RADICALLY SIMPLIFYING REGULATORY COMPLIANCE IN CYBERSECURITY

By Nadya Bartol, Brian O'Malley, Jeanne Bickford, and Michael Coden

NOT A WEEK PASSES without a new revelation of a massive cyber breach somewhere in the world. And as cybersecurity threats elevate, so do the number and extent of the regulations that seek to protect organizations and their customers.

A primary target for cyber criminals, financial services institutions must navigate both an increasing and an increasingly complex system of regulations and rules. But now they have a new tool to help them demonstrate compliance with multiple regulations—while also reducing associated costs.

Working with BITS, the technology division of the Banking Policy Institute, and a coalition of over 150 financial services institutions, BCG Platinion has developed the Financial Sector Cybersecurity Framework Profile, which harmonizes and consolidates regulatory requirements. The profile improves cybersecurity while significantly reducing administrative burdens and compliance costs.

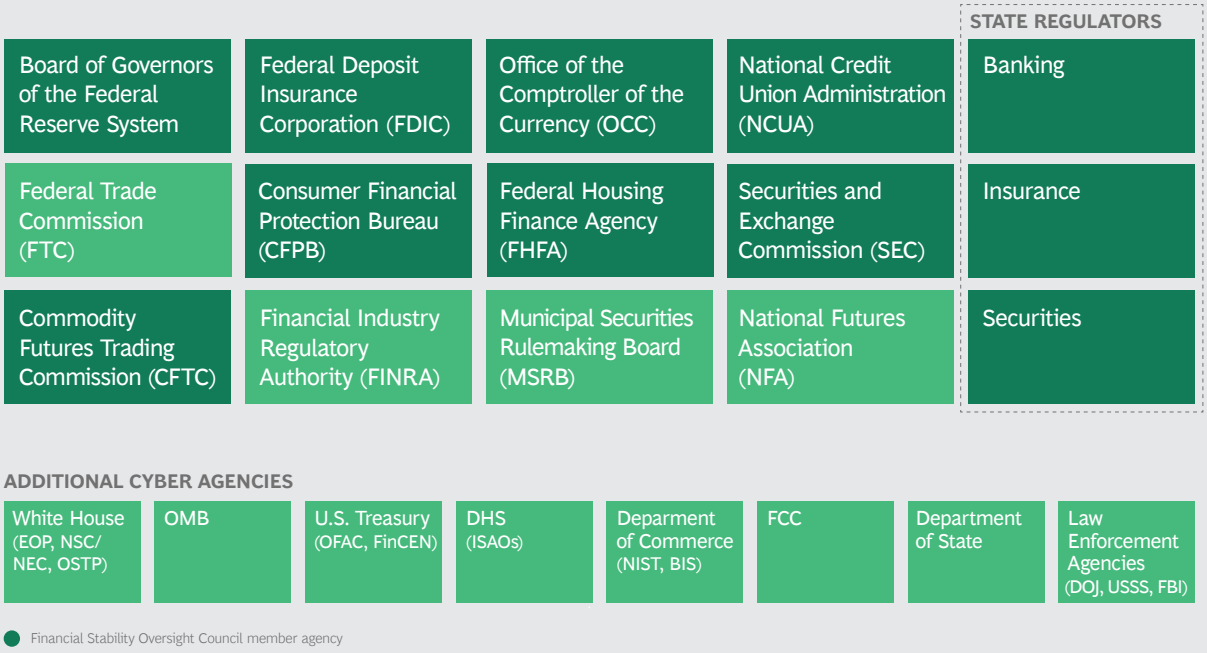
More—and More Complex—Regulations

According to industry data, in the United States alone, more than 30 cybersecurity regulations have been released since 2014. Globally, the pace has been similar. And in 2017, the Financial Stability Board announced that 72% of its 25 member jurisdictions were planning to issue further cybersecurity regulatory guidance. (See Exhibits 1, 2, and 3 for more information about the increasing regulartory burden.)

These numerous regulations aim to establish a set of robust cybersecurity practices to protect consumers and support the stability of the global economy. Unfortunately, however, they use differing vocabularies and lexicons to communicate the same concepts and practices. Consequently, they exert a significant burden on the financial services industry, which must demonstrate its compliance with the precise word of each individual regulation.

Even smaller financial services entities can work with 2 to 3 regulators. And large glob-

EXHIBIT 1 | In the US, a Broad Range of Agencies Regulate Cybersecurity...



Sources: Sources: GAO, BCG analysis.

EXHIBIT 2 | ...Enforcing Rules for Financial Institutions of All Types...

Sources: GAO, BCG analysis.

EXHIBIT 3 | . . . And Providing Oversight in a Multitude of Areas

Sources: GAO, BCG analysis.

al banks may work with 10, 20, or even more regulators around the world.

This complicated regulatory environment results in inefficiencies, lost time, and substantial financial impacts for financial institutions. According to the Banking Policy Institute, one chief information security officer indicated that he and his team spent nearly 40% of their work time reconciling various cybersecurity and regulatory frameworks.

At another multinational bank, the CIO, head of audit, and dozens of operating personnel had to conduct a two-month analysis of the bank's cybersecurity compliance. The effort consumed 15% of the operating budget for the bank's technology risk and compliance function for the entire year.

Risk assessments represent one of the greatest inefficiencies for financial institutions. Each regulator typically requires an annual risk assessment aligned to a framework it publishes, and the answers to that assessment must be supported by detailed evidence documents. The questions in these assessments and the evidence documents are often similar but worded in slightly different ways, which means each assessment requires a large amount of incremental effort.

New Framework Helps the Industry and the Regulators

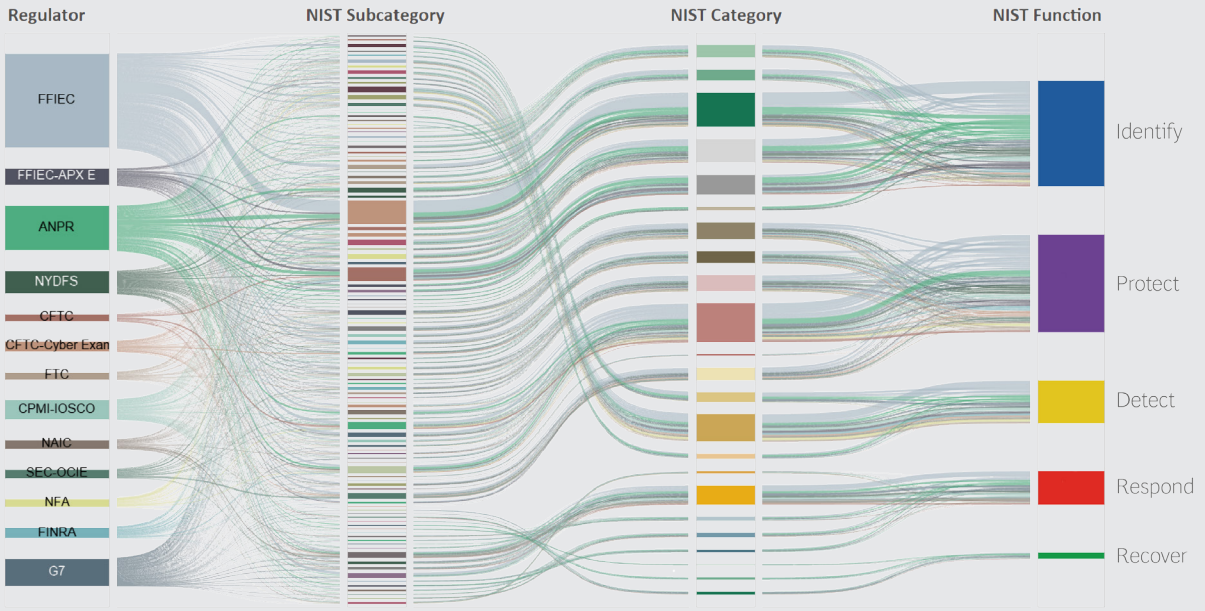
The Financial Sector Cybersecurity Framework Profile, which harmonizes and consolidates regulatory requirements, was created with assistance from BCG Platinion to help financial institutions meet their compliance obligations with less effort, time, and money. It improves cybersecurity while significantly reducing administrative burdens and compliance costs.

Through BITS, the financial services industry developed, endorsed, and committed to adopting the profile. The process took 18 months and involved more than 40 working sessions with more than 300 individual experts. Participating organizations ranged from community banks and credit unions to large multinational banking, investment, and insurance firms.

The profile reduces the number of reporting questions that financial services firms must answer—by 49% for large organizations to 73% for small ones. It integrates more than 30 regulatory requirements into a common framework that has now been endorsed by both financial institutions and by their regulators. (See Exhibit 4.)

It provides a single framework to enable financial institutions to:

EXHIBIT 4 | The Framework Aligns Cybersecurity Regulations, Reducing the Burden of Compliance



Sources: BCG and BPI/BITS.

- Engage with their boards on risk management for cyber threats
- Lay the foundation for a robust and compliant cybersecurity program
- Assess their cybersecurity risks and capabilities
- Consolidate a company's regulatory obligations
- Evaluate the cybersecurity programs of partners, vendors, and other service providers
- Facilitate technology innovation while managing cybersecurity risks
- Compare the state of cybersecurity across peer institutions
- Engage with regulators on the status of their cybersecurity and cyber risk regulatory compliance.

Further, the profile has also been endorsed by the US National Institute of Standards and Technology (NIST).

How the Profile Works

The profile is an adaptable framework designed to scale across institutions no matter their complexity, connections within and to other financial partners, size, and significance to the national and global economies. It can be used by every type of financial institution or any third -party provider to a financial services firm. The profile aligns more than 30 US federal, state, and global regulations with 3 key cybersecurity frameworks used globally:

- The NIST Cybersecurity Framework, which has become the gold standard of cybersecurity in the US and for many global entities
- The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, the prevalent global information security standard
- The Committee on Payments and Market Infrastructures (CPMI)-International Organization of Securities Commissions (IOSCO) cybersecurity guidelines.

The profile provides a common organiza-

tion, vocabulary, and taxonomy designed to incorporate future cybersecurity requirements. It allows institutions and individual regulators to focus on the core elements of their cybersecurity risk-management missions. And it eliminates the need to "reinvent the wheel" for every new rule.

It is expected to address 80% to 90% of regulatory requirements at any given point in time, providing for a single set of regulatory evidence to be shared among multiple regulators. In this way, it frees regulators and companies to focus on the areas of the greatest priority and need.

In the long run, the profile will help free both regulators and financial service executives to focus more resources on the most important emerging threats. The profile is also a living document that will expand to cover regulations beyond the US. In its next version the profile will incorporate additional regulations from Europe, Hong Kong, and other jurisdictions.

The profile consists of two parts:

Impact Tiering Questionnaire. This first part is designed to help a financial institution assess how extensive its cybersecurity practices must be. The assessment takes into account the institution's significance to the overall national economy, its interconnectivity to other financial services entities, the degree to which the company provides services to other financial services entities, and its impact on regional economy.

Cyber Diagnostic. Drawing on the results from the Impact Tiering Questionnaire, this tool lists specific cybersecurity practices that are relevant and required for the unique circumstances of the financial institution.

Of course, financial institutions using the tool can always chose to implement more rigorous practices than those dictated by the tier that the profile identifies for them. Similarly, regulators can always require a financial institution to go above and beyond their self-assessed impact tier.

Industry Response to the Profile

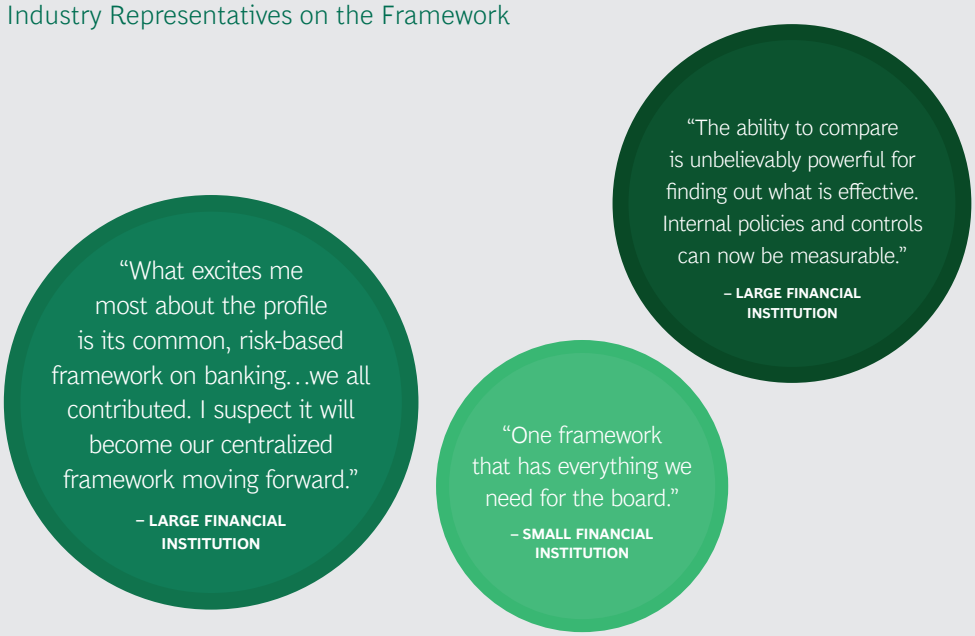
When the profile was officially launched on October 25, 2018, both the industry and the regulators committed to adopting the profile. (See Exhibits 5 and 6.)

The profile has already proven helpful in creating harmonized compliance regimens that are projected to save countless hours of staff time and millions of dollars of com-

EXHIBIT 5 | Industry Representatives on the Framework

Sources: GAO, BCG analysis.

EXHIBIT 6 | Industry Representatives on the Framework



Sources: GAO, BCG analysis.

pliance costs. The coalition that developed the profile is currently working on extending the profile globally, further simplifying compliance and helping the industry focus their resources where those matter most.

Nadya Bartol, BCG associate director, served as colead on profile development and led the BCG team supporting the framework effort. She welcomes comments and questions about the profile.

About the Authors

Nadya Bartol is the associate director in the Washington DC office of BCG Platinion. You may contact her by email at bartol.nadya@bcgplatinion.com.

Brian O'Malley is a partner and managing director in BCG's Minneapolis office. You may contact him at omally.brian@bcg.com.

Jeanne Bickford is a senior parter and managing director in BCG's New York office; he leads the cybersecurity practice. You may contact him at bickford.jeanne@bcg.com.

Michael Coden is a managing director in the New York office of BCG Platinion; he leads the cybersecurity practice. You may contact him at coden.michael@bcg.com.

Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with offices in more than 90 cities in 50 countries. For more information, please visit bcg.com.