Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

How technology is transforming the Financial Services Industry

An e-Book publication sponsored by

workday. Built for the future.®

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives. http://www.complianceweek.com

workday.
Built for the future.®

Workday is a leading provider of enterprise cloud applications for finance and human resources. Founded in 2005, Workday delivers financial management, human capital management, and analytics applications designed for the world's largest companies, educational institutions, and government agencies. Organizations ranging from medium-sized businesses to Fortune 50 enterprises have selected Workday.

Inside this e-Book

Internal auditors hear call to innovate, take up technology

The newest intelligence is calling on audit leaders to embrace their new normal—that nothing is normal—and innovate with technology to face it. **Tammy Whitehouse** has more.

For internal audit leaders, the new normal is to expect nothing to be normal. Transformation, especially as a result of technology, is inevitable.

That's the state of affairs based on a spate of new intelligence emerging from the annual General Audit Management conference of the Institute of Internal Auditors. The IIA's "pulse of the profession" study calls on internal auditors to transform their operations to remain relevant to stakeholders and improve their responses to constantly evolving business disruption.

According to the IIA's survey of more than 600 chief audit executives, directors, and senior managers, two-thirds regard agility and adaptability to change as important to the profession, yet less than half consider their departments to be highly agile. Less than half say they are fully or partially prepared to anticipate and react to disruption.

Audit leaders see some big obstacles to agility, like inadequate resources, organizational complexity, and "overly traditional" expectations of the internal audit function on the part of executive management. Yet, the survey group doesn't give itself particularly strong marks on innovation activities that might improve agility, says Jim Pelletier, vice president at the IIA.

Only 13 percent strongly agree, for example, that their internal audit functions quickly adapt to new technologies or processes. Only 32 percent strongly agree that their particular department challenges the status quo, and only 36 percent strongly agree that they seek new ways to gather audit evidence. "We're talking a lot about innovation and agility," says Pelletier. "It's an internal audit transformation imperative. There are growing expectations of the internal audit function, so it's an opportunity for internal audit to play a more critical role in the organization in support of the board."

PwC's annual "state of internal audit" study calls on internal auditors to get more comfortable with technology—both understanding how it produces risk for the entity and how internal auditors can better leverage it to identify and help mitigate those risks. The firm's poll of more than 2,500 audit professionals and audit stakeholders indicates a good number recognize emerging technologies that will be key to their operations in the future but haven't adopted them yet.

One-fourth, for example, believe robotics will have a significant impact on the organization over the next three years, but only 2 percent of internal audit functions are using robotics, and 20 percent plan to adopt the technology in the next few years. In addition to robotics, PwC identifies seven other categories of technology that deserve more attention from internal auditors in the near future, including drones, three-dimensional printing, artificial intelligence, blockchain, virtual reality, augmented reality, and the internet of things.

Innovation is a reality in most companies today, says Lauren Massey, a partner in risk assurance at PwC, and velocity of change and innovation only compound the imperative. The study identifies internal audit functions that are most advanced in their journey toward adopting new technologies as those that are also most valued by their stakeholders.

Meanwhile, Crowe Horwath and the Internal Audit Foundation focused their recent poll on cyber-security and the extent to which internal auditors are keeping pace with the demands. The report describes cyber-security as one of the most significant risks facing business today.

Gauging internal audit engagement on cyber-risks, the survey found 78 percent of internal auditors have visibility into the organization's information security plan looking one to three years out, and two-thirds are part of a formal information security steering committee. More than half of internal audit teams, however, do not have adequate

"We as humans tend to rely on the status quo, but people need to become comfortable at being uncomfortable. We have to innovate, identify problems, and solve problems."

Brian Christensen, EVP, Protiviti

access to information security assessment results and incident-related information.

The results also suggest that it may stem from a lack of connection with information security and information technology functions in organizations. The data showed internal auditors have stronger relationships with compliance and risk management offices, but not as much of a working relationship with information security or IT staff.

Chris Wilkinson, a principal at Crowe Horwath and co-author of the white paper, says survey results also suggest internal audit functions have made strides in helping organizations build up controls designed to prevent cyber-breaches, but have made less progress with detective controls and even less in incident response. "As internal audit professionals, we need to focus on all three," he says. "They all play an important part in the overall cyber-security posture of the organization."

Internal audit teams have been increasing their capabilities internally to deal with cyber-risks, says Wilkinson. But finding internal audit talent, especially in the technology areas, has been an ongoing challenge for chief audit executives. The data suggests one way audit leaders can leverage talent internally is by working on relationship building with the IT and information security functions, he says. "Building more collaborative relationships is absolutely essential to this process," he says.

Data analytics, another technology hot button, also garnered significant attention in this year's crop of internal audit studies. Protiviti's newest annual study says internal audit is making some inroads in adopting advanced analytics technologies, but the overall maturity level is considered low. The firm says its results suggest many audit functions are likely using analytics tools as "point solutions" rather than as part of a broader initiative to leverage the technology throughout the audit process.

Brian Christensen, executive vice president at Protiviti, says he sees firsthand the need for internal auditors to advance along the technology curve. Based in the Phoenix area, he's a witness to self-driving cars in his own neighborhood, the risks of which became obvious enough after a recent pedestrian fatality involving a driverless car. "This is what's happening," he says. "This is the pace of change."

Auditors are under increasing pressure to provide actionable insight to boards of directors and executive management, which suggests a need for faster audit outcomes, or even continuous auditing, says Christensen. "The high-level results say we're not moving fast enough," he says. "The pace of change in the internal audit function is not meeting the expectations. That's provocative."

