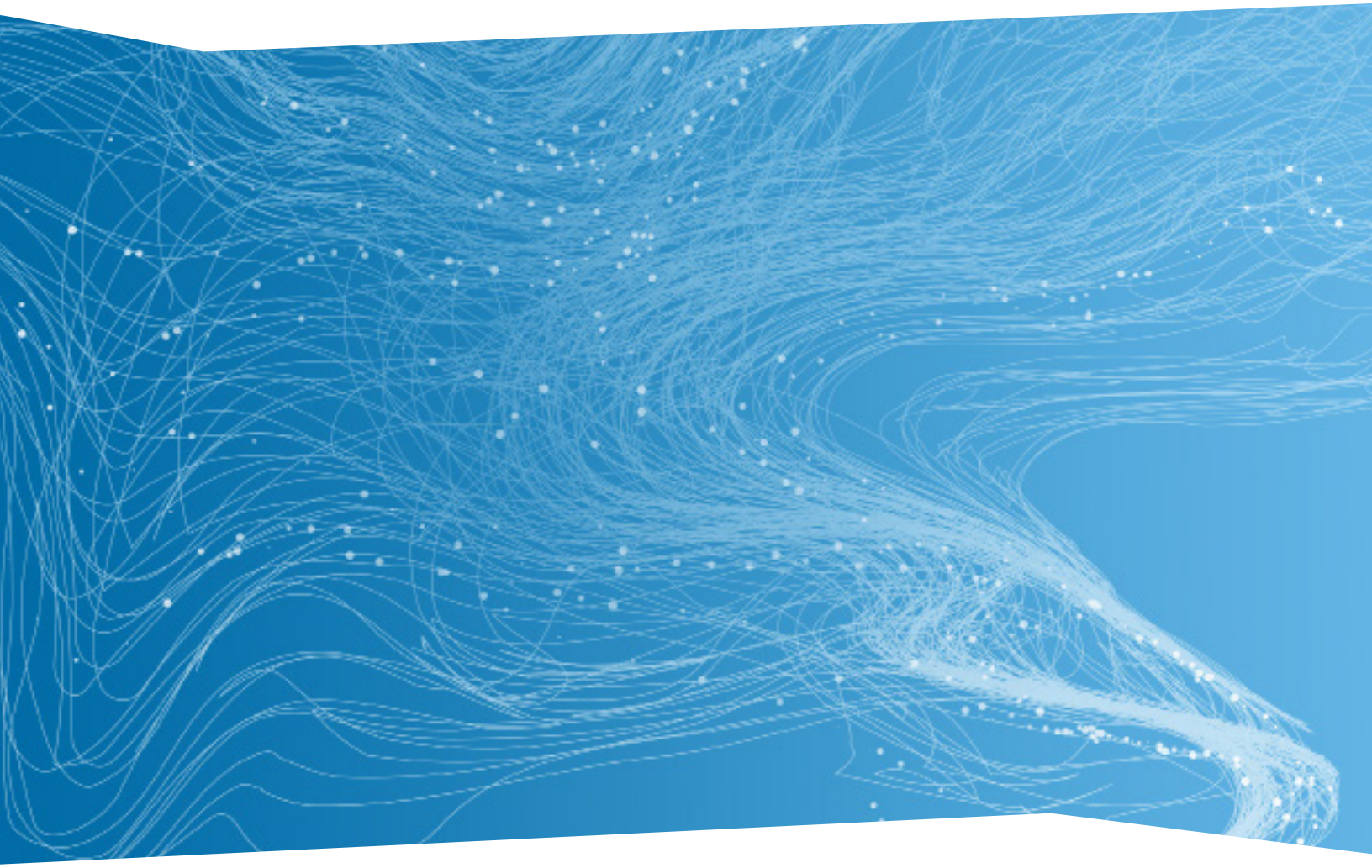
RSA



WHITEPAPER

7 STEPS TO BUILD A GRC FRAMEWORK

ALIGNING BUSINESS RISK MANAGEMENT FOR BUSINESS-DRIVEN SECURITY®

RSA

CONTENTS

Defining Business-Driven Security 3

Challenges to a Business-Driven Security Approach 3

Enabling Business-Driven Security Using Business Risk Management 4

Aligning Your Organization's Risk Appetite and Information Security 5

Conducting Information Risk Assessments 7

Establishing Your Business Risk Management Framework 8

7-Step Methodology for Business Risk Management Framework 9

- Step 1: Define What Information Needs to be Protected
- Step 2: Identify the Location and Amount of Important Information
- Step 3: Assess Inherent Risk and Evaluate its Acceptability
- Step 4: Evaluate Risk Treatments
- Step 5: Assess Residual Risk
- Step 6: Document Processes and Enterprise Risk and Controls
- Step 7: Provide Visibility and Reporting

Addressing Security Vulnerabilities and Incidents 23

RSA Solutions and Services for Business-Driven-Security 23

Summary 25

Table 1 – Inherent Risk Assessment Example 26

Table 2 –Residual Risk Assessment Example 27

Glossary of Terms 28

RSA

DEFINING BUSINESS-DRIVEN SECURITY®

Companies around the world are trying their best to manage information security, but without a holistic understanding of the risk, they are only able to address a small sliver of the problem. Security teams often purchase the latest new security gadget or system in hopes of stemming security threats, while the business risk of information security breaches continues to increase for the organization. Despite these security investments, organizations still find it difficult to put security details in the necessary business context to make the right investments in information security, or to react appropriately when information security vulnerabilities and incidents are identified.

Business-Driven Security® is an approach to understanding, managing, and depicting information security risk into the context, terms, and manner that are most efficiently and effectively utilized by the organization's business leaders, executive management, and board of directors. Understanding and communicating information security in terms of its impact to the overall business leads to better business decisions and more efficient allocation of human and capital resources to manage information security.

This fusion of information security insights with business context is critical in helping organizations know where to make strategic information security investments. It creates an explicit linkage between what the security technology indicates, and what that means in terms of risk to your business. It enables organizations of all sizes to take command of their evolving security posture in this uncertain, high-risk world, to reduce risk and ensure protection of what matters most.

CHALLENGES TO A BUSINESS-DRIVEN SECURITY APPROACH

A recent Ponemon Institute survey of executives found that 59 percent are concerned with their organization's ability to stay operational following a data breach involving high-value information assets, such as trade secrets and confidential corporate information. However, 53 percent indicated their senior management's greater concern is a breach involving credit card information or Social Security numbers.

While these executives understand the data they control could have significant impact if it were subjected to unauthorized access, alteration, or destruction, they are not prioritizing this information consistently. Moreover, they likely do not know where their organization's most critical information resides, which leads to misallocation of people, processes, and technologies to manage information security. Embracing a Business-Driven Security strategy enables senior managers to align key business priorities with security information, to ensure properly prioritized response in the event of a security crisis.

A business-driven approach to information security enables your organization's management team and board to answers questions such as:

- What information is important to our organization?
- Where is this information handled, stored, processed, transmitted, and archived?
- In the absence of controls and risk transfer, what is the likelihood that this important information can be stolen, altered, destroyed, or inaccessible for a period of time? And what is the impact to our organization?
- Are these risks of enough significance to warrant devoting human and capital resources to mitigate and transfer the risk?
- Where significant risks have been identified, are the committed human and capital resources adequate to effectively mitigate and transfer the risks?
- Where information security vulnerabilities and weaknesses have been identified, are resources being devoted to remediation on a prioritized basis, relative to the business risk presented to our organization?
- If an incident occurs, how bad could things get?

ENABLING BUSINESS-DRIVEN SECURITY WITH BUSINESS RISK MANAGEMENT

It is the fiduciary obligation of senior management and the board of directors to ensure that management of information security risk is consistent with the risk appetite of the organization in order to adhere to strategies and meet objectives. While organizations do not have enough resources to entirely eliminate risk, applying a Business-Driven Security approach enables organizations to more intelligently allocate limited resources to the biggest information security risks.

