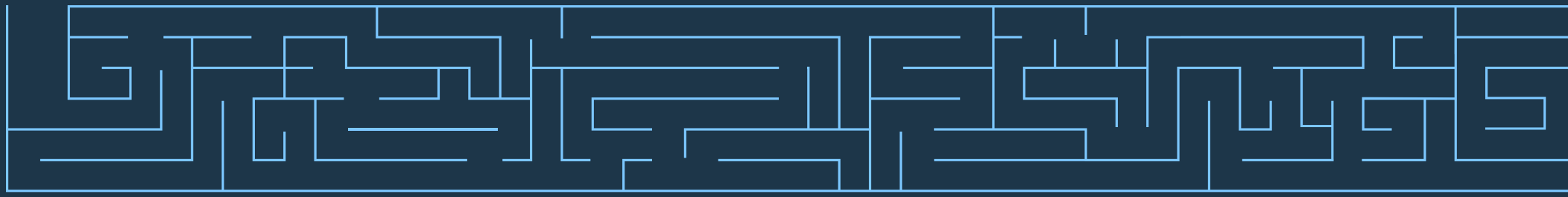
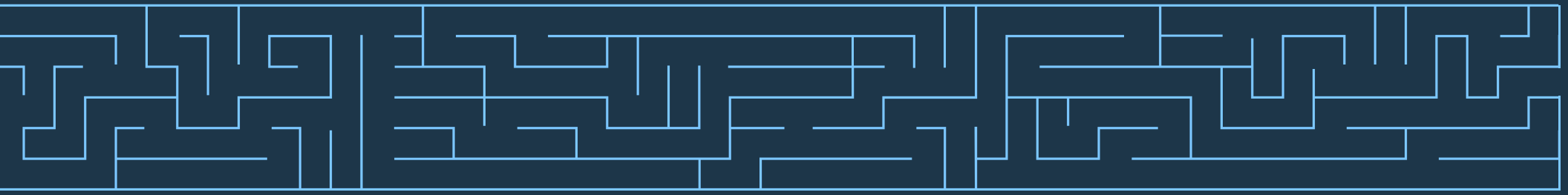
IBM Security

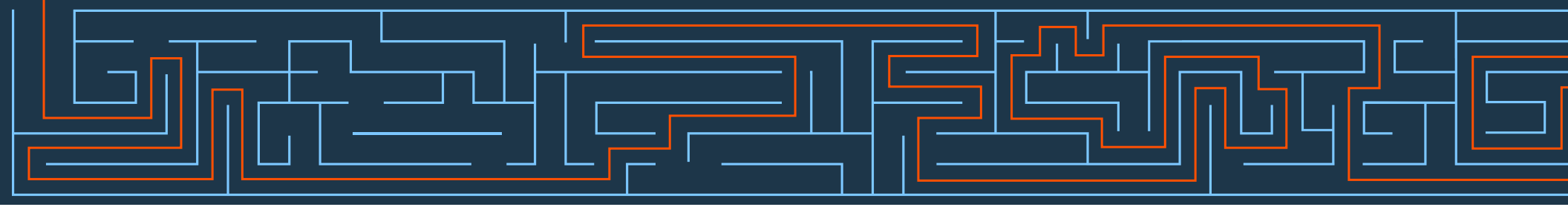


Navigating the compliance maze

How IBM Security can help prepare your organization for the world of rules, regulations and standards.



Start here →



Welcome to the world of rules, regulations and standards

Faced with a complex set of competing regulations, policies, standards and guidelines aimed at protecting sensitive customer, partner and process data, many companies are uncertain about finding the right approach to meeting their specific regulatory requirements. And for some, effectively integrating compliance requirements into existing security policies and controls can represent a significant challenge.

But where compliance is concerned, there's no such thing as a free pass. You can't opt out. And the consequences for failing to comply can mean increased costs down the road.

What's more, the term "compliance" can apply to everything from international and federal mandates to industry standards and internal policies. And while compliance is only one aspect of a comprehensive security program, it can involve non-security issues as well. So how do you develop effective measures and policies that align with the specific capabilities of your organization—and provide security? That's what we're here to discuss.