Finding and leveraging talent remains a big obstacle, Christensen acknowledges, which makes it a high priority for audit leaders. "That's the call to action that's challenging our profession," he says. "We as humans tend to rely on the status quo, but people need to become comfortable at being uncomfortable. We have to innovate, identify problems, and solve problems."

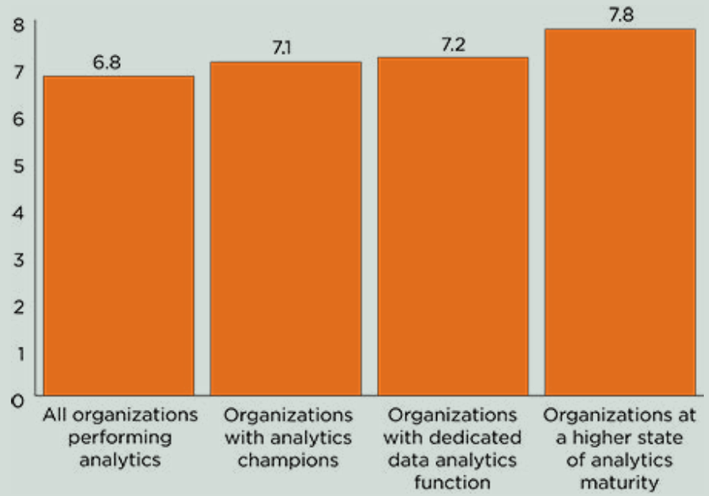
A new book by Grant Thornton and the Internal Audit Foundation tackles the challenges of data analytics in even greater depth. The very title promises to provide a roadmap to help internal auditors expand their capabilities in analytics, exploring how to harness the technology to address risks and controls.

Meredith Murphy, a director at Grant Thornton and co-author of the book, says this particular survey found more than 90 percent of internal auditors agreeing on the value of data analytics, yet less than 40 percent actually leveraging analytics. As such, the book puts some emphasis on how internal auditors can build the case internally for increased uptake in organizations, whatever the obstacles or barriers audit leaders might face.

"The most critical component to drive analytics success is people," says Murphy. "Data holds insight, but it's people that ensure the data generates value." The book tells audit executives it's up to them to understand the stakes and forge the path forward. ■

Analytics in auditing is a game changer

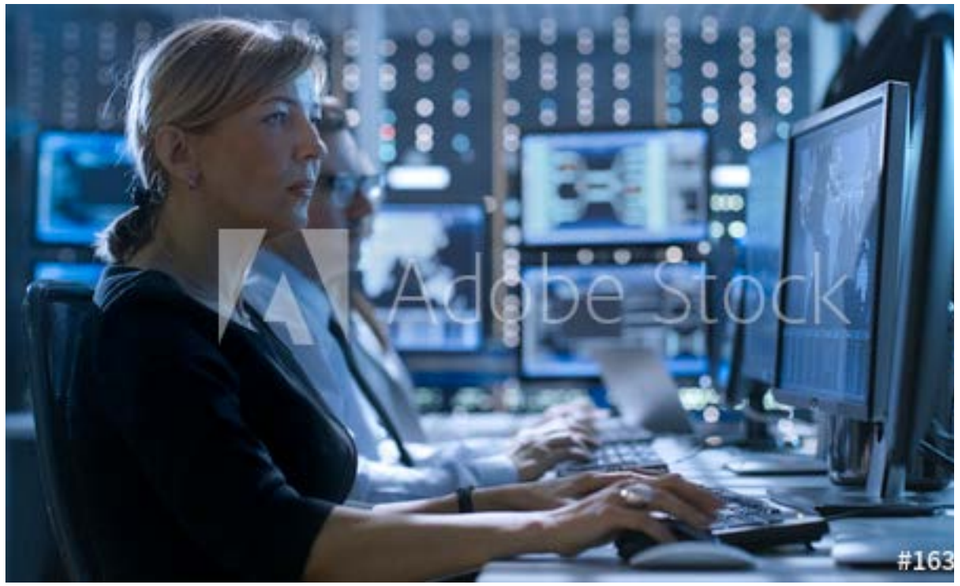
Protiviti asked respondents to its "Internal Audit Capabilities and Needs Survey" to rate on a scale of 1 to 10 (10 a high level of value and 1 little or no value) the level of value that their internal audit department receives from utilizing data analytics as part of the audit process.



Top 8 audit plan priorities for 2018:

- Fraud risk management
- Cyber-security risk/threat
- Vendor/third-party risk management
- Enterprise risk management
- New revenue recognition standard
- Agile risk and compliance
- Auditing corporate culture
- Cloud computing

Source: Protiviti



Cyber-security attestations now required for leadership at NY's financial firms

Tough new cyber-security regulations, crafted in New York, require board members and senior officials to not just talk the talk. **Joe Mont** has more.

One of the nation's most comprehensive cyber-security compliance regimes is coming into cleared focus in New York.

Beginning on Feb. 15, a staggered slate of compliance deadlines began affecting financial services firms, including some of the world's biggest banks. First up: compliance certification filings and executive/director attestations. Covered entities were required to submit a statement of compliance, covering the prior calendar year, filed electronically via a recently launched New York Department of Financial Services cyber-security portal.

Financial Services Superintendent Maria Vullo also announced that DFS will now incorporate cyber-security in all examinations, adding questions related to cyber-security to "first day letters," notices the Department issues to commence its examinations of financial services companies, "including examinations of banks and insurance companies for safety and soundness and market conduct."