No organization can achieve its objectives without taking risks but the risk-taking must be well understood and managed to ensure that it is appropriate to achieve the organization's objectives without jeopardizing the organization's existence. Organizations can optimize this balance by embracing business risk management — applying governance, risk and compliance (GRC) concepts and best practices and implementing a framework — to collect and organize information that is relevant for management of information security risk. Business risk management makes GRC actionable, enabling organizations to improve business performance through reduced risk and more informed decision making. Organizations can define and enforce accountability for risk and compliance issues, and drive efficiencies by automating processes. It also provides collaboration on risk issues across business lines and organizational boundaries and improves visibility by consolidating data and enabling risk analytics across the organization.

Business-Driven Security relies on the implementation of a framework for collecting and organizing information relevant to information risk management. A business risk management framework is a catalog of the organizational elements and their interrelationships that are necessary to ensure the success of the organization meeting its objectives and managing its risk and compliance obligations. These elements include strategies and objectives, products and services, policies and procedures, authoritative (regulatory) sources, business processes and sub-processes, third parties, and IT infrastructure elements (web services, IT software applications, IT systems, databases, and data stores both inside and outside of the cloud), and risks and controls.

ALIGNING YOUR ORGANIZATION'S RISK APPETITE FOR INFORMATION SECURITY

No organization can achieve its objectives without taking risks. Your organization's "risk appetite" defines the maximum amount of risk your organization is willing to take to achieve strategic business objectives. Deciding the types and amounts of risk to take and managing risk within those constraints is essential to increasing the likelihood that your organization will meet its objectives. In effect, your organization's risk appetite sets the parameters for prioritizing which risks need to be addressed and treated.

Within the organization's overall risk appetite, "cyber risk appetite" defines the maximum amount of loss or harm an organization is willing to take related to its technical infrastructure or use of technology. By broad definition, cyber risk appetite also includes "information risk appetite," the maximum amount of loss, destruction, alteration, or unauthorized disclosure of the organization's information or the information it maintains for customers, partners, and counterparties.

CYBER RISK APPETITE DEFINES THE MAXIMUM AMOUNT OF LOSS OR HARM AN ORGANIZATION IS WILLING TO TAKE RELATED TO ITS TECHNICAL INFRASTRUCTURE OR USE OF TECHNOLOGY.

Questions to consider when setting your organization's information risk appetite include:

- What type of information does our organization maintain about itself and others? What information is most important?
- How much and what type of information could our organization "afford" to lose or have stolen, altered, destroyed, or made inaccessible?

- At what magnitude would information that is lost, stolen, altered, destroyed, or inaccessible result in unacceptable publicity?
- At what magnitude of information loss, theft, alteration, destruction, or inaccessibility would our organization experience significant costs, including recovery, compensation, litigation, and regulatory fines and sanctions?

An information risk appetite acknowledges the reality of today's information security threats, establishing a pragmatic threshold to which risk should be managed. While the natural tendency of organizations is to say they do not want any information to be lost, stolen, altered, destroyed, or inaccessible, no organization has the time or money necessary to protect 100 percent of their information with 100 percent certainty at all times.

Calculating information risk through ongoing assessments using defined and proven methodologies, as well as both quantitative metrics and qualitative risk elements, is critical in determining how much risk your organization is willing to accept to achieve specific business goals or objectives. Determining your organization's information risk appetite cannot be a point-in-time exercise; it must be an ongoing process, involving constant evaluation and re-evaluation.

Organizations often also establish "risk tolerance" thresholds. These are almost always less than the related risk appetite and represent the level of risk the organization is willing to take on a day-to-day or transaction-by-transaction basis (Figure 1).

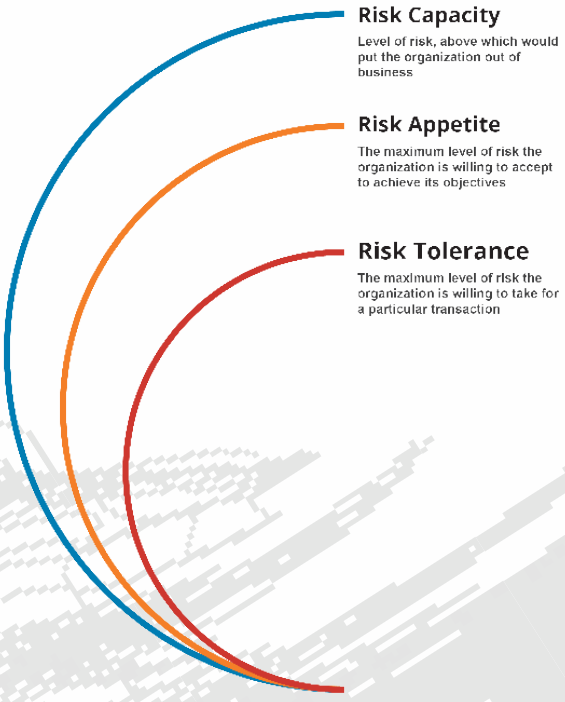


Figure 1 – Risk Taking Thresholds

Information risk appetite should be set by the CEO, CISO (Chief Information Security Officer), CLO (Chief Legal Officer), and CRO (Chief Risk Officer), codified by the board of directors as applicable, and shared throughout the organization to establish day-to-day operating risk tolerances. Information risk appetite is not a strictly technical issue; rather, it ties together operational risk, information risk, and enterprise risk, and requires conversation across technical and non-technical functions. The strategic conversation is about the risk the organization is willing to take on and what priority should be placed on information risk management. Defining and communicating risk appetite is critical in helping your organization know where to invest time and resources for the greatest impact.

CONDUCTING INFORMATION RISK ASSESSMENTS

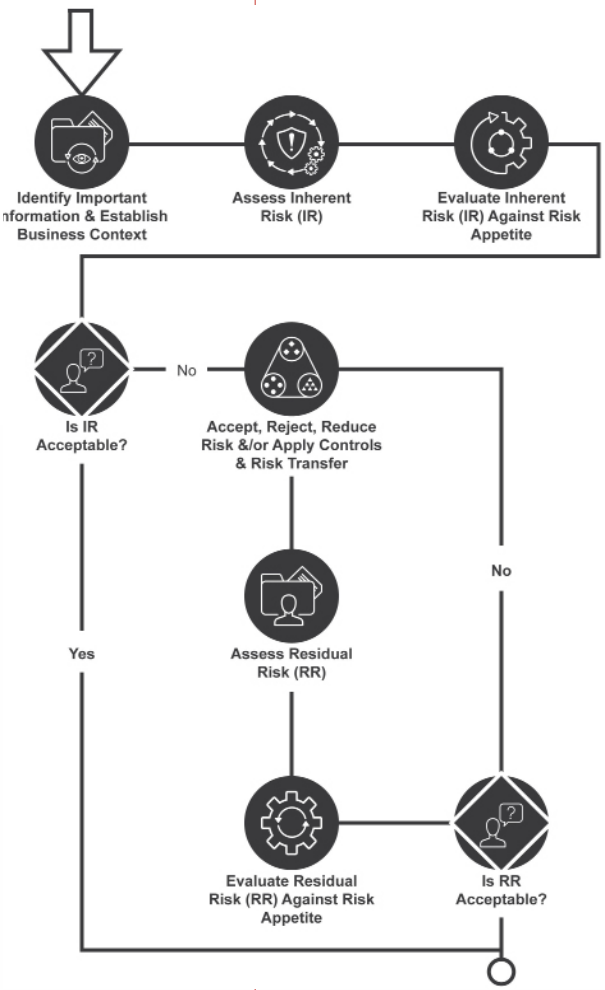


Figure 2 - Risk Assessment Approach

In keeping with the guidelines provided in ISO 31000-2009 Risk Management – Principles and Guidelines, and NIST 800-30 rev. 1, Guide for Conducting Risk Assessments, a basic approach to risk assessments (Figure 2) begins with identifying information owned or managed by the organization and determining what information is important.

Once this business context has been established, you must assess the information's inherent risk. The "inherent risk" assessment is the process of estimating the worst-case likelihood and impact of threats to the information being lost, stolen, altered, destroyed, or inaccessible as the result of malicious or unintentional acts originating internally or external to the organization, including man-made and natural disasters.

Next, inherent risk is evaluated against the level of risk the organization is willing to take. If inherent risk exceeds risk tolerance, the organization may choose to reduce the amount of information at risk, accept the risk, or apply risk treatments, which may include implementing information security technologies, manual controls, and risk transfer (cyber insurance) to lower the risk.