What compliance means in today's data-intense world

There are two things that today's organizations clearly have plenty of: data and rules governing the use and protection of that data. It's been estimated that by 2020, companies will spend over $1.5 billion on compliance efforts each year—some of which are more successful than others.[1] But whether they're successful or not, compliance isn't something organizations can choose to ignore. They have an important responsibility to their clients, customers, business partners and shareholders. And single audits alone don't fulfill that responsibility.

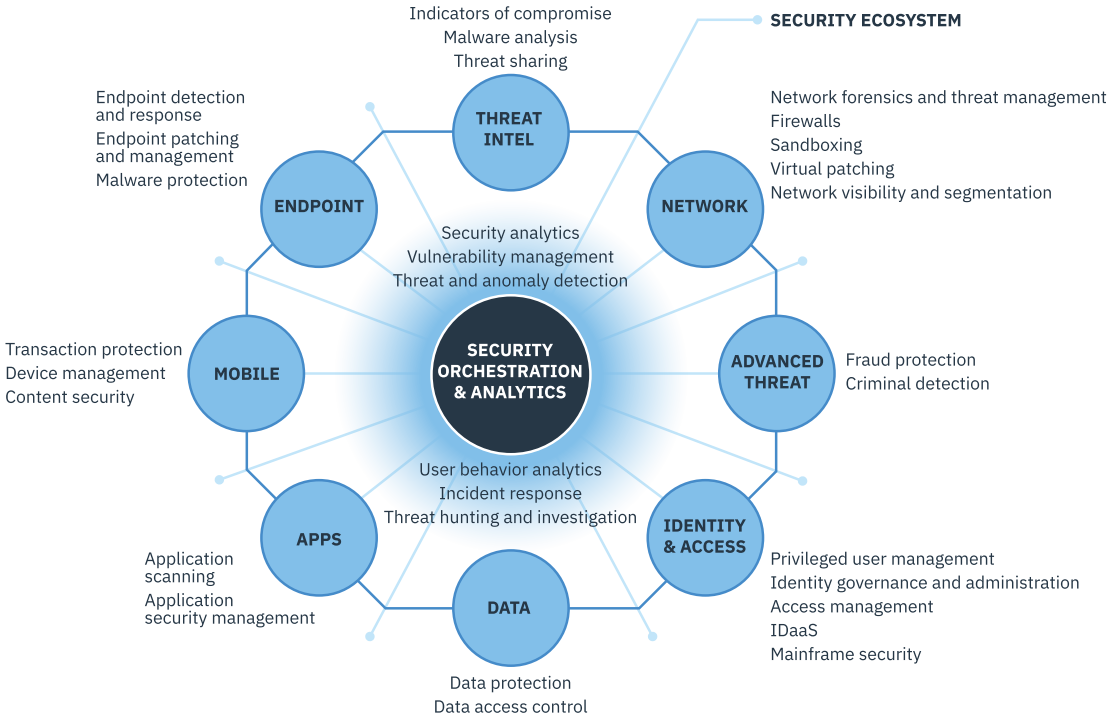
That's why so many organizations are looking for ways to develop and manage successful compliance strategies.

It's not about passing a single audit

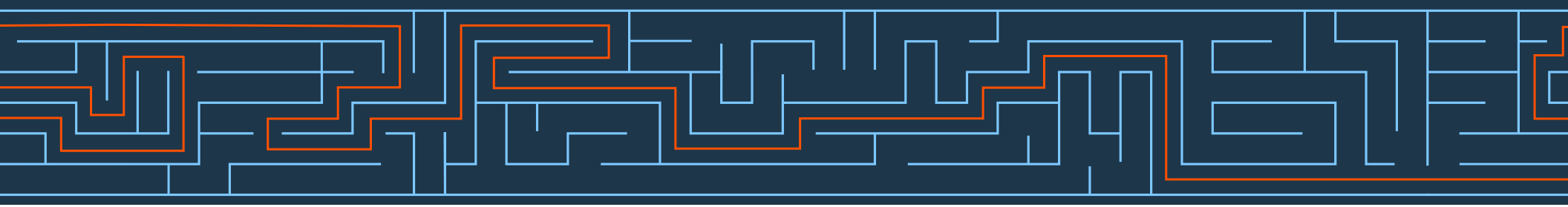
In an ideal world, compliance would be built into an organization's security policies and everyday practices. But in the real world, that's not always the case. Instead, compliance often becomes a periodic goal that's linked to passing an audit. And once the audit is over, compliance seems to become less important—until the next audit comes around. Being able to "check all the boxes" isn't a compliance and security strategy.

