IBM Security

IBM

The ABCs of security strategy

Empower your business with the building blocks of a flexible, risk-based security posture

IBM Security White Paper

Assessing risk in an ever-changing environment

In today's fast-paced world, it's more challenging than ever to protect your organization against security threats. Third-party services (such as cloud, consulting and outsourcing services) and online collaboration (via social media) are now vital for achieving business goals. There's also the added complexity of users accessing data from mobile devices.

Globally, business and technology advancements are opening up new avenues of opportunity—and unprecedented risk. Cybercriminals, nation-state actors, organized crime rings, disgruntled employees and malicious insiders are highly sophisticated, and ready to exploit vulnerabilities. As a result, government and industry-related compliance mandates are also on the rise.

Is there a "silver bullet" to solve all these challenges? No, but the right planning and security strategy can help you manage risk, today and tomorrow. Plus, it can give you a competitive advantage that helps you attract and retain clients. An effective security program can help you implement the ABCs of security strategy, so you can:

- **A**lign your business and IT technologies, while mitigating the impact from threats
- **B**uild a security posture that can adapt to changing environments and evolving threats
- **C**reate a balanced approach for optimizing people, processes and technology
- **D**evelop a risk-based security program to help manage ongoing challenges

This document highlights the challenges organizations typically face in applying these ABCs and explains how IBM can help resolve them.

Key trends:

- Increasing and sophisticated attacks
- Mobile and social access
- Cloud security risks
- Increasing and changing compliance mandates
- Complex third-party services
- Large multinational workforces

Keeping up with the evolving threat landscape

Today's attacks are complex, clever and persistent, with high impact. In fact, traditional security practices are not effective against the latest threats. That's why successful companies are transforming their security programs to better align with their business and IT strategies. Effective security programs today need to be highly adaptable to change, and to be efficient, they need a risk-based approach that balances people, processes and technologies.

So how do you get started? Think beyond a single solution. You need rigorous and integrated security governance, risk management and compliance capabilities—and the ability to continuously adjust to the changing business environment to mitigate advanced threats.

How to build effective security strategies:

Note: Click on a link above for recommendations.

Challenge 1:

How can I harden my security posture?

To defend against increasingly sophisticated threats, you need a dynamic security program that can transform and grow with your organization. Existing security programs are simply falling short in addressing the evolving threat landscape. However, rigid security policies can impede your business objectives—the challenge is how to determine how much security is enough. You need to:

- **Define a clear strategy** for aligning security practices with business needs
- **Streamline tools and processes** for continuously managing security risk
- **Establish effective controls** to drive a higher return on security investments
- **Address C-level concerns** with real-time reporting on risk and compliance activities

Beyond technology and process, people are essential to successful security. Corporate leaders have a high interest in managing security risks, thanks to the rise of high-profile security incidents. Be sure to plan for ways to build a culture of security into your organization, so everyone from top executives to third-party contractors is mindful of risk in their everyday activities.

Learn how IBM can help you with your security strategy.

Only 14% of security leaders think a **standardized way** to assess and quantify risk will be widely used in the next 3 to 5 years.[1]

Challenge 2:

What's the right way to deploy cloud security?

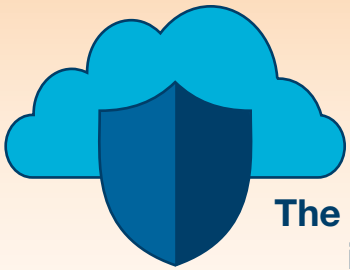
The cloud is transforming businesses at staggering rates. Although executives still have concerns about cloud security, cloud consumption is widespread and continuing to grow. In fact, 86 percent of security leaders have adopted cloud or are planning cloud initiatives. Over the next three to five years, 75 percent expect their cloud security budget to increase or increase dramatically.[1]

The key challenge in cloud usage is how to turn security into a growth enabler—not an inhibitor. When moving workloads to a private, public or hybrid cloud environment, you'll need to **assess** that the solution supports your business security and privacy priorities. You'll need to **design** actionable plans to stay ahead of threats. Plus, you'll need to **manage** the environment to mitigate risk.

An effective cloud security strategy should be comprehensive, including elements of:

- Data protection—covering data privacy and security to help drive business
- Infrastructure protection—addressing protection against network and web application attacks to help improve defenses
- Regulatory compliance—meeting regulations, laws and compliance to help reduce risk

Learn how IBM can help you with your cloud security strategy.



The security of data in the cloud is a top executive-level concern.[2]

Challenge 3:

How can I effectively manage risk and compliance?