"The DFS compliance certification is a critical governance pillar for the cyber-security program of all DFS regulated entities," Vullo said in a statement. "DFS's regulation requires each entity to have an annual review and assessment of a program's achievements, deficiencies, and overall compliance with regulatory standards, and the DFS cybersecurity portal will allow the safe and secure reporting of these certifications. DFS's goal is to prevent cyber-security attacks, and we therefore will now include cyber-security in all DFS examinations to ensure that proper cyber-security governance is being practiced by our regulated entities."

New York's first-in-the-nation cyber-security regulation became effective March 1, 2017, with a staggered set of deadlines. The agency's regulations will impose a host of new security, personnel, attestation, and reporting requirements.

Those rules will require that banks, insurance companies, and other financial services institutions overseen by the NYDFS establish a cyber-security program. Firms are also expected to adopt a written cyber-security policy; designate a chief information security officer responsible for implementing, overseeing, and enforcing its new program and policy; and have policies and procedures designed to ensure the security of information systems and non-public information accessible to, or held by, third parties.

Each covered entity will be required to implement and maintain a written cyber-security policy detailing policies and procedures for the protection of information systems and the non-public information stored on those systems. At a minimum, they must address:

- information security;
- access controls and identity management;
- business continuity and disaster recovery planning;
- systems and network monitoring;
- physical security and environmental controls;
- customer data privacy;
- vendor and third-party service provider management;
- risk assessment; and
- incident response.

A cyber-security policy, prepared on at least an annual basis, must be reviewed by a firm's board of directors and approved by a senior officer.

The CISO of each covered entity is required to develop a report, at least bi-annually, that is presented to the board of directors or equivalent governing body and made available to the superintendent upon request.

This report must assess the confidentiality, integrity, and availability of the firm's information systems; detail exceptions to the cyber-security policies and procedures; identify cyber-risks; assess the effectiveness of the cyber-security program; propose steps to remediate any identified inadequacies; and include a summary of all material cyber-security events during the time period addressed by the report.

The cyber-security program should, at a minimum, include penetration testing of information systems at least annually and vulnerability assessments on a quarterly basis. The program must include audit trail systems that track and maintain data and allow for the complete, accurate reconstruction of all the financial transactions, and accounting necessary to detect and respond to a cyber-security event.

Firms must also implement written policies and procedures designed to ensure the security of information systems and non-public data accessible to, or held by, third parties doing business with them. On an annual basis, each firm will be required to provide the NYDFS superintendent a written statement certifying that they are in compliance with all requirements. The identification of any material risk of imminent harm relating to its cyber-security pro-

Key dates under New York's cyber-security regulation

Feb. 15, 2018: Covered Entities are required to submit the first certification under 23 NYCRR 500.17(b) on or prior to this date.

March 1, 2018: One year transitional period ends. Covered Entities are required to be in compliance with the requirements of sections 500.04(b), 500.05, 500.09, 500.12 and 500.14(b) of 23 NYCRR Part 500.

Sept. 3, 2018: Eighteen month transitional period ends.Covered Entities are required to be in compliance with the requirements of sections 500.06, 500.08, 500.13, 500.14(a) and 500.15 of 23 NYCRR Part 500.

March 1, 2019: Two year transitional period ends. Covered Entities are required to be in compliance with the requirements of 23 NYCRR 500.11.

The Department has extended the initial period for making the filing of the Notice of Exemption required by 23 NYCRR 500.19(e) until October 30, 2017. Covered Entities that have determined that they qualify for a limited exemption under 23 NYCRR 500.19(a)-(d) before October 1, 2017, are now required to file a Notice of Exemption on or prior to this date.

The Department reminds Covered Entities that Notices of Exemption should be filed electronically via the DFS Web Portal (accessible by clicking the orange box marked "Cybersecurity Filing" at the top of this page). You will first be prompted to create an account and log in to the DFS Web Portal, then directed to the filing interface. That website also contains a copy of the Cybersecurity Regulation and a set of Frequently Asked Questions.

Source: NYDFS

gram requires that the superintendent be notified within 72 hours.

Jeffrey Taft, a partner in the law firm Mayer Brown's financial services regulatory and enforcement group, says that many covered firms have been stressed out by the now-implemented attestation requirement. His advice is to leverage an in-house hierarchy that probably already exists by imposing a network of sub-certifications. This is especially important when directors and senior management may not have suitably extensive backgrounds in information technology.

"There may be a lot of areas where they have overall responsibility, but not day-to-day responsibility," Taft says. "They are relying on those who work for them, on a daily basis, to keep them informed and make sure the trains are running on time."

Taft explained the process. "In some companies, they have come up with a process where the people beneath them are certifying they are compliant with the rule, in terms of what they are responsible for, and those sub-certifications form the basis by which the ultimate certifier makes their attestations to the DFS," he said. "That's a good model. It creates a level of accountability throughout the system. If the certification turns out to be problematic, the person who made it can go back and explain that they were relying on a very detailed chain of command. This also tells the DFS that you were taking these requirements very seriously, had a system in place, and assigned an individual level of accountability in the organization regarding cyber-security."

Taft compares this approach to how many public firms approach Sarbanes-Oxley requirements and demand for director attestation.

Mark Krotoski, a partner and co-leader of Morgan Lewis's privacy & cyber-security practice, previously served as national coordinator for the Computer Hacking and Intellectual Property Program in the Department of Justice's Criminal Division. In his view, much of the compliance requirements involved the evolution and application of existing protocols.

"This has certainly been a transitional, phased-in process, he says. "In many instances my clients already have some of the features that are called out by this regulation. Additionally, they have been adapting their prior policies and programs to comply with some of the specific requirements that the Department imposed. They may already have many of these features, but now they need to re-designate and reclassify them in order to be in compliance."