After these risk decisions are complete and risk treatments have been applied and are operating, risk is assessed on a residual basis. Residual risk to the organization of an information asset being stolen, altered, destroyed, or made inaccessible is, in essence, the worst case risk to the organization (i.e. inherent risk) modified by the design and operating effectiveness of each risk treatment to lower the likelihood and/or impact of the threat to the information asset. Practically speaking, residual risk can never be greater than inherent risk, nor can residual risk be reduced to zero since no set of controls are ever 100 percent effective.

Once residual risk is calculated, it is again compared with the organization's risk appetite. If the risk is still too high, more risk treatments should be applied, the activity reduced, and/or the risk accepted. Risks that are to be accepted should be cataloged and routed for approval by managers within their delegated authority to accept risk. If the risk being accepted is deemed significant enough, it should be accepted by the board of directors. These risk acceptance decisions are revisited on a periodic basis to ensure they still align with the organization's risk tolerance and appetite.

To perform meaningful and consistent risk assessments, organizations must agree on risk management-related terminology and practices, including:

- How assessments will be performed
- The definitions of inherent and residual risk
- Risk scoring and risk rating scales that will be used to depict risk

Organizations with established enterprise risk management or operational risk management functions are well advised to align these approaches with their information risk management programs. This makes it easier to roll up different kinds of risk in a comparable fashion.

ESTABLISHING YOUR BUSINESS RISK MANAGEMENT FRAMEWORK

A "business risk management framework" is a catalog of organizational elements and their interrelationships that are necessary to ensure the success of the organization in meeting its objectives and managing its risk and compliance obligations. These elements include strategies and objectives, products and services, policies and procedures, authoritative (regulatory) sources, business processes and sub-processes, third parties, and IT infrastructure elements (web services, IT software applications, IT systems, databases, and data stores), and risks and controls.

A business risk management framework for Business-Driven Security provides senior management and the board with critical insight regarding:

- What information is important to our organization
- Where this important information is handled, stored, processed, transmitted, and archived
- What the inherent risk is to our organization if this important information is lost, stolen, altered, destroyed, or inaccessible for a period of time
- Whether inherent risks are significant enough to devote human and capital resources to mitigate and transfer
- Where significant risks have been identified, whether the committed human and capital resources are adequate to effectively mitigate and transfer the risks
- How much needs to be spent to lower risk within our organization's risk appetite
- Where the gaps are in our control environment, why they are important, who is responsible for correcting them, and when they will be corrected
- If an information security incident occurs, what infrastructure elements could be involved and what the impact to the organization could be
- Whether we should buy cyber insurance, which risks should be covered, and how much we should buy
- Whether we are in compliance with our regulatory obligations around information security

7-STEP METHODOLOGY FOR A BUSINESS RISK MANAGEMENT FRAMEWORK

Based on best practices and industry standards, this seven-step methodology provides organizations with the business risk management framework necessary for Business-Driven Security.

STEP 1: DEFINE WHAT INFORMATION NEEDS TO BE PROTECTED

The organization's first step in establishing a Business-Driven Security approach to risk managements determining whether the organization handles information that needs to be protected. This determination could be done with a quick assessment. Typically, an organization documents and evaluates its strategies and objectives, the products and services being delivered (or planned to be delivered), and the regulatory obligations the organization is subject to across the jurisdictions where it does business.

Elements that should be captured to identify potentially important information that may be deemed important to protect include organizational structure and business jurisdictions, strategies and objectives, product and services, policies and procedures, and regulatory obligations (Figure 3).

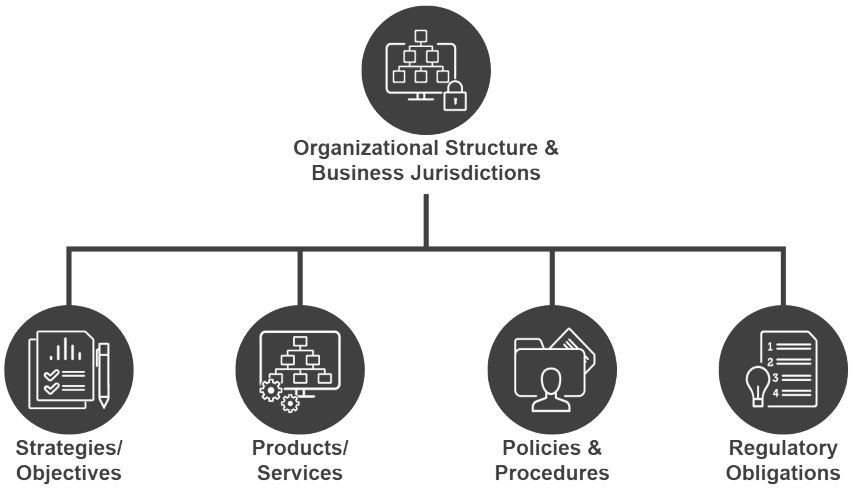


Figure 3 – Identifying information that may be important to your organization

These interconnected relationships illuminate the following business context:

- Strategies and objectives typically span the organization, rather than residing within one area of the business. Products and services are delivered relative to strategies and objectives, and how they are delivered varies by division, business unit, and jurisdiction.
- Strategies and objectives are often enabled or constrained through a myriad of policies, regulatory obligations, and covenants within the various jurisdictions where the organization does business.
- Products and services are often delivered only within constraints of policies and procedures and regulatory obligations. One need look no further than the Food and Drug Administration (FDA), consumer banking laws, HIPAA (Health Insurance Portability and Accountability Act), GLBA (Gramm-Leach-Bliley Act), PCI (Payment Card Industry), and the EU-GDPR (General Data Protection Regulation) to appreciate the requirements for bringing products to market and maintaining them in the market over the long run, without incurring material fines or sanctions or inviting litigation.

Having cataloged and depicted the interrelationship of strategies, objectives, products and services, policies and procedures, regulatory obligations, and organizational structure, the organization is now in a position to answer the following:

- Are any strategies or objectives being pursued that, if publicly disclosed or acquired by competitors or others, would impair our organization's ability to achieve strategies and objectives? This includes information that may put persons at risk of physical or financial harm, or information about strategic plans related to market strategy, customers, geographies, mergers, acquisitions, new product development, etc.

- Does our organization offer any products or services that require the collection, processing, and/or storage of information that, if publicly disclosed, accessed by unauthorized persons, lost, altered, destroyed, or inaccessible, would impair our organization's ability to achieve our strategies and objectives? Examples include collection of personal, healthcare, and credit card information from customers.
- Do any products that we offer rely on proprietary information or intellectual property that, if publicly disclosed or acquired by competitors, would impair our ability to achieve our strategies and objectives? Examples include computer software source code, "secret formulas," and designs for product manufacturing.
- What policies and procedures does our organization have in place related to classification, collection, and handling of information? The intersection of information-related policies and procedures with the organization's strategies, objectives, and products and services helps to determine what information is important to protect.
- What laws and regulations is our organization subject to, related to the collection and handling of information? The intersection of this regulated information with the organization's strategies, objectives, and products and services helps to further illuminate information what is important to protect. Examples include HIPPA, GLBA, and EU-GDPR regulations, which call out specific types of information that must be protected.

At this stage of the evaluation, the organization does not know if it actually has any of this information that needs to be protected. However, if the information does exist, it is important enough to be protected by the organization in some manner. In this analysis of business strategy, products and services, and regulatory obligations, "important information" is cataloged, along with why the information is important, the internal owner of the information, and what the information relates to, through cross-references to the business elements to which it is related (Figure 4). Visually depicting interconnections provides meaningful business context as to why the information is important.

ROLE OF POLICIES, PROCEDURES, AND STANDARDS IN BUSINESS-DRIVEN SECURITY

Step 1 in the Methodology for Risk Assessments, "Define information that needs to be protected," is the documentation and use of policies and procedures and regulatory obligations to help identify important information that should be secured.

Organizations must not overlook regulations, policies and procedures, and

standards as key considerations in their business-driven security strategy. By incorporating these elements, organizations can better ensure compliance with management expectations, regulatory obligations, and best practice control standards in day-to-day operations. They will also be in a better position to demonstrate how well the organization complies with policies, procedures, and regulations, where they are out of compliance, what is being doing to regain compliance, and when compliance is expected to be restored. Lastly, organizations can more efficiently demonstrate compliance, which is difficult with a haphazard approach to control testing.

