G00296694

Managing Risk and Security at the Speed of Digital Business

Analyst(s): Tom Scholtz

Digital business challenges the basic principles of information risk and security management. Risk and security leaders must understand the risks associated with business unit innovation, and balance the imperative to protect the enterprise with the need to adopt innovative technology approaches.

Key Challenges

- Increasing adoption of digital business strategies is challenging conventional approaches to security and risk management.
- Risk and security programs must adapt to this new reality or face being sidelined by the digital business initiatives, ironically exposing the enterprise to even bigger risk.

Recommendations

- Develop a compelling vision for risk and security management based on establishing trust and resilience in your digital business.
- Adapt the strategic objectives of your risk and security program to encompass the new realities of digital business.
- Embrace the six principles of trust and resilience.
- Develop and evolve an adaptive, context-aware security architecture.
- Implement and manage a formal, process-based risk and security management program to support the digital business.

Table of Contents

List of Tables

List of Figures

Introduction

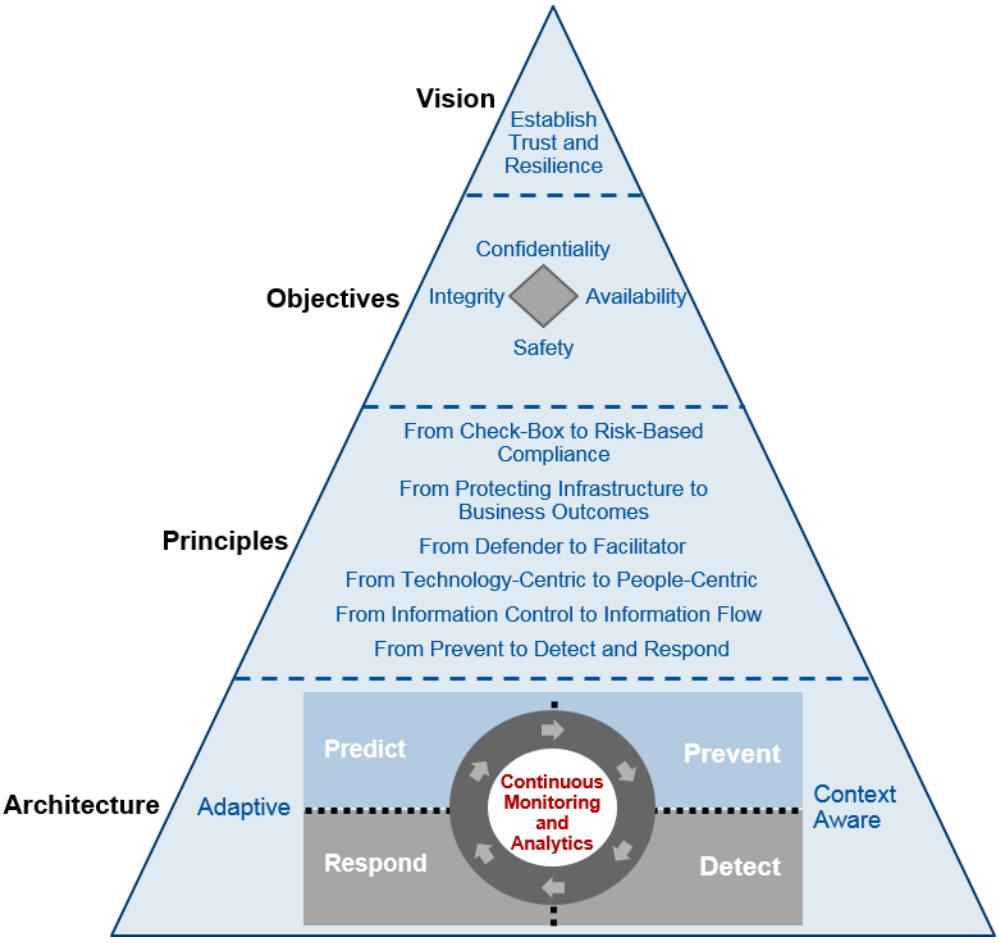
The increasing adoption of digital business approaches is changing the traditional IT governance and control landscape. Two key characteristics of digital business are challenging conventional IT control:

- As the business claims increasing autonomy in deploying new digital technologies, it degrades the authority of the central IT organization.
- The dramatic increase in the number of elements (e.g., systems, devices, things, data and dynamic relationships) exposes scalability issues with many traditional security control solutions.