As firms do an in-house assessment to see if they have the in-house capabilities required by the new rules, many are finding they need to bring in outside vendor on both the technical and legal sides of the task before them, Taft says, stressing that cyber-security "has to be tailored to particular circumstances" of a covered entity.

What companies need to do is assess how are they going to deal with the costs.

"The firms covered by this regulation include financial institutions, financial service organizations, and insurance companies. Many that fall under those three categories already have some form of program in place," Taft says. "When it comes to cost, what some companies are struggling with is the cost of compliance versus the cost of security. In some instances, they already had strong programs; now they need to ensure that they are in compliance with these new standards."

The attestation demand, already causing worry at many firms, will only grow more complex. Upcoming deadlines are going to include requirements for penetration testing, risk assessments, multi-factor authentication, and training and monitoring.

One important question still awaits an answer: What will enforcement look like?

"This is an area of overlapping—and in some instances conflicting—requirements," Taft says. Nearly all states and most federal agencies already have cyber-security and breach notifications in place. Others, including the Securities and Exchange Commission, are expected to deliver new requirements very soon. For some financial firms, there are also international requirements piled on.

"Whenever you have an enforcer at the state or federal level, you are trying to read the tea leaves of what their first enforcement actions will be and what they mean," Taft says. His advice, whether they come out swinging or not, is to make sure your firm can attest to a "Reasonable good faith effort."

One specific section that separates New York's rules from other cyber-security regulations is that it takes advanced authentication to the next level.

Section 500.12 (Multi-Factor Authentication) recommends authentication procedures that rely on anomaly detection and/or changes in normal use patterns.

Istvan Molnar, compliance specialist at Balabit, a security firm specializing in IT security systems, says some of the most effective anomaly detection strategies that organizations can implement in order to be in compliance include using behavioral biometrics.

"Nowadays, we don't define biometric characteristics as narrowly as we did a few years back," he says "Apart from the usual fingerprint and retina scans, there are also so-called, digital biometric identifiers. These are regularly occurring patterns and constantly performed actions that can reflect an individual's unique behavior. These characteristics are bound to an individual, impossible to mimic or reproduce yet easily distinguish one user from another."

Anomaly detection based on digital behavior, also known as User Behavior Analytics, is becoming increasingly important, he says, breaking the process into three stages.

First: Generate a custom profile for each user based on collected, digital biometric identifiers. This will act as a baseline to identify a specific user.

Second: Use "continuous authentication" to continually compare the baseline profile to actual behavior during the whole period of time the user is operating within the security perimeter.

Third: When the difference between the baseline and the current behavior exceeds an established tolerance threshold and risk scoring, assess the type of data accessed and provide evidence of illicit, insider activity to security teams to judge the criticality of the event. ■

Financial services seeks stronger cyber-safeguards

A rising tide of sophisticated cyber-thievery has the financial services industry scrambling to improve its electronic defenses. But can they find a solution before the next big heist? **Jaclyn Jaeger** has more.

In February 2016, cyber-thieves stole $81 million from the Central Bank of Bangladesh by sending fraudulent messages through the SWIFT payment network. The heist sounded a wake-up call that if financial services firms wanted to protect themselves against similar acts of thievery, they would have to evolve their defenses, and quickly.

First, some background. SWIFT is short for the Society for Worldwide Interbank Financial Telecommunication, a global industry cooperative. More than 11,000 financial institutions in more than 200 countries and territories around the world use SWIFT's messaging platform, averaging some 26 million SWIFT messages per day, and more than six billion in 2016, according to SWIFT figures.

The Bank of Bangladesh attack opened a Pandora's Box, as criminal groups ramped up copycat attacks. SWIFT stopped short of disclosing the number of attacks, identifying the banks involved or disclosing how much money was stolen, but details of some of these attacks have become public. Far Eastern International Bank, for example, lost $500,000 in a cyber-heist, believed to have been launched by a North Korean Lazarus hacking group, suspected to be the same hacking group behind the Bangladesh heist. In another reported attack, Nepal's NIC Asia Bank lost $580,000 in a cyber-heist in November 2017.

In all these attacks, security weaknesses in the compromised banks enabled cyber-thieves to gain administrator access to the banks' payment environments, according to the SWIFT report. With this access, hackers not only stealthily monitored the banks' operations—sometimes for months—but also were able to modify security defenses and the operation of software to enable their attacks by updating firewalls and bypassing security features.

SWIFT Chairman Yawar Shah highlighted the urgency of the situation in remarks at last year's London Business Forum: "The disruptive forces of fraud and cyber have always existed and had to be dealt with in our industry; what is different now is that these threats are more organized, more sophisticated, and more global than ever before."

As part of its efforts, SWIFT recently published a 16-page report, co-authored by the cyber-security division of BAE Systems, that describes how today's cyber-criminals are infiltrating banks' systems and networks and provides best practices for better securing them.

"The inevitable criminal focus on the heart of the financial system means that the financial services industry needs to ensure it has effective cyber-defenses against well-funded, motivated, and organized attackers," said James Hatch, BAE Systems director of cyber-services.

Cyber-security safeguards

Those in the financial services industry generally acknowledge that stronger safeguards against cyber-threats necessitates industry-wide collaboration, which is the impetus behind SWIFT launching its Customer Security Program (CSP), which aims to improve information-sharing throughout the financial services community and is comprised of its Customer Security Controls Framework.

SWIFT's Customer Security Controls Framework introduces both mandatory and advisory security controls. The deadline for SWIFT users to have implemented and self-attested to the 16 total mandatory controls was Dec. 31, 2017, and they must self-attest at least annually thereafter through SWIFT's KYC Registry.

