WHITE PAPER

CDW PEOPLE WHO GET IT

# HOW TECHNOLOGY HELPS BANKS AND CREDIT UNIONS MEET REGULATORY MANDATES

The right solutions and services can help **banks and credit unions** navigate the compliance minefield.


## EXECUTIVE SUMMARY

Regulatory compliance is a major consideration in any bank or credit union's cybersecurity strategy. Not only will financial institutions lose the trust of their customers in the event of a data breach, but they also operate within a framework of stringent regulations that govern how they must manage data. Keeping up with these regulatory demands is a major challenge — especially for small firms that lack the resources of their larger competitors — and running afoul of the rules can bring stiff penalties, even when customer financial data hasn't been exposed.

The strategic deployment of key technologies and services can help ease this burden, allowing institutions to focus more attention on their core business. A trusted partner can help banks and credit unions make sure they are meeting all of the mandates of the regulations that govern them. Technology solutions can also bolster compliance efforts while improving security as well.

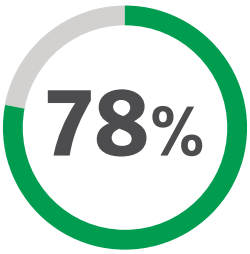
## A Minefield of Compliance Issues

Banks, credit unions and other financial institutions face a patchwork of various regulations. Some of the most significant include:

**Gramm–Leach–Bliley Act:** This 1999 law requires financial institutions to safeguard information such as account numbers, credit and income histories and Social Security numbers. Organizations must take several steps to ensure compliance, including identifying and assessing the risks to customer information in each relevant area of the company's operations. The measure also requires banks and credit unions to provide customers with privacy notices that explain their information-sharing practices.

**Dodd–Frank Act:** Passed in the wake of the 2008 financial industry collapse, and primarily meant to lower overall risk in the sector, this 2010 legislation also requires financial institutions to share confidential data with regulatory agencies. Some observers have also expressed concerns that the law's expansion of whistleblower rewards and provisions to grant consumers broader access to their information could weaken information security.

**USA PATRIOT Act:** This landmark anti-terrorism law requires that all financial institutions implement a customer identification program. To comply, banks and credit unions must verify the identity of any person seeking to open an account and maintain records of that verification process for five years after the account is closed.




The percentage of large financial institutions that have implemented data loss prevention tools, compared with 57% of small institutions.[1]

**Bank Secrecy Act:** This 1970 law (formally, the Currency and Foreign Transactions Reporting Act) requires financial institutions to keep records of cash purchases of negotiable instruments, to file reports of cash transactions exceeding $10,000 per day and to report activity that points to criminal activity.

**Home Mortgage Disclosure Act (HMDA):** The 1975 HMDA requires many financial institutions to maintain, report and publicly disclose information about mortgages.

**Payment Card Industry Data Security Standard (PCI DSS):** All businesses that handle payment card transactions must comply with the PCI DSS standard, but the importance of protecting payment card data is multiplied for banks and credit unions that issue debit and credit cards to their customers. Compliance with PCI can be both technically challenging and expensive, particularly without taking steps to understand and isolate the Card Data Environment.

## Services to Help Manage the Regulatory Burden

With so many different regulations to manage, many financial institutions turn to trusted IT partners such as CDW to provide security and compliance services. These services include:

**Penetration testing:** In a penetration test, security experts assume the role of hacker, running creative, in-depth analyses to determine whether security controls are operating as intended. By attempting to gain access to corporate resources, these experts are able to find holes and weaknesses within an organization's cybersecurity infrastructure, providing valuable information about vulnerabilities before malicious actors can exploit them. CDW's experts then use the information gleaned from the test to craft customized and prioritized cybersecurity roadmaps that shore up weaknesses and protect IT systems and assets. Often, the results of a penetration test help convince previously hesitant stakeholders within an organization (usually those outside of the IT department) that further investments in cybersecurity are warranted.

**NIST assessments:** The National Institute of Standards and Technology (NIST) has established the Cybersecurity Framework for federal agencies to follow. The guidance for agencies applies to banks and credit unions as well. During a NIST assessment, CDW places cybersecurity experts onsite at an organization to gather in-depth information about the enterprise's existing practices. These experts speak with representatives from various company departments, such as human resources and payroll, to better understand the organization's IT processes and policies — as well as other safeguards that may or may not be in place, such as employee background checks — to determine the greatest sources of cybersecurity risk. Then, CDW's experts create a list of recommendations, ranking each solution by what it will cost the organization and how much of a security gain it represents, to help reduce cyber risk in the most targeted and cost-effective manner possible.