This reality challenges the status quo in information risk and security management. Many conventions and technologies on which risk and security practices have been based do not scale in the new reality. For example, the principle of least privilege is being challenged by new approaches that support business agility. IT risk and information security leaders must assess and transform their programs to become digital business enablers rather than obstacles to innovation.

Gartner has developed a series of foundational research that conveys risk and security practices appropriate for the digital business era (see Figure 1). We will continue to develop applicable research on this topic (see the Gartner Recommended Reading section).

Figure 1. The Foundations of Risk and Security in the Digital Business World



Vision: "Trust and Resilience: The Future of Digital Business Risk"
Objectives: "Cybersecurity Scenario 2020 Phase 2: Guardians for Big Change"
Principles: "Use Six Principles of Resilience to Address Digital Business Risk and Security"
Architecture: "Designing an Adaptive Security Architecture for Protection From Advanced Attacks"

Source: Gartner (2016)

Analysis

Develop a Compelling Vision for Risk and Security Management Based on Establishing Trust and Resilience in Your Digital Business

The starting point for any risk and security program is to develop a compelling vision that the rest of the business can comprehend and that will act as a target state for strategy planning activities. The

typical objective of an information security and risk management program is to establish a continuous, iteratively improving regimen of planning, building and running security solutions that are aligned to business requirements. Most organizations will develop an initial vision of such an information security management system (ISMS) from existing standards and frameworks, such as ISO/IEC 27001.

However, it is crucial that the vision is customized by complementing the basic ISMS model through articulating the business, technology and risk drivers that are unique to the enterprise. Within the context of digital business, it is important to acknowledge that the digital business environment comes with unprecedented risks that go beyond IT operations, encompassing the enterprise and its ecosystem (see "Predicts 2016: Security for the Internet of Things").

Hence, the vision for risk and security in the digital business must be based on establishing an ecosystem that enables trust and resilience (see "Trust and Resilience: The Future of Digital Business Risk"). The vision must:

- **Make the people, processes and technology more resilient.** The transformation to full-scale digital business extends well beyond the IT organization, impacting the design and staffing of nearly every business function. Its sheer scale underscores the importance of applying resilience to people, processes and technology. It emphasizes the need to focus beyond IT risk to operational risk. As digital business takes hold, digital risk becomes increasingly synonymous with operational risk. More and more enterprise business functions, including IT, are now architected for agility and convenience. In the next decade, the trade-offs between convenience and resilience will be difficult, and significant investment will be required throughout the enterprise (see "Use KPI and KRI Mapping to Make the Business Case for Business Resilience").
- **Increase awareness among stakeholders to build trust and resilience.** Technology alone will not protect the individual and the enterprise, whether from their own carelessness or malicious actors. Increased personal awareness and responsibility with respect to safety and propriety must come into play (see "Definition: People-Centric Security"). Enterprises should replace once-a-year training with ongoing awareness campaigns. Given that the lines between personal and business technology are blurring, enterprises should also consider extending protections to employees at home.
- **Support a bimodal IT strategy** (see "How to Achieve Enterprise Agility With a Bimodal Capability"). Risk and security specialists must get a seat at the bimodal table and work with business and IT stakeholders to get visibility into Mode 2 projects. While not neglecting the risks inherent in Mode 1 operations, they must use a risk-based approach that is cognizant of the unique risk appetite associated with Mode 2 initiatives rather than trying to enforce conventional standard controls.
- **Plan for the unprecedented.** Digital business is an unprecedented era. To assume that tomorrow will be just like today, or only slightly different, is a risk in itself. At this early stage, there are precious few best practices for digital business (risk management included), and most of these are only "next" practices. To succeed, enterprises will have to blaze new trails. To be resilient, they will need to go beyond the ordinary, imagining responses to unprecedented but plausible circumstances.