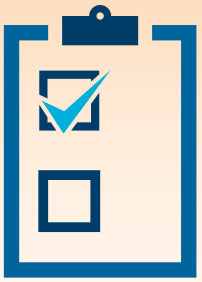
Security breaches are on the rise—and so are security mandates. In fact, it's an increasing challenge to demonstrate compliance with:

- Security frameworks, such as ISO 27000 Series
- Regulatory mandates, such as the Health Insurance Portability and Accountability Act (HIPAA) or the Sarbanes-Oxley Act (SOX)
- Industry requirements, such as those from the payment card industry (PCI)

Governments are increasing the pressure to comply with regulatory mandates, and organizations are losing in court when fighting compliance-related cases. There is also a low tolerance for noncompliance from shareholders, customers and industry peers. To avoid the penalties of noncompliance, you'll need to **evaluate** your technical, operational and IT security risks, **define** plans for remediation, and **manage** ongoing governance and reporting.

As the complexity of compliance grows, you need a flexible security program that can evolve to meet any shifts in regulations. You need to consider if you have the right tools for privacy and PCI compliance. What's more, you cannot afford to have redundant roles and processes, which can result in inconsistent reporting and ineffective security.

Learn how IBM can help you manage your risk and compliance issues.



79% of security leaders said the challenge from government regulations and industry standards has

increased

over the past three years.[1]

Challenge 4:

How can I automate my governance processes?

Security skills are in short supply worldwide. And with the growing need to secure your organization against evolving threats—while also ensuring compliance with the latest regulatory mandates—the skills gap is expanding further.

By automating your processes for governance, risk and compliance, you can **minimize surprises** and **simplify routine tasks.** The right tools can provide executives with information on regulatory compliance, while empowering your IT team with the right metrics for risk-based decision making. Security controls with integrated analytics are essential for visualizing threats, developing insights and responding faster to the highest priority offenses.

Learn how IBM can help you automate your risk management processes.

92% of security decision-makers say that

staffing issues

contribute to heightened levels of risk.[3]

Challenge 5:

How can I reduce my ERP vulnerabilities?

If you're using enterprise resource planning (ERP) software such as SAP to run critical business processes, a security breach could lead to the loss of highly valuable and regulated data. But the inherent complexity and scale of these systems makes them extremely challenging to protect. Specialized security consultants are often required to help:

- Manage the security considerations in individual SAP components
- Reduce risk in new SAP areas, including HANA, mobile, cloud, fraud analytics and managed services
- Facilitate compliance across the ERP and non-ERP environments

To reduce ERP vulnerabilities, you'll need a security strategy that addresses governance, risk management and compliance in specific SAP components. Plus, you'll need to focus on protecting new SAP capabilities.

Learn how IBM can help you with your SAP security issues.

In 2014, more than

391

security alerts

affecting SAP were issued—46% ranked as "high priority."[4]

Challenge 6:

What's the right way to protect my critical infrastructure?

If you operate in the "critical infrastructure" sector, you face a double challenge: defending your systems against attacks, while trying to manage the convergence of IT and Operational Technology (OT). After all, IT security was traditionally separate from industrial control and automation. But as IT and OT networks converge, you'll need to carefully manage the transformation and safeguard against cyber attacks.

Everyone from power and energy companies to oil and gas firms is at an increased risk of attack. To help protect your critical infrastructure, you need to:

- **Assess the baseline security** of your industrial control systems
- **Develop a roadmap** for improving your overall security
- **Perform self-assessments** to verify security of high-risk areas

Government mandates about critical infrastructure security are also providing a new urgency for deploying the right tools and processes to demonstrate compliance.

To develop an effective security strategy, you'll need to evaluate the current state of your security and focus on how to improve it—across your OT assets, systems, networks, and related security processes and technologies. You'll also need to assess your compliance readiness with regulatory requirements and/or industry frameworks, and identify how to mitigate risks and help improve protection.

Learn how IBM can help you secure your critical infrastructure.

More than a third of critical infrastructure systems are vulnerable to attack via the Internet.[5]

IBM can help conquer your security challenges

With IBM Security Strategy, Risk and Compliance Services, we can help you effectively manage risk and help you understand how your IT security needs to evolve as your business grows. Our security experts can provide recommendations to help you reach beyond point products and compliance-driven practices and work with you to develop a comprehensive security strategy—one that can adapt to changing threats and gives you the confidence to pursue new opportunities.

Learn how IBM can help you solve your security challenges:

Note: Click on a link above for more information.

How IBM can help—Solution 1:

Evolve your security posture with security strategy consulting services

Security strategy consulting services from IBM can help you define a strategy and establish IT security controls to better manage your risk. Data breaches aren't going away, but IBM experts can work with your organization to help you reduce their impact. We can help you be prepared to respond to ever-evolving threats.