### The Importance of Training

In its "Cybersecurity 101" resource guide for bank executives, the Conference of State Bank Supervisors warns that many financial institutions focus on the IT side of cybersecurity while ignoring staff training.

"Your staff can either be the weakest link in your bank's cybersecurity program," the guide's authors state, "or your greatest protection measure."

The organization recommends these staff training resources:

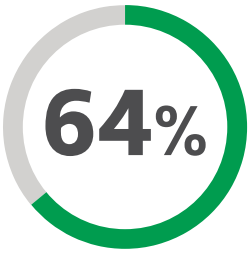
- "Cyber Challenge: A Community Bank Cyber Exercise," available online from the Federal Deposit Insurance Corp., helps banks conduct short exercises around risk-related scenarios.
- The National Cyber Security Alliance's Safe Online website highlights cybersecurity topics for management to talk about with staff.
- The Small Business Administration provides a free training course, available online, on cybersecurity for small businesses.
- The SANS Institute offers "Securing the Human," a two-day security awareness course about changing employee behavior to reduce cyber risk.

**SOURCE:** [1]New York State Department of Financial Services, "Report on Cyber Security in the Banking Sector," May 2014

**Configuration services:** When financial institutions bring in a partner such as CDW to configure new hardware and software — or to check on the configuration of existing solutions — they can be confident that they are taking advantage of all the cybersecurity features these tools have to offer, and that these systems are not exposing them to unnecessary vulnerabilities. Configuration services are helpful for optimizing the cybersecurity performance of firewalls, network switches, databases and other IT tools and systems.

**Managed services:** Especially in complex environments such as banks and credit unions, cybersecurity is not merely a matter of deploying the right tools and letting them run. Experienced IT professionals must also constantly monitor these solutions, watching carefully for any anomalous activity and taking appropriate action when a threat is detected. Smaller organizations, in particular, often lack the staff resources to appropriately monitor and maintain cybersecurity tools, and therefore may choose to outsource these services to a partner with the expertise to keep the organization safe.

**Phishing and ransomware services:** The number and sophistication of phishing attempts have increased in recent years. Further, research conducted by security provider Phishme indicates that 93 percent of phishing emails contain ransomware. Security providers can help banks and credit unions address these threats through services such as phishing intelligence and advanced user training.




The percentage of security incidents at financial institutions for which current and former employees are responsible.[2]

**Incident response:** No matter how carefully banks and credit unions work to protect their IT assets, breaches can still happen. When they do, it is important for these institutions to respond quickly and strategically, not only to root out the cause of the problem and prevent further damage, but also to fulfill their obligations to notify account holders of the breach and to preserve evidence. CDW works with partners that specialize in cybersecurity forensics and can help institutions rebound from incidents as quickly as possible. CDW's experts can also help organizations implement disaster recovery solutions.

## The Technology of Compliance

A number of IT solutions are either mandated by regulators or can help financial institutions meet their compliance and cybersecurity demands. These include:

**Wireless security and management:** With users routinely bringing two or more personal devices into work with them, it is crucial that banks and credit unions deploy sophisticated tools that give them visibility and control over their wireless networks. (Some users have even been known to bring wireless routers into the office to create their own mobile hotspots.) In addition to giving IT managers real-time visibility into their wireless networks, cloud-based wireless management platforms such as Cisco Meraki speed up deployment and allow financial institutions to quickly scale up their networks as they grow or merge with other organizations.

**Anti-virus/anti-malware software:** While practically all financial institutions run anti-virus and anti-malware tools in their IT environments, many do not take full advantage of the features that these tools offer. In some cases, organizations activate no more than 20 or 30 percent of optional features, missing out on benefits such as desktop firewalls, host-based intrusion prevention systems and tools that send alerts when potential threats are detected. Organizations can also improve the performance of their anti-virus and anti-malware tools by investing in "upstream" solutions such as next-generation firewalls, web gateways and cloud-enabled malware inspection and sandboxing tools that reduce the burden on endpoint protection software.