- **Address the need to protect assets that IT no longer owns or controls** (e.g., cloud-based services or new mobile-based applications). In digital businesses, more technology is being procured and operated outside of the visibility or control of the IT department. Decentralized IT spend implicitly puts more control in the business units for deciding how much risk they will accept and how much they will spend to address risk.

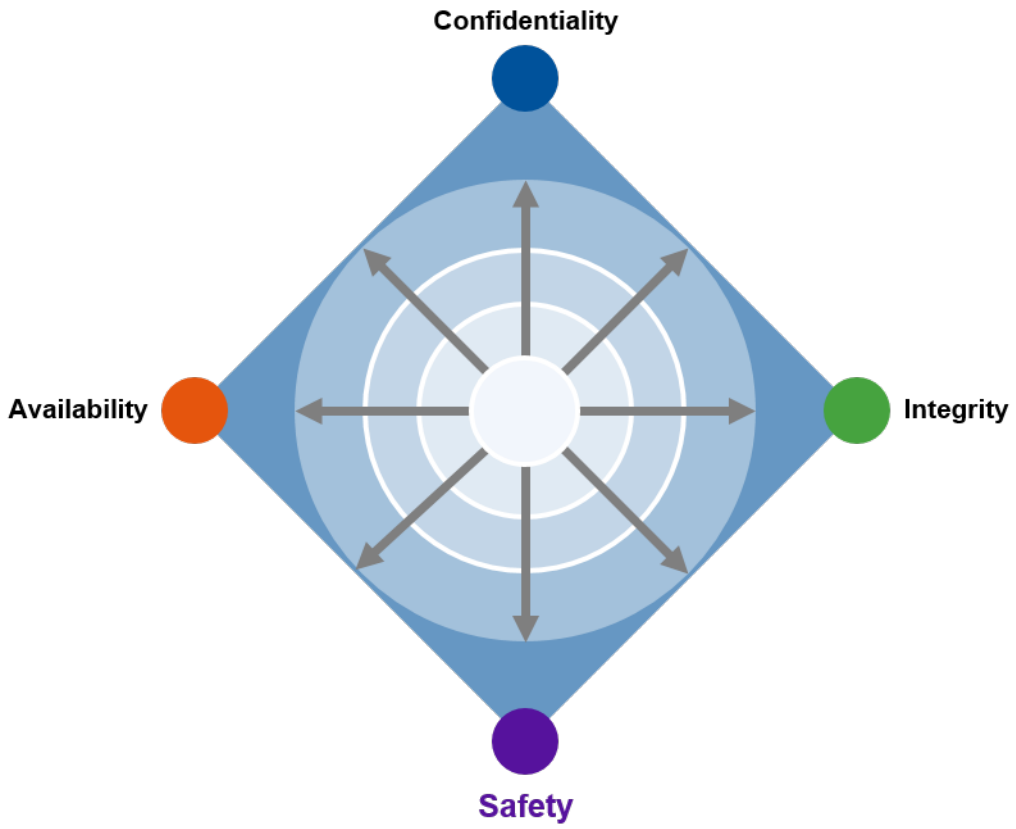
The objective is to provide an ecosystem that balances the imperative to protect the enterprise with the need to adopt innovative, risky new technology approaches to remain competitive.

Adapt the Strategic Objectives of Your Risk and Security Program to Encompass the New Realities of Digital Business

The digital explosion is reshaping organizational security and risk management. The traditional model ascribed to for decades has been based on the objectives of confidentiality, integrity and availability (CIA). However, in the digital business world, the CIA model isn't enough.

Digital business is pushing the environment for protecting data and infrastructure into the physical world, merging functions focused on data and information with functions that make actual changes to people and their surrounding environments. Protecting information alone isn't enough, and ensuring the confidentiality, integrity and availability of that information isn't enough. Leaders in risk and cybersecurity must now assume the responsibility of providing safety for both people and their environments or, at minimum, participate in providing that safety with other security practices (see Figure 2 and "Cybersecurity Scenario 2020 Phase 2: Guardians for Big Change").