A typical integration of IT security-related policies and procedures, regulations, and standards with controls procedures, and the resulting findings, is depicted below. (Figure 3.1)

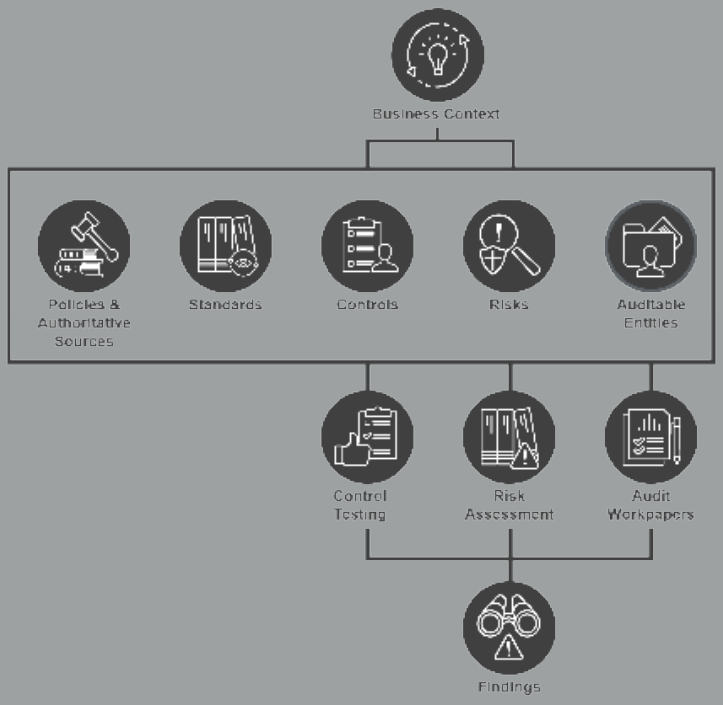


Figure 3.1 – Typical integration of regulations, policies and procedures, standards, and control procedures

This structure allows multiple overlapping regulations to be normalized with policies through common control standards. By relating control standards with control procedures, organizations can demonstrate compliance with multiple policies and regulations using minimum controls. This highly efficient approach supports “test once, satisfy many.”

While this is the most common approach for integrating policies and procedures and regulations within a business-driven security strategy, there are other integrations to consider. (Figure 3.2)

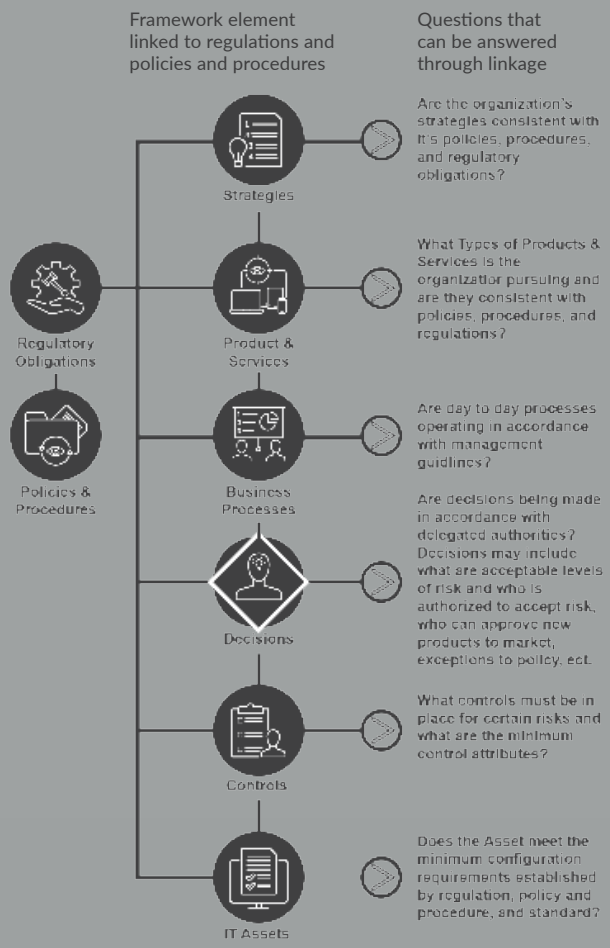


Figure 3.2 – Business-driven security, regulations, and policies and procedures

By integrating regulations, policies, and procedures with the business-driven security framework, organizations can more effectively answer these questions:

- Are we operating in accordance with policies, procedures, and regulatory obligations?
- Which business processes and assets are operating inconsistently with policies, procedures, and regulations?
- How much risk is being introduced to the organization by policies, procedures, and regulations that are not being followed?
- How are findings and exceptions to regulations, policies, and procedures being managed?
- Who is responsible for managing findings and exceptions, and when will the exceptions be remediated?

STEP 2: IDENTIFY THE LOCATION AND AMOUNT OF IMPORTANT INFORMATION

Once important information has been identified and documented, the next step is to locate where this information exists within the organization. To make informed decisions about where to invest information security resources, it is necessary to more concretely determine where this information is stored, processed, and transmitted and to validate that there is no other important information that needs to be protected.

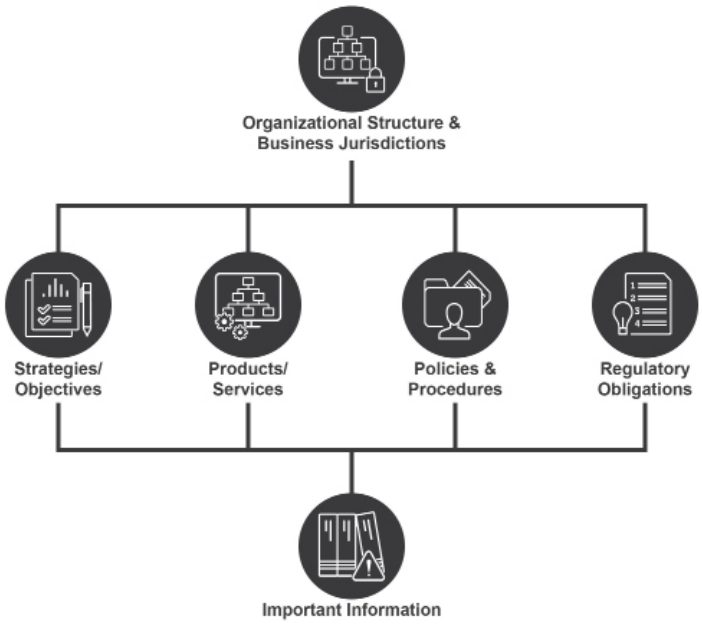


Figure 4 – Documentation of important information

Step 2 is identifying where and how much important information resides in the organization. Since important information may reside in physical or electronic form, it is necessary to identify both formats.

Fulfillment of strategies and objectives, delivery of products and services, and compliance with regulatory obligations are accomplished through a plethora of business processes. Business processes are a collection of related tasks organized for the purpose of keeping the organization running, delivering products and services, fulfilling a strategy or objective, maintaining compliance, etc. Business processes may be represented in their totality or as a group of interrelated sub-processes to facilitate clarity.

To identify where important information is handled within the organization, it is first necessary to identify the business processes that involve handling important information or could introduce problems in the management of important information. Examples of processes include the administration of security (physical and electronic access, firewall administration, etc.), introduction of a new product and service, or implementation of new IT hardware and software. Business processes are documented, as are the specific types and amounts of information that are related to the process and the individuals responsible for the operation and management of the process.

Once important information-related business processes are documented, supporting IT and third party relationships are documented and related to the business processes they support. Understanding this information and its relationships is essential to understanding the business context of information security, performing risk assessments, and ensuring the organization's resilience to business interruption.

By understanding public-facing services, which software applications support these services, which servers and other systems support the software applications, where and how the information is stored and transmitted, and with which third parties information is shared, the organization is in a better position to understand the magnitude of importance of information involved with any given threat or incident.

Each of the business risk management framework elements highlighted (Figure 5) is documented, including the name of element record, the individual and business unit that "own" the business process, the third party, and the IT infrastructure element, as well as the types and amounts of electronic and physical information associated with each element. This information will be critical in Step 3 in assessing the inherent risk of each business risk management framework element.