**Data storage and encryption:** Like all organizations, banks and credit unions must consider three factors when architecting data storage solution components: confidentiality, integrity and availability. Confidentiality requires that data be made available only to authorized users, while integrity refers to the need to maintain consistency, accuracy and trustworthiness over the lifecycle of the data. Availability simply means that data can be accessed when and where it is needed. Each of these three components is crucial to both cybersecurity and regulatory compliance. Additionally, regulations require that certain types of data be encrypted while in storage, while in transit or both.

**Authentication and access management:** Sophisticated access management tools allow banks and credit unions to

### The Growing Need for HPC in Security and Compliance

The use of high-performance computing (HPC) for security and compliance has generally been limited to the biggest financial institutions because they have the resources necessary to implement this technology. However, HPC solutions are becoming more mainstream, and smaller banks, as well as credit unions, are likely to consider adopting them over the next decade.

Here are three ways HPC can improve cybersecurity:

**Real-time traffic monitoring:** By simultaneously monitoring thousands of entry points on IT networks, HPC solutions can detect anomalies and shut down attacks before they inflict extensive damage.

**Advanced fraud detection:** Through real-time monitoring and analysis of millions of payment card transactions, HPC systems can detect suspicious patterns, and can also prevent legitimate transactions from being flagged as fraudulent.

**Past intrusion identification:** In addition to monitoring current activity, HPC tools can be used to explore past intrusions, giving organizations information on how hackers have circumvented their existing cybersecurity solutions.

**SOURCE:** [2]PricewaterhouseCoopers, "The Global State of Information Security Survey 2016," October 2015

operate according to "the principle of least privilege," meaning that users are able to access only the systems, resources and data they need to do their jobs, and no more. Authentication and access management tools make it simple for organizations to grant access by identity and user role, and can prohibit noncompliant devices from assessing critical applications. In addition, the auditing features of such solutions allow organizations to track who has accessed resources and when, providing valuable information in the event of a data breach.

**Data loss prevention (DLP) solutions:** DLP tools can track and protect data wherever it travels on an enterprise network — on desktops and mobile devices, in storage, through file-sharing and email, and even in the cloud. With a thorough risk assessment and an understanding of a company's business processes, IT managers can deploy DLP tools in a targeted manner so that they protect the most sensitive data in the enterprise.

## CDW: A Financial Industry Partner that Gets IT

For nearly 30 years, CDW has helped more than 15,000 banks, credit unions, capital markets firms and specialty financial services companies assess and improve their IT infrastructure. CDW's partnerships with leading IT manufacturers give these financial institutions access to the industry's leading technologies, and CDW's solutions experts have the knowledge and experience to help organizations choose the right security tools and create customized regulatory compliance plans.

The CDW approach to customer service includes:

- An initial discovery session to understand your goals, requirements and budget
- An assessment of your existing environment and definition of project requirements
- Detailed manufacturer evaluations, recommendations, future environment design and proof-of-concept
- Procurement, configuration and deployment of a security solution
- Ongoing product lifecycle support

**To learn more about how CDW solutions and services can help banks and credit unions secure their systems and data, visit CDW.com/security**

## The CDW Approach

### ASSESS

Evaluate business objectives, technology environments, and processes; identify opportunities for performance improvements and cost savings.

### DESIGN

Recommend relevant technologies and services, document technical architecture, deployment plans, "measures of success," budgets and timelines.

### DEPLOY

Assist with product fulfillment, configuration, broad-scale implementation, integration and training.

### MANAGE

Proactively monitor systems to ensure technology is running as intended and provide support when and how you need it.

## You and CDW

FORTINET®

The award-winning FortiGate® Network Security Platform delivers unmatched performance and protection while simplifying the network. Fortinet offers models for any deployment requirement, from the desktop FortiGate-20 series for small offices and retail networks to the FortiGate-5000 series for large enterprises, service providers, data centers and carriers. Every FortiGate product guarantees value and ease of management combined with the strongest protection in the industry.

TREND MICRO™

The Trend Micro™ Smart Protection Suites™ provides better, simpler, more flexible security. This connected suite delivers the best protection at multiple layers using the broadest range of anti-malware techniques available.

zscaler

Zscaler® protects your employees from malware, viruses, advanced persistent threats and other risks, and can also stop inadvertent or malicious leaks of your company's sensitive data. Our security services scan and filter every byte of your network traffic, including SSL-encrypted sessions, as it passes to and from the Internet. Give your executives instant insight into threats and get real-time recommendations on how to improve your security posture.



CDW® PEOPLE WHO GET IT™