IBM consultants can help examine your security landscape to identify gaps, develop a roadmap to harden your security posture and deploy technologies to mitigate risks. We can help you:

- Assess how your security program meets business risk mitigation objectives
- Define a strategy to align your security program to business requirements
- Optimize security investments to achieve greater benefits from your security budget
- Understand how your security capabilities relate to one another to facilitate risk and regulatory compliance management

We can also map your current security posture against 10 essential practices—a security model that IBM uses within our organization to safeguard ourselves. This can help develop a profile of your security maturity and how to move forward in planning and deploying a comprehensive strategy.

Learn more

Nearly 60% of security leaders said the sophistication of attackers was outstripping the sophistication of their organization's defenses.[1]

How IBM can help—Solution 2:

Safeguard your cloud with cloud security strategy consulting services

Cloud security strategy consulting services from IBM can help you identify and prioritize cloud computing scenarios for your specific security requirements and business needs. Likewise, our security experts can identify security and privacy solutions to help protect your unique cloud initiatives. Our methodology includes baseline assessments, strategy planning and implementation programs for cloud security solutions.

Our cloud computing specialists work with you on-site to help you:

- Develop a holistic approach to the cloud for effective security—across infrastructure, platforms and software-as-a-service (SaaS)
- Better protect the confidentiality, integrity and availability of your computing resources and data
- Establish appropriate risk management strategies and cloud computing goals
- Understand and identify the security and privacy risks associated with cloud computing
- Develop a security strategy to better manage corporate, regulatory and customer security requirements

Learn more

82% of security leaders said the very

definition of security

has changed in the last three years.[1]

How IBM can help—Solution 3:

Bridge security gaps with risk and compliance consulting services

Risk and compliance consulting services from IBM are designed to provide a "big picture" approach to managing risk. Using the Unified Compliance Framework (UCF), our experts can assess your security capabilities across common industry standards to identify gaps in your controls, score the level of IT risk and prioritize remediation activities. The UCF helps define the scope of controls needed to comply with multiple regulatory initiatives in an efficient manner—reducing duplicate efforts and inconsistent reporting.

For example, our PCI compliance advisory services can help you achieve and maintain PCI compliance in accordance with annual audits. We help clients identify and fix root causes of noncompliance and establish internal controls to better support ongoing compliance. Our holistic PCI compliance program includes distinct phases of planning, assessment, remediation and compliance reporting.

IBM enables your organization to go beyond "checkbox compliance" and focus on managing risk at all levels of the business. We can help you:

- Assess the impact of identified threats and vulnerabilities
- Implement short- and long-term strategies to enhance your security posture
- Align IT security with business goals by verifying the right controls are in place
- Establish processes for understanding threats, their sources and effective responses
- Focus on managing risk, not just compliance audits

Learn more

Security leaders say that

regulations, standards and compliance

will continue to be a major factor—particularly for businesses operating on a global level.[1]

How IBM can help—Solution 4:

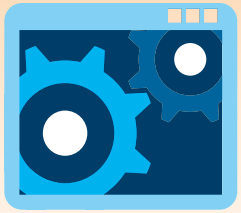
Empower staff with automated IT risk management services

Automated IT risk management services from IBM can enable your security teams to focus on the high-priority tasks that matter the most to the business. With the right governance, risk and compliance (GRC) tools, you can streamline compliance reporting, visualize risks and quickly respond to future needs.

IBM has a full portfolio of integrated services to help you:

- Identify, manage, monitor, and analyze risk and compliance across the enterprise
- Integrate governance, risk management and compliance processes to meet the persistent challenge of regulatory oversight
- Leverage GRC information to make better business decisions
- Empower decision makers with fully scalable and interactive GRC reporting and trending tools

Learn more



Only 51% of organizations see themselves as mature with respect to automated tools for IT GRC.[1]

How IBM can help—Solution 5:

Protect your critical SAP operations with IBM Security services

IBM Security services can help reduce the vulnerabilities in the SAP systems that house your organization's most valuable information. With the right combination of SAP monitoring, automated alerts and rapid responses, attacks can be disrupted in real time.

IBM offers flexible services for the full range of SAP systems:

- Assess SAP systems for vulnerability and compliance risks—tying business context into remediation planning processes
- Align your SAP security policies with the latest industry standards
- Help protect against known-but-unpublished vulnerabilities
- Leverage continuous monitoring and advanced threat protection against zero-day attacks
- Streamline auditing and compliance management

Learn more

Improve security across SAP:

- Enterprise resource planning (ERP)
- Human resources (HR)
- Supplier relationship management (SRM)
- Customer relationship management (CRM)
- HANA, mobile and cloud

How IBM can help—Solution 6:

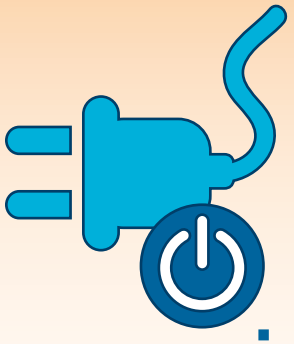
Reduce cyber risks with critical infrastructure security services

Critical infrastructure security services from IBM are designed to help deliver a cost-effective, long-term solution to securing your critical infrastructure and industrial controls. Our experts can help you navigate the convergence of IT and OT networks and deploy the right security to help you protect your critical assets.