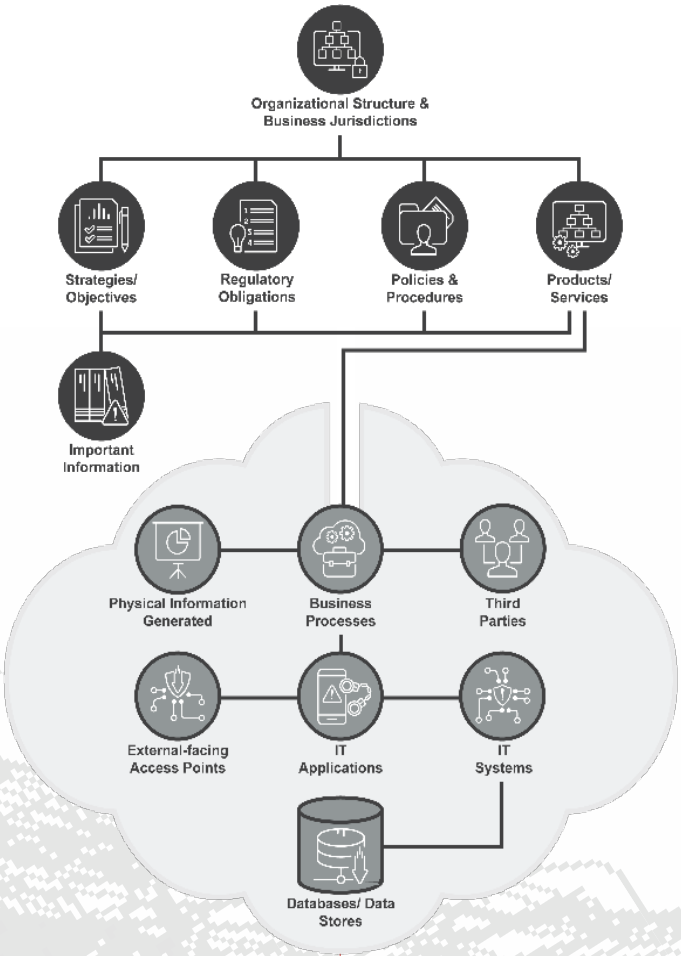


Figure 5– Identifying location and amount of important information

Two complementary approaches are typically implemented to collect this information:

- Questionnaires and forms manually collect information from the "owners" of each process, third party, and IT infrastructure element.
- Automated tools identify the IT infrastructure and the type and amount of data either residing on or being processed through each element. Utilizing automated tools to identify where and how much important information resides on IT infrastructure elements is an efficient means to capture this information and assists in generating a more up-to-date risk profile.

Comprehensive information security management encompasses more than electronic information. During this step, the organization must also identify whether important information is maintained in physical form.

The type and amount of information associated with each business risk management framework element is recorded for each business risk management framework element record. Recording this information provides greater business context about the purpose, scope, and magnitude of each business risk management framework element. It can be easily queried and analyzed for many purposes, including information security risk assessments, business continuity planning, and internal, external, and regulatory examinations. The ability to use the same pool of information for multiple purposes provides efficiencies, as it takes less capital and human resources to collect and manage it collectively.

By the end of Step 2, the following has been identified:

- Business processes, IT assets, and third party relationships involved in handling important information
- Types, formats, and volume of important information being handled
- How our organization's IT infrastructure and third party relationships support the delivery of business processes, products and services, and strategic objectives
- Where information that is subject to regulatory guidance and oversight resides
- The parties responsible for this information

STEP 3: ASSESS INHERENT RISK AND EVALUATE ITS ACCEPTABILITY

In Step 3, the inherent risk of information security is computed around each business process, third party, and IT infrastructure element. Inherent risk is the risk to the organization in the absence of any risk treatments, and it is typically considered to be worst case risk. With respect to information security risk assessments, the type and amount of important information processed, stored, or transmitted is used to assess the inherent risk of unauthorized access, alteration, interruption, or destruction of the information. It is important to look at information risk on an inherent risk basis to understand where the most significant risks exist on a worst case basis. This generates more meaningful conversations around "what if" this information were to be accessed, altered, destroyed, or inaccessible and whether the organization is doing enough to manage the risk.

In its most basic form, inherent risk is estimated assuming there are no risk treatments (controls or risk transfer) in place, and may be calculated as:

Inherent Risk = (Criticality of Information x Number of Records)

x Impact per Record Associated with each Type of Threat

There are numerous ways to assess risk. Organizations frequently revise their assessment methods as best practices and regulatory obligations change, additional information becomes available, and / or resources and assessor skills grow. For many organizations that are just starting out with limited resources, it may be acceptable to have a subject matter expert or infrastructure element owner rate the element qualitatively as "high," "medium," or "low." A more robust approach uses information collected about each framework element to automatically score the criticality of the information and calculate the risk to the organization should a breach, alteration, interruption, or destruction of the information occur (Table 1, Inherent Risk Assessment Example).

If the organization wants to estimate the monetary impact associated with a breach, alteration, interruption, or destruction of information, monetary values can easily be added to the calculation. Some organizations may also apply Monte Carlo simulation to estimate risk.

Regardless of the approach, there is a need to depict the inherent risk assessment in a format that is consistent both with other risk management programs operating within the organization and how risk is communicated to senior leadership and the board of directors. Often, this means visually depicting risk on a basic five-point scale using heat maps or other visual aids. The process of translating granular risk assessments to an organization-wide set rating scale is referred to as "calibration."

If risk is assessed using monetary values, it is straightforward to use this example rating scale (Figure 6):

Rating	Risk	Color
Critical	> $5,000,000	
High	$4,000,000 - $4,999,999	
Medium	$3,000,000 – $3,999,999	
Medium-Low	$2,000,000 - $2,999,999	
Low	< $2,000,0000	

Figure 6 – Risk rating scale example

With this rating scale, an IT system breach that could result in more than $5 million in losses to the organization would be rated critical and color-coded red.

However, risk cannot always be easily rated in monetary terms. Risks arise across multiple risk categories. A breach may pose operational risk to an organization as the result of theft, customer reimbursements, credit monitoring, additional costs of managing an incident, litigation, and regulatory fines and sanctions. Information security breaches often introduce unquantifiable risk. A story about a breach in the local newspaper would likely present much less reputational risk for an organization than if the breach were reported by *The Wall Street Journal*. Consequently, it is necessary for organizations to create rating scales that blend both monetary and qualitative considerations.

To ensure the integrity of the risk assessment process and Business-Driven Security management, it is critical that the stakeholders within the organization agree upon and internally publish their rating scales so that all parties can easily understand the approach and what is being communicated in the risk assessment. The organization's risk ratings scale should reflect risk in business terms the organization understands.

Once inherent risk assessment calculations are complete and calibrated to the organization's risk rating scale, the results may be displayed as the number of business risk management framework elements by inherent risk level (Figure 7).

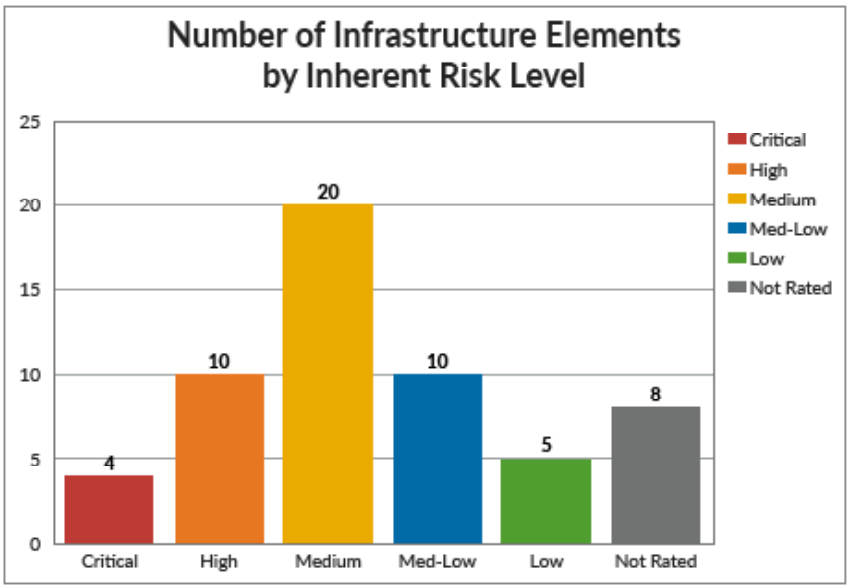


Figure 7 – Inherent risk by infrastructure element

Easily understood by business leaders, this graph indicates there are four infrastructure elements that pose critical inherent information security risk. The organization can drill into each of the bars on this graph to understand the business context, the affected infrastructure elements posing the risk, the type and amount of information at risk, and why the element received its rating. Figure 7 shows there are four infrastructure elements with high ratings for critical inherent risk. Assuming the organization's definition of "critical" equates to material risk, a significant compromise of any one of these four critical elements would materially impact the organization.