Where readiness meets security

The IBM Security immune system



Because many compliance requirements overlap with security issues, it makes sense to unify your overall strategy for managing security and governance. The IBM® Security immune system combines enterprise security intelligence and expertise in a single framework. It's a fully integrated approach that allows its components to grow and adapt within an organization's infrastructure—working together to improve their effectiveness. And since compliance-related activities are rarely confined to a single area within your systems, it allows all the necessary "parts and pieces" to come together to provide a comprehensive approach to addressing requirements.



Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of network and information systems (NIS Directive)	International Standards for IT Service Management (ISO/IEC 27001)
Federal Financial Institutions Examination Council (FFIEC)	National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
Federal Risk and Automation Management Program (FedRAMP)	New York Department of Financial Services (NY DFS Part 504)
General Data Protection Regulation (GDPR)	North American Electric Reliability Corporation Critical Infrastructure Project (NERC CIP V)
Gramm Leach Bliley Act (GLBA)	Payment Card Industry Data Security Standard (PCI DSS)
Health Information Technology for Economic and Clinical Health Act (HITECH)	Payment Services Directive 2 (PSD2)
Health Insurance Portability and Accountability Act (HIPAA)	Sarbanes-Oxley Act (SOX)
Health Information Trust Alliance (HITRUST)	Society for Worldwide Interbank Financial Telecommunication (SWIFT)

What makes compliance so complicated?

Three use cases provide the details

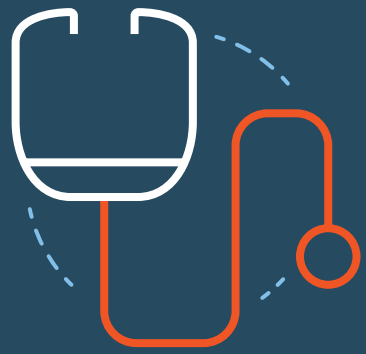
Because the same set of rules can mean different things to different industries—and to different companies within those industries—here are three use cases that offer examples of how IBM solutions can help you prepare to meet your compliance requirements.

Click on a panel below to see the details

A hospital stumbles into noncompliance

A utility company powers through IT/OT challenges

A major bank faces new regulations



A hospital stumbles into noncompliance

While efforts to strengthen cyber security among healthcare organizations have increased in recent years, many hospitals, medical insurers and pharmaceutical companies remain unprotected and unprepared to successfully fend off external attacks—which could expose confidential patient, scientific and financial data. Here's an example of what could happen to a hospital's compliance status without the proper controls and security measures in place.[2]

A mid-level billing analyst opens an infected attachment in an email that appears to come from a known vendor. The attachment launches malware that infects the analyst's computer. The malware then sends phishing emails to privileged users with high-level access in the hospital's system, with the goal of capturing IDs and passwords. Using those credentials, the attackers gain access to massive quantities of patient records and financial data, which they quietly export to concealed computers outside the system. And at that point the hospital reaches a state of noncompliance with a multitude of rules and regulations designed to protect private health information and financial details.

IBM Security solutions are designed to help hospitals prepare for situations like these. **IBM BigFix®** would have been patching the latest vulnerabilities and would have quarantined infected computers to prevent more damage, while **IBM MaaS360®** would have detected and stopped malware from spreading to mobile devices. And at the same time, **IBM QRadar® Network Protection (XGS)** would have blocked zero-day exploit traffic and sent flows to **IBM QRadar Security and Event Management (SIEM)** for anomaly detection—while **IBM AppScan** and **IBM Security Guardium®** would monitor all applications and data files and halt unauthorized access to them. QRadar would also have correlated network flows and security events from other security controls into a list of priority offenses.