Figure 2. The CIAS Model of Cybersecurity



Source: Gartner (2016)

As digital business transforms the way in which technology and information are used in the enterprise, it is prudent to investigate the effectiveness of the current risk and security leadership function and organization. In many organizations, the existing risk and security roles are constrained by the limits of their scope, authority and experience. A digital risk officer (see "Innovation Insight: Digital Business Innovation Risk Will Bring About the Rise of the Digital Risk Officer") can potentially provide the authority (and attract the requisite skills) to deal effectively with digital business risks.

Embrace the Six Principles of Trust and Resilience

Digital business is challenging key security conventions such as the principle of least privilege or that prevention is always better than cure. In this dynamic environment, successful risk and security requires adopting a new set of key principles (see "Use Six Principles of Resilience to Address Digital Business Risk and Security").

Principle No. 1: Stop Focusing on Check-Box Compliance, and Shift to Risk-Based Decision Making

Risk-based thinking is about understanding the major perils a business will face and prioritizing controls and investments in IT risk and security to achieve business outcomes. As technological complexity increases, leaders won't have enough money to address all threats equally. Risk-based thinking allows cybersecurity investments to be targeted where the greatest risk resides — but risk according to the business itself, not IT's view of risk. While many organizations believe they have already achieved this transition, Gartner still observes many compliance-driven behaviors (see "Compliance Is No Longer a Primary Driver for IT Risk and Security").

Principle No. 2: Stop Solely Protecting Infrastructure, and Begin Supporting Business Outcomes

The infrastructure must be protected; however, leaders must elevate the risk and security strategy to protect desired business outcomes. For businesses, this means corporate performance, such as profitability. For government, this means public service delivery and citizen welfare. For the military, this means protecting the mission (see "Developing Key Risk Indicators: Developing Causal Chains to Link Risk to Business Outcomes").

Principle No. 3: Stop Being a Defender, and Become a Facilitator

As part of the transition to supporting a business outcome mindset, IT risk and security leaders must move from being the righteous defenders of the organization to acting as the facilitators of a balance between the need to protect the organization and the need to achieve desired business outcomes. Organizations must continue to invest in legacy technology, traditional cybersecurity and availability operations activities, where they are still appropriate. However, rapid innovation to facilitate digital business requires IT risk and cybersecurity programs to adopt a different approach to developing new controls that is more fluid, agile and adaptable.

Principle No. 4: Stop Trying to Control Information, and Determine How It Flows

IT risk and security leaders must move from trying to control the flow of information to understanding how information flows. This understanding will improve organizational resilience and support the achievement of desired outcomes. Digital business will introduce massive new volumes and types of information, and business processes that must be understood and appropriately protected.

Principle No. 5: Accept the Limits of Technology and Become People-Centric

IT risk and security leaders must understand the limits of security and availability solutions and recognize that properly motivated people can be the strongest links in the chain. It is necessary to shape behavior and motivate people to do the right thing; it's not enough to just try to force people to do what they are told.

Gartner has pioneered a strategic approach to information security known as "people-centric security" (see "Definition: People-Centric Security"). This emphasizes individual accountability and trust, and it de-emphasizes restrictive, preventive security controls. People-centric security is all about individual trust and accountability.

Principle No. 6: Stop Trying to Perfectly Protect Your Organization, and Invest in Detection and Response

Compromised IT environments are inevitable. IT risk and security leaders must move from a singular focus on trying to prevent compromise to acknowledge that perfect prevention is not achievable. The organization needs to be able to detect a compromised IT environment and react quickly. In the digital world, the pace of change will be too fast to anticipate, and it will be impossible to defend against every type of attack. IT risk and security leaders must invest in technical, procedural and human capabilities to detect when a compromise occurs. They must provide the tools for first responders to react quickly and investigate the source and impact of breaches, compromise and incidents (see "Shift Cybersecurity Investment to Detection and Response").