The SWIFT framework contains 27 controls in total, divided by eight principles, focused on the following three core measures, as summarized in the SWIFT/BAE report:

Secure your environment. Embed security into the design of the bank's network architecture, including physical security measures—such as limiting access rights to authorized personnel as it concerns sensitive areas and ensuring processes are in place to actively control and monitor who is accessing those areas. Additionally, authorized personnel must be properly screened and trained.

Banks should further ensure that they have in place robust and clearly defined perimeter security, with appropriate prevention measures like firewalls and filters, and detection capabilities in case of intrusion. Through the construction of multiple barriers, they should segregate internal networks according to business needs and risk requirements and actively monitor internal networks.

The bank's most critical systems should be isolated from the internet, and a further layer of defenses and detection measures should be deployed. "As a matter of course, you should install the latest versions of anti-virus and system software and immediately implement the latest security updates," the SWIFT/BAE report states.

Know and limit access. After building defenses to prevent hackers coming through the front door, operating procedures and processes must be put in place to then limit and protect administrator and system privileges. This demands the implementation of strong ID management, with strict and actively managed profile and password rules to ensure basic access controls. Additional access controls—such as two-factor authentication across all sensitive or critical applications—should be used to provide another layer of defense.

In addition, banks must identify and protect access rights to all critical systems like interfaces to SWIFT and other payment gateways. "These access rules should clearly allocate rights and capabilities to separate roles and ensure that no single operator can—intentionally or otherwise—open systems to potential abuse," the SWIFT/BAE report states.

Detect and respond. Having in place adequate intrusion-detection capabilities is the third core measure. Banks should actively monitor networks and systems activity, including interfaces to SWIFT, for unusual behavior—such as users logging in at random times of the day or from new or unknown systems, or multiple failed password attempts. Where gaps in capabilities or layers of defense are identified, consider employing the help of cyber-security professionals to ensure the local environment is sanitized and properly defended with the latest anti-virus applications.

> "The disruptive forces of fraud and cyber have always existed and had to be dealt with in our industry; what is different now is that these threats are more organized, more sophisticated, and more global than ever before."
>
> Yawar Shah, Chairman, SWIFT

To be clear, SWIFT is focused on the infrastructure connected to its messaging platform, and thus its Customer Security Controls Framework is "not intended as a be-all and end-all framework for all banks," says Steven Grossman, vice president of strategy at cyber-security software provider Bay Dynamics. "It's all about strengthening the security of all 11,000 banks as they connect to and use the SWIFT messaging platform and making sure they know who is doing those transactions."

"This entails strong authentication, monitoring the behavior of users with tools such as user and entity behavior analytics, making sure there's a segregation of privileges so one person doesn't have too much access and control, implementing proper segmentation between the banks and SWIFT environment, and more," Grossman adds. "It's really about making sure that those parts of the banks that are connected to the SWIFT platform, and the transactions they perform, have the strongest security at all times."

Counterparty risk

Financial institutions must consider not just their internal cyber-security risks, but their interactions and relationships with counterparties as well. Understanding counterparties' credit and compliance risks should be a determining factor in whether and how to do business with them, and cyber-considerations should form an integral part of these routine know-your-counterparty processes, the SWIFT/BAE report states.

As of January 2018, banks that use SWIFT's messaging platform are now able to assess who they are doing business with by requesting their self-attestations against SWIFT's Customer Security Controls Framework to ensure counterparties are taking the necessary precautions and protections.

"Financial institutions in major economies and high-risk jurisdictions are increasingly looking to adopt financial crime compliance tools to show correspondent banks that they have strong controls in place," says Paul Taylor of SWIFT's financial crime compliance division. "This enables them to be a lot more transparent in terms of the controls they have and the lists they are screening against," he says.

That should provide some comfort to correspondent banks that their bank counterparties have security controls in place. "The argument there is if you're a counterparty that doesn't have risk and control solutions in place and a good framework and good diligence around how that works, then you might not necessarily be an attractive counterparty to continue business with," Taylor says.

Findings from a recent anti-money laundering and sanctions compliance survey conducted by AlixPartners speaks to that point. According to that survey, 63 percent of 361 respondents from financial institutions said they've experienced de-risking in their operations in one form or another. Financial institutions have sought to—and continue to—reduce perceived risk by eliminating portfolios, counterparties, or entire lines of business.

For its part, SWIFT has introduced a new module, Correspondent Monitoring, to help banks address money-laundering risk within correspondent banking networks. Correspondent Monitoring allows banks to analyze their SWIFT message traffic to uncover unusual activity patterns and risk exposures within their correspondent banking networks. For example, a user can find out whether it was in receipt of transactions originating in a country considered high risk or subject to sanctions via correspondents operating in a low-risk jurisdiction.

Also related to correspondent banking due diligence, the Wolfsberg Group, a non-governmental association of thirteen global banks, recently announced significant revisions to its correspondent banking due diligence questionnaire (DDQ) in response to evolving regulatory expectations and industry practice, which will be released in February 2018.

Concurrently, SWIFT announced that it would be aligning its KYC Registry with the new Wolfsberg DDQ for correspondent banks. KYC Registry members can now answer every Wolfsberg DDQ question directly on the KYC Registry platform, increasing transparency and streamlining due diligence processes.