Typically, infrastructure elements that pose higher inherent information risk would be the first to be addressed. The process of allocating risk treatments based on information at risk promotes efficient resource allocation and reduces the likelihood of spending resources over controlling lower risk elements.

Figure 7 also indicates there are eight infrastructure elements that have not yet been assessed; they are "Not Rated." This is also actionable information, telling management there may be other material information risk that needs to be addressed. This depiction provides a means to manage these omissions to completion by establishing explicit accountability, tasks, due dates, and management escalation.

By the end of Step 3, organizations know:

- Which processes, third parties, and IT infrastructure pose the greatest risk to the organization if the information were breached, altered, or inaccessible
- Which processes, third parties, and IT infrastructure warrant the most attention from management and the board
- Where the organization should be spending its limited human and capital resources to control information risk
- If an information security incident were to occur around any process, third party, and/or IT infrastructure element, what the worst case impact to the organization would be, as well as what the interconnections between elements known to have been breached and those that could still be breached through those interconnections

STEP 4: EVALUATE RISK TREATMENTS

In Step 4, the inherent business risk associated with information security is compared with the organization's information risk tolerance and appetite. Risk that exceeds the organization's information risk tolerance is addressed by reducing the activity that generated the risk, accepting the risk, reducing the risk with controls, transferring the risk (such as with cyber insurance), or a combination of these. Most organizations choose to reduce risk by applying manual and automated controls.

In this step, the organization needs to document controls mitigating risk, assess the design and effectiveness of the controls, create and manage remediation plans where controls have failed or are missing, and compute the remaining risk (residual risk) considering those controls and other risk treatments in place.

For IT infrastructure elements, questionnaires can be launched to IT infrastructure element owners to complete manually, and/or the results of automated vulnerability assessment tools can be utilized. Control questions being assessed may include:

- Is information encrypted?
- Are patches current and are they applied within a reasonable period of time from their release date?
- Have default passwords been changed?
- Are passwords required to be changed on a regular basis?
- Do all passwords conform to the organization's construction requirements of length, character mix, or use of multifactor authentication tokens?
- Is the system designed to prevent SQL injection attacks?

- Are logs reviewed daily to identify anomalous activity?
- Have individuals been adequately trained and are they qualified to manage the specific IT infrastructure asset to which they have been assigned?
- Have security vulnerabilities been evaluated, tested for, and remediated prior to placing new products and program changes into production?
- Do third parties handling important information have well designed security and resiliency controls in place and are they operating?

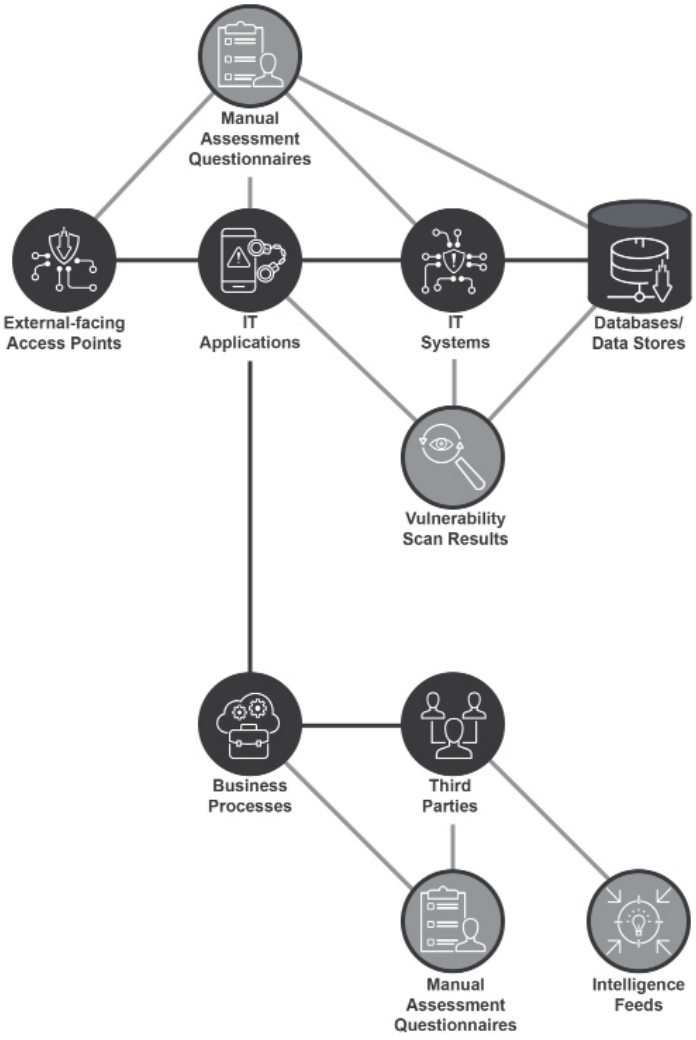


Figure 8 – Control Assessment

These types of questions should be configured into questionnaires unique to each type of element, which are automatically generated and distributed to the Business Risk Management framework element owners. Questions can typically be drawn from pre-established control libraries associated with the organization's policies and procedures, as well as regulatory obligations, as applicable. The response to each question should be weighted and scored, then factored into the residual risk assessment, with exceptions automatically logged for monitoring and management remediation.

The results of manual assessments and automated assessment feeds are applied in evaluating the design and operation of controls to mitigate the risk of unauthorized access, alteration, interruption, or destruction of the organization's important information (Figure 8).

By the end of Step 4, the following is understood:

- What controls are in place to mitigate risk to each Business Risk Management framework element involved with the organization's important information
- Where controls have not been evaluated within required timeframes
- Which controls have been found to be missing or not operating
- What the inherent risk is of those business risk management framework elements that have missing controls or non-operational controls

- What is being done to address control deficiencies, who is responsible for addressing control gaps, and by what date the gaps will be addressed

STEP 5: ASSESS RESIDUAL RISK

By Step 5, the organization knows where controls exist to mitigate the risk to important information associated with each business risk management framework element and whether controls are in place and operating to mitigate risk. With this information, plus the inherent risk assessment results, the organization can assess the residual information risk of each business risk management framework element.

One approach often used to assess residual risk is to start with each infrastructure element's inherent risk and reduce it by an estimate of how effective each control is in reducing the inherent risk. Using this approach, residual risk is calculated as:

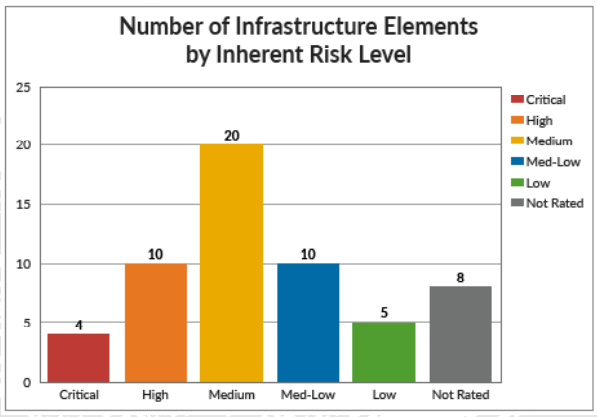
Residual Risk = Inherent Risk x Risk Reduction percentage of all applied and operating Risk Treatments

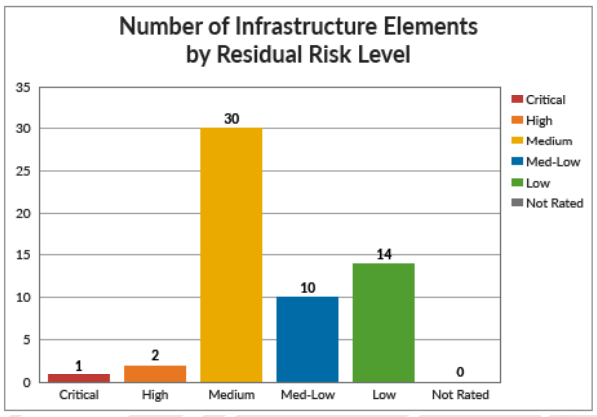
Since controls are never 100 percent effective, residual risk should never be zero. Table 2 – Residual Risk Assessment Example provides some examples of the calculation of residual risk by IT GRC infrastructure element.