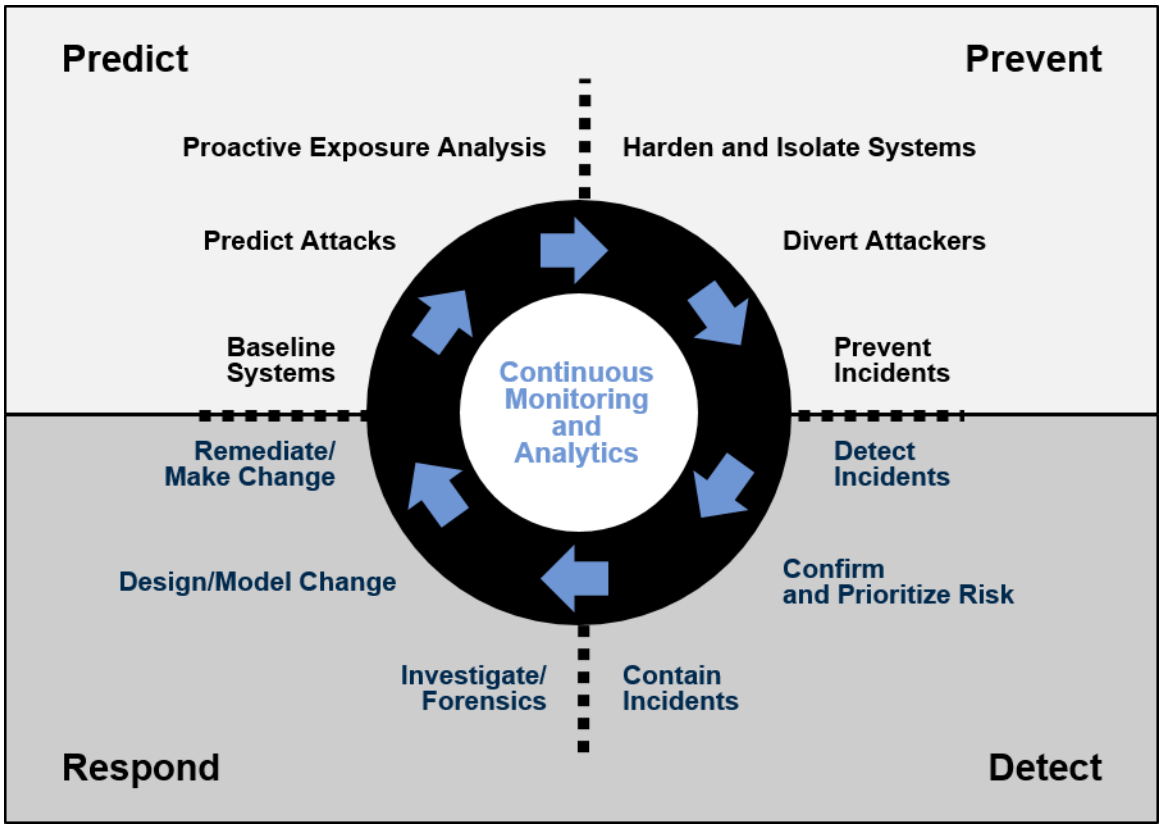
Embracing these six principles predicates a willingness to deviate from perceived security conventions and best practices. This requires not just a willingness to change on behalf of incumbent staff, it also impacts the hiring of new risk and security resources. Hiring leaders should not just look for digital business technology skills, but also for people willing to move beyond conventional thinking (see "CISOs Should Review Their Enterprise's Security Skills Portfolio Now").

Develop and Evolve an Adaptive, Context-Aware Security Architecture

Most conventional security efforts and products have traditionally focused on blocking and prevention techniques (such as antivirus) as well as on policy-based controls (such as firewalls) to block threats (see the upper-right quadrant of Figure 3). However, perfect prevention is impossible (see "Prevention Is Futile in 2020: Protect Information via Pervasive Monitoring and Collective Intelligence"). Advanced targeted attacks are easily bypassing traditional firewalls and signature-based prevention mechanisms. All organizations should now assume that they are in a state of continuous compromise. However, organizations have deluded themselves into believing that 100% prevention is possible, and they have become overly reliant on blocking-based and signature-based mechanisms for protection. As a result, most enterprises have limited capabilities to detect and respond to breaches when they inevitably occur (see the bottom half of Figure 3), resulting in longer dwell times and increased damage.