Aside from cyber-security processes and KYC diligence, information-sharing between banks is another vital part of fending off a cyber-attack. Thus, SWIFT is urging banks that are targeted or breached to share all relevant information and alert SWIFT as soon as possible, so that it can share anonymized information on indicators of compromise in the SWIFT environment to limit further damage. ■

Mandatory security controls	Control objective
1. Restrict Internet Access and Protect Critical Systems from General IT Environment	
1.1 SWIFT Environment Protection	Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.
1.2 Operating System Privileged Account Control	Restrict and control the allocation and usage of administrator-level operating system accounts.
2. Reduce Attack Surface and Vulnerabilities	
2.1 Internal Data Flow Security	Ensure the confidentiality, integrity, and authenticity of data flows between local SWIFT-related applications and their link to the operator PC.
2.2 Security Updates	Minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.
2.3 System Hardening	Reduce the cyber attack surface of SWIFT-related components by performing system hardening.
3. Physically Secure the Environment	
3.1 Physical Security	Prevent unauthorised physical access to sensitive equipment, workplace environments, hosting sites, and storage.
4. Prevent Compromise of Credentials	
4.1 Password Policy	Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy.
4.2 Multi-factor Authentication	Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication.
5. Manage Identities and Segregate Privileges	
5.1 Logical Access Control	Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts.
5.2 Token Management	Ensure the proper management, tracking, and use of connected hardware authentication tokens (if tokens are used).
6. Detect Anomalous Activity to Systems or Transaction Records	
6.1 Malware Protection	Ensure that local SWIFT infrastructure is protected against malware.
6.2 Software Integrity	Ensure the software integrity of the SWIFT-related applications.
6.3 Database Integrity	Ensure the integrity of the database records for the SWIFT messaging interface.
6.4 Logging and Monitoring	Record security events and detect anomalous actions and operations within the local SWIFT environment.
7. Plan for Incident Response and Information Sharing	
7.1 Cyber Incident Response Planning	Ensure a consistent and effective approach for the management of cyber incidents.
7.2 Security Training and Awareness	Ensure all staff are aware of and fulfil their security responsibilities by performing regular security training and awareness activities.

Source: SWIFT

COMMUNITY VOICES

How Financial Services Firms Can Shift from Data Hoarding to Decision-Making

by Chris Artemenko, on Industries

Chris Artemenko is the Workday strategic advisor for the financial services industry which includes banking, insurance, investment management, and other financial services companies. She works with prospects and clients, advocating for the needs of the financial services industry within Workday. The role helps both Workday and our clients understand each other better and have a deeper partnership to support the growth of this industry through technology.

Today, many financial services institutions are hoarding significant amounts of operational data, including data about their people and finances. The volume of data organizations store will only increase as data continues to grow in importance. By 2025, IDC estimates that the data created and replicated in the world will reach 163 zettabytes, or 163 trillion gigabytes. That's roughly 3.3 quadrillion four-drawer file cabinets. Annually.

Contrast this to a time in the not-too-distant past when companies weren't storing data beyond what was legally required or essential to running their businesses. In fact, due to system constraints and physical storage limitations, storing large amounts of data simply wasn't possible.

Yet here's the rub—much of the internal data around finance and human resources (HR), which can be used to better run and grow the business, isn't actionable because it can't be combined with other available data or easily analyzed at all. While financial services firms have innovated their front office with new technologies to meet rising customer expectations, they may have overlooked the needs of their internal customers—their employees—who are operating on outdated systems that store data in siloes. Because of this, many organizations and their employees are at risk of overlooking critical information as they become increasingly overwhelmed with data without the means to handle it.

But with the right strategy and systems to make sense of information, you can turn valuable finance and HR data from a collection of facts into actionable insights.

Distinguish Value from Noise

As a financial services firm, where do you start in determining what data you need and how to use it? At the core of every business are its people, finance, and operations, so looking at data from these dimensions is a good beginning. This can be accomplished by identifying your business problem or goal, and then determining what data you have available that can be used to make informed decisions about those challenges.

For example, maybe your organization is a bank with a goal to improve customer satisfaction and increase customer loyalty. Your branch employees, who serve on the front lines of customer communications, are key to this. By comparing workforce data with operational data, organizations can better understand how employee performance correlates with branch performance and then recommend relevant training to get employees up-to-speed.

You also want to retain employees who excel at customer communications and loyalty. If you have the right HR and finance analytics capabilities, you'll be able to identify high performers at risk of leaving based on historical data related to performance, tenure, and compensation.

> Making sense of information requires a unified system that can not only disaggregate data to the line item level but can also pull in different data sources.

Improve the Back-End

The data deluge problem isn't just about the amount of internal, operational data being stored, but also the level of granularity available. The finance and HR teams of many institutions still operate on outdated systems that are only able to store aggregate data with complex details summarized. While these systems may be sufficient for the purpose of financial reporting, they're unable to keep up with the level of complexity needed to drive business decisions.

Making sense of information requires a unified system that can not only disaggregate data to the line item level but can also pull in different data sources. This way, financial services firms can get a comprehensive view into their organizations by comparing and analyzing performance across products, customer segments, regions, and other dimensions. Combining all this data at the lowest level of granularity provides better insight into cash inflows and outflows—as well as your key ratios—to better manage risk and drive profitability.

Financial institutions also need a comprehensive view of all this granular data in a real-time dashboard. For instance, a branch or lending manager could use a credit risk dashboard that details loan charge-offs and delinquencies to determine what changes need to be made to meet revenue goals or to identify a disruptive pattern. Or, a financial institution could use benchmarking capabilities to understand how they compare to companies of a similar size or industry, helping them understand their strengths and weaknesses in relation to other organizations.

Data can be a blessing or a burden. Don't hoard your data. With the right strategy and the technology to support it, your organization can hone in on the right data to make decisions that will move the needle forward.

+1-925-951-9000 | +1-877-WORKDAY (+1-877-967-5329) | Fax: +1-925-951-9001 | workday.com

Collaboration enhances risk management in financial services

The OCC recently endorsed collaboration between banks as a way to reduce costs on managing third-party risk, and compliance officers are more than ready for it. **Jaclyn Jaeger** has more.

Collaboration among financial institutions is how many banks today are enhancing their third-party risk management programs.

Although collaboration is not a new concept among banks, the Office of the Comptroller of the Currency (OCC) recently endorsed it as an acceptable means for banks to alleviate the significant cost burdens associated with a third-party risk management (TPRM) program. That endorsement came in the form of a supplemental guidance (Bulletin 2017-21) the OCC issued in June, which discussed, among other areas, the use of collaboration for managing third-party relationships.

The OCC guidance should come as a welcome development for compliance and risk officers in the financial services industry, as it provides banks substantial flexibility to enhance their own individual third-party risk management programs. "They're really embracing a best-practices approach and one that gives us all more guidance and instruction on what we need to be doing to make sure the regulators are happy," Brad Keller, senior director of third-party strategy at Prevalent, said during a recent Compliance Week Webinar on the OCC guidance.

OCC Bulletin 2017-21 was issued in response to questions submitted by banks as a follow-up to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance." Issued in 2013, Bulletin 2013-29 provides a comprehensive framework for banks for assessing and managing risks associated with third-party relationships.

In Bulletin 2017-21, in response to questions about collaboration, the OCC responded that when banks use the same service providers to secure or obtain like products or services, they may collaborate to meet certain expectations described in OCC Bulletin 2013-29—such as performing due diligence, contract negotiation, and ongoing monitoring responsibilities. "Collaboration can leverage resources by distributing costs across multiple banks," the OCC stated.

The OCC further stated that banks may take advantage of various tools designed to help them evaluate third-party service provider controls. In general, these types of tools offer standardized approaches to perform due diligence and ongoing monitoring of third-party service providers by having participating third parties complete common security, privacy, and business resiliency control assessment questionnaires. Once third parties complete the questionnaires, the results can be shared with banks.

To gauge how banks are embracing collaboration as outlined in Bulletin 2017-21, Compliance Week conducted an online poll during the Webinar. In that poll, the plurality of respondents (44 percent) said their institution "fully understands the benefits of a more collaborative approach and is investigating how to leverage them in our TPRM program."

The second highest number of respondents (33 percent) said that their "institution is unsure how to utilize/execute a collaborative approach in our TPRM program," while another 15 percent answered that their institution is "actively engaged in collaboration with other banks with whom we share common third-party service providers." Nine percent said their institution is "unsure of the actual benefits from a collaborative approach."

Executing collaborative efforts. Compliance officers and risk officers at banks seeking guidance on how to execute a collaborative approach in their TPRM program may want to check out a policy paper issued by the OCC in 2015. That policy paper described a variety of ways that banks currently collaborate, including through the exchange of information and ideas.

Other collaborative efforts used by banks, the OCC said, include:

- Jointly purchasing materials or services;
- Sharing back-office or other services;
- Sharing a specialized staff member or team;
- Jointly owning a service organization;
- Participating in disaster mitigation agreements; and
- Jointly providing/developing products and services.

"They're really embracing a best-practices approach and one that gives us all more guidance and instruction on what we need to be doing to make sure the regulators are happy."

Brad Keller, Senior Director, Third-Party Strategy, Prevalent

OCC Bulletin 2017-21 also discussed collaboration opportunities to help mitigate cyber-threats to banks, as well as to their third-party relationships, including engaging with information-sharing organizations. "Banks participating in information-sharing forums have improved their ability to identify attack tactics and successfully mitigate cyber-attacks on their systems," the OCC noted.

The OCC cited a variety of information-sharing organizations that help banks monitor cyber-threats and vulnerabilities and enhance risk management and internal controls. These organizations include the Financial Services Information Sharing and Analysis Center (FS-ISAC), the U.S. Computer Emergency Readiness Team (US-CERT), and InfraGard, among others. Banks also may use the FS-ISAC to share information with other banks, the OCC said.

Bank-specific responsibilities. The OCC has repeatedly warned, however, that collaboration cannot be used to satisfy all oversight responsibilities, particularly third-party risk management processes that must be tailored to each bank's specific needs. Examples of individual bank-specific responsibilities include:

» Integrating the use of product and delivery channels into the bank's strategic planning process and ensuring consistency with the bank's internal controls, corporate governance, business plan, and risk appetite.
» Assessing the quantity of risk posed to the bank through the third-party service provider and the ability of the bank to monitor and control the risk.
» Implementing information technology controls at the bank.
» Ongoing benchmarking of service provider performance against the contract or service-level agreement.
» Evaluating the third party's fee structure to determine if it creates incentives that encourage inappropriate risk taking.
» Monitoring the third party's actions on behalf of the bank for compliance with applicable laws and regulations.
» Monitoring the third party's disaster recovery and business continuity time frames for resuming activities and recovering data for consistency with the bank's disaster recovery and business continuity plans.

"Banks participating in information-sharing forums have improved their ability to identify attack tactics and successfully mitigate cyber-attacks on their systems."

OCC Bulletin 2017-21

Furthermore, the OCC stressed that any collaborative activities among financial institutions must comply with antitrust laws, and that banks should take appropriate steps to ensure compliance with these laws. In this regard, financial institutions should review the Federal Trade Commission and U.S. Department of Justice's joint "Antitrust Guidelines for Collaborations Among Competitors."

Ongoing monitoring. Another focus area for examiners is what banks are doing from an ongoing monitoring standpoint for each of the bank's third-party service providers that support critical activities, which Bulletin 2017-21 also discussed in broad detail.

OCC's 2013 guidance provides specific criteria that a bank's board and management may use to identify its critical activities, but some examples can include significant bank functions—such as payments, clearing, settlements, and custody—or significant shared services, such as information technology.

Other potential critical activities may be those that:

» Could cause the bank to face significant risk if a third party fails to meet expectations;
» Could have significant bank customer impact;
» Require significant investment in resources to implement third-party relationships and manage risks; or that
» Could majorly effect a bank's operations if the bank must find an alternative third party or if the outsourced activities must be brought in-house.

When a bank does not receive all the information it seeks about third-party service providers that support the bank's critical activities, the OCC said it expects the bank's board of directors and management to:

» Develop alternative ways to analyze these critical third-party service providers;
» Establish risk-mitigating controls;
» Be prepared to address interruptions in delivery—multiple payment systems and multiple telecommunications lines in and out of critical sites, for example;
» Ensure that contracts meet the bank's needs; and
» Retain appropriate documentation of all related decisions and efforts to obtain information.

Ongoing monitoring involves looking at not just the bank's third parties' threat environments concerning areas outside of contractual requirements, but also the threat environment of the third parties' sub-contractors. Areas to monitor could include legal activity that could impair the third party's ability to deliver services; regulatory actions; financial viability; operational issues like a merger or acquisition or any senior-leadership changes; or brand and reputational issues.

"Ongoing monitoring lets you address issues before they become events," said Keller, who has been developing and leading risk management programs for more than 25 years. For example, a third-party vendor doesn't have to alert a bank to a data breach that occurred at a data center other than where the bank's sensitive data is stored, but that's something the financial institution ought to know, because both locations likely employ the same IT security controls, he said. Thus, the bank's chief compliance or risk officer should have that conversation with that third-party vendor to determine what they're doing to address that threat.

Another critical piece to ongoing monitoring is documentation. Examiners are going to want to see how the bank's compliance function is executing ongoing monitoring and evaluating third parties' processes against the bank's specifically identified criteria, Keller said.

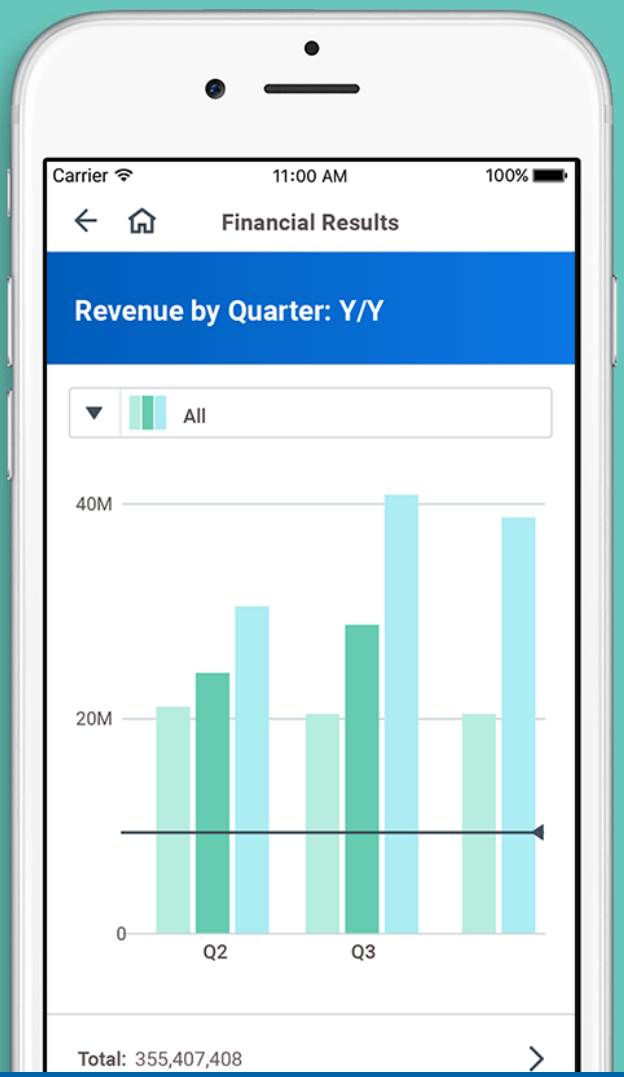
"No matter how robust the bank's third-party risk management processes are, if those efforts are not documented and compliance cannot provide actual evidence of that process, the OCC, for all intents and purposes, will treat those efforts as non-existent. "It becomes something they view more as aspirational on behalf of the institution, as opposed to something they can say the institution is, in fact, actually doing," Keller said.

A third helpful guidance for compliance and risk professionals in financial services to peruse is OCC Bulletin 2017-07, because it describes what examination procedures OCC examiners may use during the examination of a bank's risk management of third-party relationships. "If you haven't looked at 2017-07, I would suggest you do, particularly if you think you're up for an examination soon," Keller said.

In another polling question provided during the Compliance Week Webinar, respondents were asked to describe their financial institution's response to OCC examination procedures. Most (52 percent) said they treat them the same as any other regulation, while 32 percent said they treat them as an "indication of preparedness."

Another 16 percent of respondents said they treat OCC examination procedures as informational, rather than as a regulatory requirement. "The best approach," Keller said, "is to treat it as any other regulation." ■

Planning, transactions, and reporting in the same system? That's music to my ears.



Say goodbye to export-import workarounds. With Workday, you can finally do planning, transactions, and reporting in the same system. And that sounds pretty great.

workday.com/truth

workday
Built for the future.®