At the end of the residual risk assessment process, the organization is in a position to see, side by side, the IT GRC Infrastructure Elements by Inherent Risk level and Residual Risk Level. In the example (Figure 9), the number of critically risky GRC infrastructure elements has declined from four to one, and the high risk elements have declined from ten to two. Furthermore, there are no remaining unassessed (not rated) elements.

Figure 9 – Inherent versus residual risk example

With this information, the organization is again faced with the question of





what to do with those elements that have a residual risk level that exceeds their information security risk tolerance and appetite. This information provides the organization with a clear understanding of what elements are too high in risk and what is causing the risk to be too high. The organization now has the information it needs to make decisions about allocations for people, processes, and technology to lower the residual risk to acceptable levels, or to exit the business activity that introduces unacceptable risk.

STEP 6: DOCUMENT PROCESSES AND ENTERPRISE RISKS AND CONTROLS

Certain other business activities unrelated to existing third parties and IT infrastructure can introduce material risk to unauthorized information access, alteration, and availability. These activities include:

- Physical access to important information or to the IT processing environment
- Hiring, developing, and retaining sufficient qualified human resources
- Employee information handling and security awareness
- Contingency planning, business continuity and disaster recovery preparedness
- Incident management
- Software and system development lifecycle and change control
- New product development
- Business process change
- Regulatory change
- Mergers and acquisitions

It is important to understand and manage these activities in a manner that keeps potential information security risk at an acceptable level. This is accomplished by documenting the activities as business processes, documenting the risks associated with the processes, and documenting each of the controls mitigating the identified risks. (Figure 10). Risks are assessed in the risk register on an inherent and residual basis using the same rating scales used to evaluate the other business risk management framework elements. Risks may be assessed using a top-down approach and/or through self-assessments completed by business unit managers that are responsible for the risks and controls.

Figure 10 – Business process risks and controls

The design and operating effectiveness of controls in the control register can be validated through management assertions and tests, or through tests completed by the compliance team or the "third line of defense" (i.e. independent internal or external auditors). The result is the production of a dynamic risk register that depicts each business process risk and its calculated residual risk.

STEP 7: PROVIDE VISIBILITY AND REPORTING

Visibility and reporting is key to a successful business-driven security framework. Analytics that provide timely information depicted through visual dashboards are critical for business leaders to gain visibility based on the most accurate and complete information in real time. Exceptional transparency into the risk profile of the organization can be obtained utilizing GRC process workflows, notifications, and reporting, to engage individual accountability for the management of Business Risk Management framework elements, risk and control assessments, and exceptions and remediation commitments.

ADDRESSING SECURITY VULNERABILITIES AND INCIDENTS

All organization's today routinely identify security vulnerabilities and experience periodic information security incidents. Often, the volume of vulnerabilities and incidents can overwhelm an organization's available resources to remediate vulnerabilities and address incidents in a timely manner.

Business-Driven Security allows organizations to apply the same risk identification and assessment strategies to prioritization of vulnerability remediation and incident handling. There is no longer a need to immediately address and research every vulnerability and incident on every system to the nth degree. Rather, the organization can prioritize remediation based on an understanding of the business context of the affected infrastructure element and its associated inherent risk (worst case) outcome.

RSA

RSA SOLUTIONS AND SERVICES FOR BUSINESS-DRIVEN SECURITY

RSA solutions and services uniquely link business context with security, enabling organizations to reduce risk and ensure they are protecting what matters most.

At their core, RSA solutions are based on two complementary building blocks. Security exclusion keeps the bad guys out, using detection and response. Security inclusion lets the good guys in, which is driven by identity and access assurance. Common analytics are designed to detect anomalies – deviations from the norm that may be indications of malicious activity – on the network, endpoints, or patterns of user behavior. Orchestration and automation then turn these insights into actionable items, ad facilitate remediation that is repeatable and scalable. Contextual intelligence rolls up to the organization's risk portfolio, providing critical insights to the impacts of IT and cyber risk to the business.

The **RSA Archer® Suite** enables you to take command of risk, including new sources of cyber risk that continue to emerge. It includes multi-disciplinary risk management solutions and use cases that address the most critical domains of business risk. RSA Archer is designed to help you evolve your risk management program as your business changes, and integrates with the RSA product portfolio to address threat detection and response and identity.

The **RSA NetWitness® Suite** provides visibility to detect advanced threats and deliver the right response in minutes, not months. Based on information maintained in RSA Archer, organizations can understand the business context and significance of identified threats. Organizations can prioritize threat response based on risk and integrate threat detection results in RSA Archer to understand the effect on the organization's cyber risk profile.

The **RSA SecurID® Suite** reimagines identity strategy for the modern enterprise, and enables the business to get more done. RSA Identity Governance and Lifecycle provides identity and access management around important information. Utilizing the RSA Archer Suite, organizations can document important information and make informed decisions about where identity and access management should be established to prevent unauthorized access. The RSA SecurID Access and RSA Identity Governance Suites maintain access security on an ongoing basis and provide the tools needed to efficiently provision access as internal and extended workforce and partner networks change.

The **RSA® Fraud & Risk Intelligence Suite** exposes cybercriminals to help organizations protect customers. RSA Fraud Prevention is designed to identify high-risk logins, protect e-commerce transactions, and obtain and manage

fraud intelligence. Organization can correlate fraud intelligence to assets documented in RSA Archer, enabling adjustments to the information security risk profile based on the relationship of intelligence to documented controls.

The **RSA® Risk & Cyber Security Practice** provides essential expertise to enable organizations to take command of evolving risk and security.

SUMMARY

Business-driven security is an approach to information security risk management that focuses on understanding and managing information security risk in terms that can be generally understood by an organization's business leaders and board of directors. It is depicted in a manner that can be compared with the organization's other risks, regardless of their type or source. Understanding and communicating information security in business terms leads to better business decisions and more efficient allocation of human and capital resources across the organization.

Business-driven security solutions and services uniquely link business context with security incidents, enabling your organization to reduce risk and ensure protection of what matters most to your organization.

TABLE 1 – INHERENT RISK ASSESSMENT EXAMPLE

Notes:	A	B	C	D	E	F	G	H	I	J
Row	Important Info	Element Assessed	Threat (Theft, Alteration, Destruction	Info Criticality (1 Low to 5 High)	Information Format	# of Records at Risk	Systemic Information Risk	Calibrated Inherent Risk Level	Threat Scenario	Source(s)
1	Password	Third Party 1	Theft	5	Physical	5	25	5	One or more user IDs and passwords used for third party access are compromised and exploited for the purpose of stealing or destroying customer and company information.	Cleaning crews, Maintenance
2	Customer Name, Social security number, age, address	Third Party 2	Theft	4	Electronic	50,000	200,000	5	Physical records disposed for shredding are compromised	Shredding vendors
3	Outbound payment instructions	Data Store 1	Alteration	5	Electronic	100	500	5	Outbound payment instructions are altered, creating fraudulent payment instructions, and losses for the organization	Hackers, Disgruntled employees
4	Customer name, and phone number	IT System 1	Destruction / Interruption of Access	2	Electronic	50,000	100,000	4	Software operating on IT System 1 and Records accessible via IT System 1 destroyed, interrupted, held for ransom	Hackers
5	Intellectual Property	Data Store 2	Theft	5	Electronic	2	10	5	Theft of trade secrets results in lost competitive advantage and undercuts future sales	Hackers

Summary

This example depicts 5 types of information important to the organization, worth protecting in some manner. 1 piece of information is physical and 4 are maintained electronically. Two pieces of information reside with third parties, two in data stores, and one resides on a system (server). The importance of access to one record is reflected in the information criticality rating and the number of records that reside on or could be accessed through a third party or the IT infrastructure element are known through Step 2 - Identifying Location and Amount of Important Information. The systemic worst case impact and calibrated inherent risk depict how important it is to properly manage the assessed element. In this example, the highest risks are around managing third party 1's access to systems; how Third Party 2 manages important information they have about customers, unauthorized access to outbound payment instructions and intellectual property maintained in Data Store 1 and Data Store 2, respectively.

Notes

A – Information recorded in column A are the types of information identified in the risk assessment as being important

B – Information recorded in column B are the framework element where the information is handled, stored, processed. It is a business process, a third party, or a specific IT infrastructure element (external-facing access point, application, system, database / store)

C – Information recorded in column C is the type of threat to the information noted in column A and the threat scenario and source(s) of risk are listed in columns I and J

D – Information criticality relates to the importance of the information to the organization.

E – Column E represents the worst-case impact to the organization should the information in Column A be exploited.

F – Colum F represents the number of records described in column A that could be exploited, worst-case via the threat-source.

G – Column G = (Column D, Info Criticality, * Column F, number of records at risk). Systemic risk in context of information security refers to the risk that all of the records of importance could be accessed and exploited. This is characterized as a cascading failure which could potentially compromise most or all of the organizations systems and records resulting in a massive information security breach or service disruption.

H – This column represents the security risk to the organization after considering the existence and effectiveness of controls. Risk is represented using the reporting rating scales of the organization as discussed in Step 3, above. Calibrated Inherent risk is computed as follows: If Single Record Worst Case Impact = 5, Calibrated Inherent Risk Level = 5, Else Calibrated Inherent Risk Level = Systemic Worst Case Impact represented based on the reporting rating scales of the organization.

I – See Note C, above

J – See Note C, above

TABLE 2 –RESIDUAL RISK ASSESSMENT EXAMPLE

Notes:	A	B	C	D	E	F	G	H	I
Row	Important Information	Element Assessed	Information Format	Calibrated Inherent Risk	Control	Control Operating (Y/N)	Control Effectiveness %	Calculated Residual Risk Level	Scale
1	Password	Third Party 1	Physical	5	• Passwords access has been replaced with multifactor authentication • Third Party 1 provides end-user training to the employees annually	Y N	70 0	1.5	Med-Low.
2	Customer Name, Social Security Number, age, address	Third Party 2	Electronic	5	• Third party2 provides end user training to employees annually around info sec • Independent third party info sec audit report of third party shows no deficiencies (a.k.a. SSAE-16)	Y Y	20 50	1.5	Med-Low.
3	Outbound Payment Instructions	Data Store 1	Electronic	5	• Payment Instructions are only accepted across encrypted VPN • Payment instructions in route are not written to temporary storage (so unauthorized access to data store not a threat to payment instructions)	Y Y	30 60	.5	Low
4	Customer Name and Phone Number	IT System 1	Electronic	4	• System Patches are applied within 24 hours of release	Y	25	3.4	High
5	Intellectual Property	Data Store 2	Electronic	5	• Default Admin passwords are changed	Y	25	3.75	High

Summary

This table provides an example of controls that might be implemented for the inherent information risk examples provided in Table 1. Each risk is pulled across from with its inherent risk rating. One or more controls implemented to address the risk is identified in Column C. A determination is made as to whether the control is operating (Column E). If the Control is operating, a control effectiveness rating is assigned to the control (column F). Control effectiveness is an estimate of how much the inherent risk would be reduced by the operating control. Residual Risk level of each item (column G) is derived by taking the inherent risk of the item (column D) and reducing it by the control effectiveness of the applied, operating controls. In this example H = D – (F*D). In other words, inherent information risk is reduced by an amount commensurate with the effectiveness of controls in place.

Notes

A – Information recorded in column A is types of information identified in the risk assessment as being important

B – Information recorded in column B are the framework element where the information is handled, stored, processed. It is a business process, a third party, or a specific IT infrastructure element

C – Information Format carried forward from inherent risk assessment, Column C, Table 1

D – Calibrated Inherent Risk carried forward from inherent risk assessment, Column H, Table 1

E – Control is a description of the control(s) in place to mitigate the inherent risk

F – Control Operating is a determination through periodic manual or continuous monitoring / scanning as to whether the control is operating. Some practitioners may wish to include a measurement of both design and operating effectiveness

G – Control Effectiveness % is an estimate, usually provided by a subject matter expert regarding the degree to which the control mitigates the risk. The estimate of control effectiveness will change over time as technology, best practice, and threat-sources change and so should be reaffirmed with each risk assessment cycle.

H – The Calculated Residual Risk level is calculated by reducing the amount of inherent risk by the combined effectiveness of controls. In Row 1, for example, the inherent risk associated with exploiting a password used by Third Party 1 = 5 (critical). Two controls exist to mitigate this risk: Passwords access has been replaced with multifactor authentication and the third party provides end-user training to employees annually. The effectiveness of multifactor authentication is deemed to be 70% while employee training has 0% effectiveness because the control was not operating. Residual Risk of a password exploit at Third Party 1 is 1.5 = (IR of 5 – (IR of 5*70% control effectiveness). This translates to a medium-low residual risk rating.

I – The residual risk rating scale used for residual risk is the same as used for inherent risk. It is based on a 5 point scale with 5 = Critical and 1 = Low risk. The Calculated Residual Risk levels in column H are depicted in the residual risk rating scale column.

RSA

GLOSSARY OF TERMS

Business-Driven Security - the fusion of information security insights with business context to help organizations know where to make strategic information security investments. Creating an explicit linkage between what the security technology indicates, and what that means in terms of risk to the business

business risk management framework element - refers to any risk management record. Within the scope of this whitepaper, business risk management framework elements may include strategies and objectives, products and services, policies and procedures, authoritative (regulatory) sources, business processes and sub-processes, third parties, and IT Infrastructure elements (web services, IT software applications, IT systems, databases and data stores.)

calibration - risk calibration refers to the process of translating individual risk assessments into a common agreed upon rating scale

cyber risk appetite - the amount of loss or harm the organization is willing to take related to its technical infrastructure or the use of technology within an organization in order to achieve its objectives

cyber risk tolerance - the amount of loss or harm the organization is willing to take

external-facing access points - a business risk management framework element that refers to internet-facing web services, routers, hubs, switches, and any other kind of telecommunications-related devices that are accessible by any external parties

inherent risk - the risk that an activity would pose if no controls, other mitigating factors, or risk transfer was in place

inherent risk assessment - the process of estimating the likelihood and impact of threats of the information being stolen, altered, or made unavailable as the result of malicious or unintentional acts originating internally or external to the organization, including man-made disasters and “acts of God”

policy - records a high-level principle or course of action that has been decided by senior management and / or the board. The intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by the enterprise’s management teams. In addition to policy content, policies typically describe the consequences of failing to comply with the policy, the means for handling exceptions, and the manner in which compliance with the policy will be checked and measured. Examples of security policies include: Regulatory Compliance policy, Acceptable Use policy, and Human Resources policy.

procedure - a document that contains a detailed description of the steps necessary to perform specific operations in conformance with applicable policies and regulations. Procedures are defined as part of business processes.

regulation - a rule or law defined and enforced by an authority to regulate the conduct of the enterprise within specific geographic or political boundaries. Large organizations operating across multiple boundaries will typically be subject to many duplicative, overlapping regulations. Examples of security-related regulations include the EU GDPR, Gramm-Leach Bliley Act, and HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule.

risk appetite - the maximum level of risk the organization is willing to accept to achieve its objectives

risk tolerance - the maximum level of risk the organization is willing to take on a particular transaction

standard - a mandatory requirement that an organization has chosen to follow. It may be a code of practice or specification approved by a recognized external standards organization, such as International Organization for Standardization (ISO). Standards logically connect an organization's policies and the regulations under which it operates.

The information in this publication is provided "as is." Dell Inc. or its subsidiaries make no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA 04/17 White Paper H16083

Dell Inc. or its subsidiaries believe the information in this document is accurate as of its publication date. The information is subject to change without notice.