IBM provides a cost-effective way to determine your organization's overall risk tolerance. We help you:

- Adopt a sustainable methodology for assessing and planning your industrial controls security
- Better manage industry and government standards, such as the National Institute of Standards and Technology (NIST) guidance
- Assess the maturity of your cyber-security program and if you should make changes—and how it may affect your business
- Develop a prioritized mitigation strategy to help you realize a more security-rich cyber environment

Learn more



There's been a tenfold increase in the number of successful attacks into critical infrastructure systems since 2000.[5]

Client success stories

Building a security strategy for cloud and IoT initiatives

A global manufacturing company wanted to market a smart appliance, which would enable customers to control and manage appliances remotely. The company needed help in ensuring effective security of the solution. IBM worked with the company in a two-month engagement to develop a comprehensive cyber-security strategy for the solution—including prioritized security roadmaps with both strategic and tactical recommendations. Now, the company has specific tactics to help protect Internet of Things (IoT) devices, mobile applications and cloud data.

Meeting compliance demands for power-grid infrastructure

Like most power companies, this electric company lacked the time, resources and expertise to cost-effectively manage and monitor its network security. With the help of IBM security experts, the company was able to identify ways to help reduce security risk and comply with government and industry regulations. The company now has the expertise it needs to maintain compliance with current regulations. Plus, it can help protect critical power-grid assets without having to hire and train additional in-house staff.

Managing SAP licenses for improved security and cost savings

A major consumer goods manufacturer was facing huge penalties from SAP due to inappropriately managed user and engine licenses—along with security gaps from the lack of management of inactive user identities. By working with IBM, the manufacturer deployed SAP best practices for managing user access across multiple business units, which helped reduce insider threats. It can also now reliably measure license use at the transaction level, avoiding the financial penalties of not complying with its SAP contract.

Why IBM?

The IBM Security Strategy, Risk and Compliance Services team serves as a trusted advisor for managing risk for organizations across the globe. We use a balanced approach to applying people, processes and technologies to create an adaptable security posture that can scale as your business grows. Using our deep security expertise, proven best practices, security intelligence and comprehensive security portfolio, we can help protect even the most complex IT environments. IBM works closely with clients to help them build effective security programs that not only protect infrastructure, but also enhance business operations.

IBM security consultants have deep experience in IT security consulting, many with certifications in domains such as compliance, data protection, application services, risk management, cyber security, mobility, cloud and so on. They have access to the world's largest known database of threats. Plus, they work closely with the IBM security research, development and delivery organizations which monitor 15 billion security events per day in more than 130 countries, and hold more than 3,000 security patents. Our security teams are backed by 10 security research centers, nine Security Operations Centers and 14 security development laboratories.

IBM Security Strategy, Risk and Compliance Services:

- Focuses on helping you align your security program to mitigate the latest security challenges
- Provides a comprehensive view of compliance through the unified compliance framework
- Offers the support of security specialists that understand industry-specific challenges and solutions

IBM helps organizations apply the ABCs of security strategy

Align business and IT technologies

Build an adaptable security posture

Create a balanced approach for optimizing people, processes and technology

Develop a risk-based security program

Learn more

[1] Marc van Zadelhoff, Kristin Lovejoy and David Jarvis, "Fortifying for the future: Insights from the 2014 IBM Chief Information Security Officer Assessment," *IBM Center for Applied Insights*, December 2014. http://www-935.ibm.com/services/us/en/it-services/security-services/index.html?lnk=sec_home

[2] Adam Greenberg, "Executives concerned about cloud security, report shows," *SC Magazine*, January 13, 2015. http://www.scmagazine.com/cloud-security-is-a-top-executive-level-concern/article/392329/

[3] Forrester Consulting, "Surviving the Technical Security Skills Crisis: An Assessment Of The Current Security Skills Landscape And How To Overcome It," *Commissioned by IBM Corp.*, May 2013. http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03030usen/SEW03030USEN.PDF http://www-935.ibm.com/services/us/en/security/infographic/skillsshortage.html

[4] Ezequiel Gutesman, "2014 SAP Security Advisories: A Year in Review and Future Trends," *Onapsis, Inc.*, December 2014. http://www.onapsis.com/blog/sap-security-advisories-a-preview-of-a-year-in-review-and-future-trends/

[5] Matthew E. Luallen, "SANS SCADA and Process Control Security Survey," *The SANS Institute*, February 2013. http://www.sans.org/reading-room/analysts-program/sans-survey-scada-2013

SEW03081-USEN-00