Meanwhile, **IBM i2®** would team with **IBM X-Force® Exchange** to investigate potential threats while **IBM QRadar Incident Forensics** would reconstruct any abnormal activity. And going forward, **IBM Resilient® Incident Response Platform™** would allow responders to coordinate activity before serious damage could occur, while **IBM Managed Security Services** deliver governance, risk and compliance consulting and systems integration to continue safeguarding the organization.

Back to content →

A utility company powers through IT/OT challenges

Today's utility companies face massive challenges as they attempt to deal with security issues that threaten their infrastructures, frustrating even the most adept security professionals. Advances in smart grid technologies are crossing the border to corporate IT, posing potential new risks to operational technology (OT) networks. But a sizable number of utilities may not have the operational security experience or resources to both secure operational grid processes and provide OT security.

Facing these challenges, a mid-sized utility company approached IBM for help in preparing for a growing set of compliance requirements, while boosting the overall security of its IT and OT operations. The company's security team wanted help determining how to:

- Prepare for new NIST Cyber Security Framework requirements and reuse any ISO 27000 series measures already in place
- Handle potential gaps related to technology, people or processes
- Prioritize objectives, address key challenges to success and identify the fastest route to success
- Build a governance model that retains a positive security culture

IBM Security Strategy Risk and Compliance services offered the company a risk-based approach to addressing its concerns. Starting with a gap analysis that focused on a selected set of regulations and standards—including the NIST Cyber Security Framework—IBM assessed the utility's cyber security capabilities from both an organizational and a technical point of view. The resulting strategy recommendations allowed the company to understand the resource allocations and planning efforts necessary to help mitigate the risks that had been identified.

In addition, IBM recommended that the company increase its reporting requirements and resolve an observed shortfall in security monitoring. IBM also uncovered a need for greater network security insights, which would allow the company to identify security breaches in operational real time—for both its IT and OT networks.

The utility chose **IBM QRadar® SIEM** to provide automated security information and event management and establish companywide threat coverage. The company also gained IT and OT overarching security event insights and developed an OT security policy with IBM Security Strategy Risk and Compliance services.

Finally, the company went on to include incident response capabilities—to help it meet another regulatory requirement. **IBM Resilient® Incident Response Platform™** allowed it to build its own resources and offer response playbooks as a service to smaller local utilities.

Back to content →

A major bank faces new regulations

The financial services industry is one of the most highly regulated marketplaces in the world. And New York is arguably at the epicenter of that world. So when a new set of cybersecurity requirements went into effect March 1, 2017, its impact was felt by thousands of banks, financial services companies and insurance firms doing business in the state—whether or not they're headquartered there.

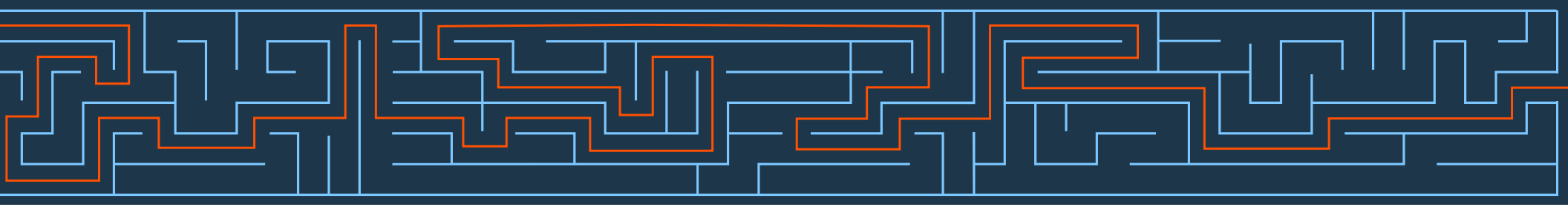
The challenges they face are enormous. For starters, it's important to recognize that virtually every financial services organization operating in New York is doing business online and/or in the cloud. And that means the new regulations apply to just about all of them. The rules cover nonpublic data along with customer data, mandate the presence of a CISO (or third-party equivalent) and require a program for secure data destruction. They also require that firms publish a documented incident response plan, monitor the activities of authorized users and maintain audit logs.

If that sounds daunting, consider this: Companies impacted by the new regulations were given 180 days (that is, until August 28, 2017) to become compliant. In today's hyper-competitive business environment it can take six months just to find and hire the right CISO. And that doesn't even include time for him or her to hire a team.

Not surprisingly, a number of those companies affected by the new regulation are seeking help from IBM Security—including a major bank with global operations. Faced with the new requirements and a short timeframe, the bank wanted to start by reviewing its end-to-end cyber and cloud programs against regulatory requirements. **IBM Security Framework and Risk Assessment services** provided gap analyses and recommended practical enhancements to the bank's processes and controls to help address regulatory alignment. Additional IBM services offerings provided an outside-in assessment "through the regulators' eyes" to help identify potential gaps that should be addressed before regulatory examination. And with help from **Cloud Security Readiness Assessment Services**, the bank was able to assess governance and organization of cyber information and public cloud programs.

Meanwhile, IBM Security Framework and Risk Assessment services—along with **IBM X-Force® Incident Response and Intelligence services**—are allowing a deep-dive assessment and enhancement work on particular aspects of information and technology risk management monitoring. The bank has also adopted **IBM Security QRadar®** for monitoring and **IBM Resilient® Incident Response Platform™** for incident response, and **IBM Trusteer Pinpoint™ Detect** for real-time fraud detection.

Back to content →



Why IBM

There's no shortage of rules and regulations governing how today's massive quantities of data must be handled and protected. Likewise, there's no shortage of ways in which your efforts to comply with those rules and regulations can go wrong. The good news is that when it comes to compliance, organizations are shifting their approach from checking boxes to managing risks. They're becoming more proactive in the face of new rules and regulations, completing risk assessments to help reveal gaps and taking action before noncompliance can become an issue.

That's why it's now more important than ever to develop and implement a compliance strategy that meshes successfully with your overall security strategy.

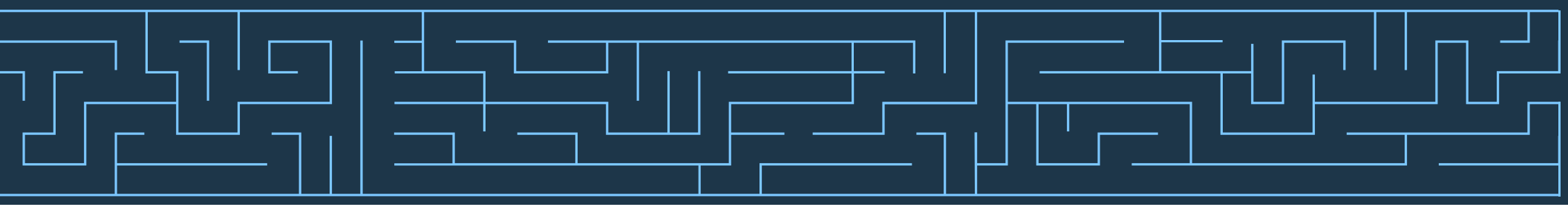
IBM offers a comprehensive set of solutions and services designed to help you integrate readiness into your organization's ongoing operations—instead of as a fire drill that disrupts nearly everyone and everything associated with the data you need to protect. Within that context, we deliver leading technology, best practices and, above all, flexibility.

When you partner with IBM, you gain access to a security team of 8,000 people supporting more than 12,000 customers in 133 countries. As a proven leader in enterprise security, we hold more than 3,500 security patents. And with an approach based on the security immune system discussed here, along with advanced cognitive computing, we let organizations like yours continue to innovate while addressing risk. So you can continue to grow your business—while securing your most critical data and processes.

For more information

To learn more about the IBM Security portfolio of solutions, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

Additionally, IBM Global Financing offers numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing



© Copyright IBM Corporation 2017

IBM Security
75 Binney Street
Cambridge MA 02142

Produced in the United States of America
October 2017

IBM, the IBM logo, ibm.com, BigFix, Guardium, Maas360, QRadar, Resilient Incident Response Platform, Trusteer and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

[1] Gartner, Forecast Snapshot: Integrated Risk Management Solutions, Worldwide, 2017.
[2] http://www.hipaajournal.com/category/hipaa-breach-news/

WGB03036-USEN-01

Back to start

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of r (NIS Directive)	ce Management (ISO/IEC 27001)
Federal Financial Institut	Technology SF)
Federal Risk and Autom	Services (NY DFS Part 504)
General Data Protection	Corporation Critical)
Gramm Leach Bliley Act	rity Standard (PCI DSS)
Health Information Tech Health Act (HITECH)	02)
Health Insurance Portab	
Health Information Trust Alliance (HITRUST)	Society for Worldwide Interbank Financial Telecommunication (SWIFT)

Directive on security of network and information systems (NIS Directive)

The NIS Directive was adopted by the European Parliament in July 2016 and is the first piece of European Union-wide legislation on cybersecurity. It calls for member states to each develop a computer security incident response team (CSIRT) and a competent national NIS authority, along with a CSIRT network to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks. **(More information)**

Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on se (NIS Directive)		SO/IEC 27001)
Federal Financ		
Federal Risk ar		S Part 504)
General Data P		cal
Gramm Leach		DSS)
Health Informa Health Act (HIT		
Health Insuran		
Health Informa		

Federal Financial Institutions Examination Council (FFIEC)

The FFIEC is a formal US interagency body empowered to prescribe uniform principles, standards and report forms for the examination of financial institutions by the board of governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS) and the State Liaison Committee (SLC)—which includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS). The council is also responsible for making recommendations to promote uniformity in the supervision of financial institutions. **(More information)**

← Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on (NIS Directiv		/IEC 27001)
Federal Fina		
Federal Risk		art 504)
General Data		
Gramm Lea		SS)
Health Inforr Health Act (H		
Health Insura		
Health Inforr		

Federal Risk and Automation Management Program (FedRAMP)

FedRAMP is a US government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services. Based on a "do once, use many times" framework that can save an estimated 30 to 40 percent of government costs, it also reduces both the amount of time and staff required to conduct redundant agency security assessments. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry. **(More information)**

← Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of network and information systems (NIS Directive)	International Standards for IT Service Management (ISO/IEC 27001)
Federal Financial Inst	y
Federal Risk and Aut	NY DFS Part 504)
General Data Protect	on Critical
Gramm Leach Bliley	rd (PCI DSS)
Health Information Te Health Act (HITECH)	
Health Insurance Por	
Health Information Trust Alliance (HITRUST)	Telecommunication (SWIFT)

General Data Protection Regulation (GDPR)

GDPR (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union. It also addresses export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. **(More information)**

← Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of network and information systems (NIS Directive)	International Standards for IT Service Management (ISO/IEC 27001)
Federal Financial Institutions Exam	and Technology T CSF)
Federal Risk and Automation Man	cial Services (NY DFS Part 504)
General Data Protection Regulatio	ility Corporation Critical IP V)
Gramm Leach Bliley Act (GLBA)	ecurity Standard (PCI DSS)
Health Information Technology for Health Act (HITECH)	PSD2)
Health Insurance Portability and A	
Health Information Trust Alliance (	k Financial

Gramm Leach Bliley Act (GLBA)

The GLBA requires financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data. **(More information)**

← Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of network a (NIS Directive)	vice Management (ISO/IEC 27001)
Federal Financial Institutions Exar	d Technology CSF)
Federal Risk and Automation Mar	al Services (NY DFS Part 504)
General Data Protection Regulatic	y Corporation Critical V)
Gramm Leach Bliley Act (GLBA)	urity Standard (PCI DSS)
Health Information Technology fo Health Act (HITECH)	SD2)
Health Insurance Portability and A	
Health Information Trust Alliance (	Financial

Health Information Technology for Economic and Clinical Health Act (HITECH)

The HITECH Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was created to promote the adoption and meaningful use of health information technology. Subtitle D of the act addresses the privacy and security concerns associated with the electronic transmission of health information by strengthening civil and criminal enforcement of HIPAA rules. **(More information)**

← Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of network and information systems (NIS Directive)	International Standards for IT Service Management (ISO/IEC 27001)
Federal Financial Institutions	nology
Federal Risk and Automatio	vices (NY DFS Part 504)
General Data Protection Reg	poration Critical
Gramm Leach Bliley Act (GL	Standard (PCI DSS)
Health Information Technolo Health Act (HITECH)	
Health Insurance Portability	
Health Information Trust Alli	cial

Health Insurance Portability and Accountability Act (HIPAA)

Title II of HIPAA requires the establishment of national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans and employers. It also addresses the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the US healthcare system by encouraging the widespread use of electronic data interchange. **(More information)**

Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of network and information systems (NIS Directive)	International Standards for IT Service Management (ISO/IEC 27001)
Federal Financial Institutions Examination Council (FFIEC)	National Institute of Standards and Technology SF)
Federal Risk and Automation Ma	l Services (NY DFS Part 504)
General Data Protection Regulati	y Corporation Critical V)
Gramm Leach Bliley Act (GLBA)	urity Standard (PCI DSS)
Health Information Technology fo Health Act (HITECH)	D2)
Health Insurance Portability and	
Health Information Trust Alliance	inancial

Health Information Trust Alliance (HITRUST)

The not-for-profit HITRUST Alliance develops, maintains and provides broad access to its common risk and compliance management and de-identification frameworks, and related assessment and assurance methodologies, as well as programs supporting cyber sharing, analysis and resilience. **(More information)**

Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of networ (NIS Directive)	Management (ISO/IEC 27001)
Federal Financial Institutions E	echnology F)
Federal Risk and Automation M	ervices (NY DFS Part 504)
General Data Protection Regul	Corporation Critical
Gramm Leach Bliley Act (GLBA	y Standard (PCI DSS)
Health Information Technology Health Act (HITECH)	)
Health Insurance Portability and Accountability Act (HIPAA)	Sarbanes-Oxley Act (SOX)
Health Information Trust Alliance (HITRUST)	Society for Worldwide Interbank Financial Telecommunication (SWIFT)

International Standards for IT Service Management (ISO/IEC 27001)

The ISO/IEC 27001 family of more than a dozen standards is designed to help organizations keep information assets secure. These include financial information, intellectual property, employee details and information entrusted to organizations by third parties. **(More information)**

Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on securit (NIS Directive)	ent (ISO/IEC 27001)
Federal Financial In	
Federal Risk and A	Y DFS Part 504)
General Data Prote	Critical
Gramm Leach Blile	(PCI DSS)
Health Information Health Act (HITECH	
Health Insurance Portability and Accountability Act (HIPAA)	Sarbanes-Oxley Act (SOX)
Health Information Trust Alliance (HITRUST)	Society for Worldwide Interbank Financial Telecommunication (SWIFT)

National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

A US executive order aimed at improving critical infrastructure cybersecurity led to the development of a voluntary risk-based cybersecurity framework—which is a set of industry standards and best practices designed to help organizations manage cybersecurity risks. Created through collaboration between government and the private sector, the framework uses a common language to cost-effectively address and manage cybersecurity risk, based on business needs. **(More information)**

Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of network and information systems (NIS Directive)	International Standards for IT Service Management (ISO/IEC 27001)
Federal Financial Institutio	ology
Federal Risk and Automat	ces (NY DFS Part 504)
General Data Protection R	oration Critical
Gramm Leach Bliley Act (	andard (PCI DSS)
Health Information Techno Health Act (HITECH)	
Health Insurance Portabili	
Health Information Trust A	l

New York Department of Financial Services (NY DFS Part 504)

NY DFS Part 504 is a risk-based anti-terrorism and anti-money laundering regulation that requires regulated institutions to maintain programs to monitor and filter transactions for potential Bank Secrecy Act and anti-money laundering violations and prevent transactions with sanctioned entities. The final regulation requires regulated institutions annually to submit a board resolution or senior officer compliance finding confirming steps taken to ascertain compliance with the regulation. **(More information)**

← **Back to table**

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of network and information systems (NIS Directive)	International Standards for IT Service Management (ISO/IEC 27001)
Federal Financial Institut	ogy
Federal Risk and Automa	es (NY DFS Part 504)
General Data Protection	ation Critical
Gramm Leach Bliley Act	ndard (PCI DSS)
Health Information Techn Health Act (HITECH)	
Health Insurance Portab	
Health Information Trust	

North American Electric Reliability Corporation Critical Infrastructure Project (NERC CIP V)

The NERC ensures the reliability of the bulk power system in North America. It develops and enforces reliability standards; assesses adequacy annually via a 10-year forecast and winter and summer forecasts; monitors the bulk power system and educates, trains, and certifies industry personnel. As a self-regulatory organization, it's subject to oversight by the US Federal Energy Regulatory Commission and governmental authorities in Canada. **(More information)**

← Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of network and information systems (NIS Directive)	International Standards for IT Service Management (ISO/IEC 27001)
Federal Financial Institutio	ology
Federal Risk and Automat	ces (NY DFS Part 504)
General Data Protection R	oration Critical
Gramm Leach Bliley Act (G	andard (PCI DSS)
Health Information Techno Health Act (HITECH)	
Health Insurance Portabili	
Health Information Trust A	al

Payment Card Industry Data Security Standard (PCI DSS)

The PCI Data Security Standard is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. The standards apply to all entities that store, process or transmit cardholder data—with guidance for software developers and manufacturers of applications and devices used in those transactions. **(More information)**

← Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of network and information systems (NIS Directive)	International Standards for IT Service Management (ISO/IEC 27001)
Federal Financial Instit	gy
Federal Risk and Auto	(NY DFS Part 504)
General Data Protecti	on Critical
Gramm Leach Bliley A	ard (PCI DSS)
Health Information Tec Health Act (HITECH)	
Health Insurance Porta	
Health Information Tru	

Payment Services Directive 2 (PSD2)

PSD2 is the second iteration of the directive on payment services adopted in 2007 by the European Parliament. Its goal is to streamline existing payment processing in Europe for any given transaction. The original legislation sought to clarify and ease payment processing through uniform rules and the by allowing new competition in the marketplace across the European Union. PSD2 seeks to level the playing field among countries and among payment service providers, while normalizing new payment methods such as online and mobile payments. **(More information)**

Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of network and information systems (NIS Directive)	International Standards for IT Service Management (ISO/IEC 27001)
Federal Financial Institutions E	chnology
Federal Risk and Automation	ervices (NY DFS Part 504)
General Data Protection Regu	orporation Critical
Gramm Leach Bliley Act (GLE	Standard (PCI DSS)
Health Information Technolog Health Act (HITECH)	
Health Insurance Portability a	
Health Information Trust Allian	ncial

Sarbanes-Oxley Act (SOX)

SOX became law in 2002, introducing major changes to the regulation of financial practice and corporate governance in the US. Its goal was to implement accounting and disclosure requirements that increase transparency in corporate governance and financial reporting and formalize a system of internal checks and balances. A typical SOX audit covers data access, IT security measures, change management and backup procedures. **(More information)**

Back to table

Playing by the rules

There are thousands of important regulations, certifications and standards governing how data is to be handled and protected around the world—and across virtually every major industry. As a result, organizations in those industries have had to make compliance a priority in developing their security strategies. But it hasn't been easy. Organizations in different industries need to contend with different challenges—even when dealing with the same regulation, certification or standard. To illustrate what that means, here are just 16 of the vast variety of rules that apply to multiple industries worldwide. Click on any of the names below to learn more about their individual requirements.

Directive on security of network and information systems (NIS Directive)	International Standards for IT Service Management (ISO/IEC 27001)
Federal Financial Institu	ogy
Federal Risk and Autom	s (NY DFS Part 504)
General Data Protectior	tion Critical
Gramm Leach Bliley Ac	dard (PCI DSS)
Health Information Tech Health Act (HITECH)	
Health Insurance Porta	
Health Information Trus	

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

Founded in 1973, SWIFT is a co-operative organization dedicated to promoting and developing standardized global interactivity for financial transactions. Its original mandate was to establish a global communications link for data processing and a common language for international financial transactions. With its headquarters in Brussels and data centers in Belgium and the US, SWIFT operates a messaging service for financial messages, such as letters of credit, payments, and securities transactions, between member banks. **(More information)**

← Back to table