To enable a comprehensive, adaptive security protection architecture, we believe that 12 specific capabilities are necessary to augment the ability to block and prevent attacks, as well as detect and respond to attacks (see Figure 3 and "Designing an Adaptive Security Architecture for Protection From Advanced Attacks").

Figure 3. Twelve Critical Capabilities of Gartner's Adaptive Security Architecture



Source: Gartner (2016)

Implement and Manage a Formal, Process-Based Risk and Security Management Program to Support the Digital Business

Effective risk and security management requires an integrated approach in which risk and security are made part of the core fabric of business processes and become key components of the organizational culture. This requires infusing the key components of risk and security management (i.e., policies, processes, behavior and technology) across all the dimensions of IT — business processes, applications, technology infrastructure and, most importantly, people.

In larger enterprises, this predicates the establishment of a strategic, process-based risk-and-security program. Such a program is a complex ecosystem consisting of multiple elements (see Table 1).

Table 1. Elements of a Risk-and-Security Program

Component	Purpose	Content/Deliverables	Foundational Gartner Research
Enterprise Security Charter	Executive Mandate	■ Business Need ■ Scope ■ Accountability Statement ■ Mandate for CISO ■ Mandate for Program and Policy	"Best Practices for Creating an Enterprise Information Security Charter"
Security Program Framework	Terms of Reference/ Reference Model	■ Vision Statement ■ ISMS Description ■ Principles ■ Program Components ■ Capabilities/Functions Taxonomy ■ Security Architecture Framework ■ Policy Framework	"Toolkit: Simple Functional Information Security Taxonomy" "Five Golden Rules for Creating Effective Security Policy"
Annual Strategy Plan	Plan of Action	■ Target State ■ Current State ■ Gap Analysis ■ Roadmap of Technical, Strategic and BAU Initiatives	"Security Management Strategy Planning Best Practices"
Governance Model	Implementation of Accountability and Decision Rights	■ Policy Framework ■ Steering Committees/Bodies ■ Organization Model ■ Executive/Assurance Reporting Framework	"Best Practices for Establishing an Information Security Steering Committee"
Process Model	Operational/Maturity Improvements; Foundation for Organization Model	■ Process Catalog ■ Maturity Model	"The Security Processes You Must Get Right"

Source: Gartner (2016)

To support digital business initiatives, this program must support a bimodal IT strategy (see "Bimodal IT: How to Be Digitally Agile Without Making a Mess"). As Mode 2 projects will require increased agility, existing formalized security programs might need refinements, principally in supporting the plan and budget phases of Mode 2 projects. Organizations without a formalized security program might mistakenly think they can be more flexible, but security for bimodal IT requires more, not less, rigor to effectively balance risks with necessary agility.

To support bimodal initiatives, risk and security leaders must:

- Take steps to prepare security and risk management teams for bimodal IT. Learn about bimodal IT, evaluate where your organization is on the bimodal journey, and identify the primary skills and technology gaps.
- Build additional organizational capabilities to support increased agility and defend against new digital risks.
- Understand the higher-risk appetite represented by Mode 2 projects.
- Adapt security practices to the pace of Mode 2 projects, with laser focus on low interferences during early stages and continuous monitoring of security debt.
- Maximize effectiveness with a bimodal security program. Start before you are ready with small scale, autonomous projects to lead cultural change toward increased agility.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Information Security Management Program Primer for 2016"

"Cloud Security and Emerging Technology Security Primer for 2016"

"Business Continuity Management Program Primer for 2016"

"Risk Management Program Primer for 2016"

"Identity and Access Management Program Primer for 2016"

More on This Topic

This is part of three in-depth collections of research. See the collections:

- Explore Algorithmic Business to Drive Differentiation
- Special Report: Cybersecurity at the Speed of Digital Business
- Special Report: Cybersecurity at the Speed of Digital Business

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp