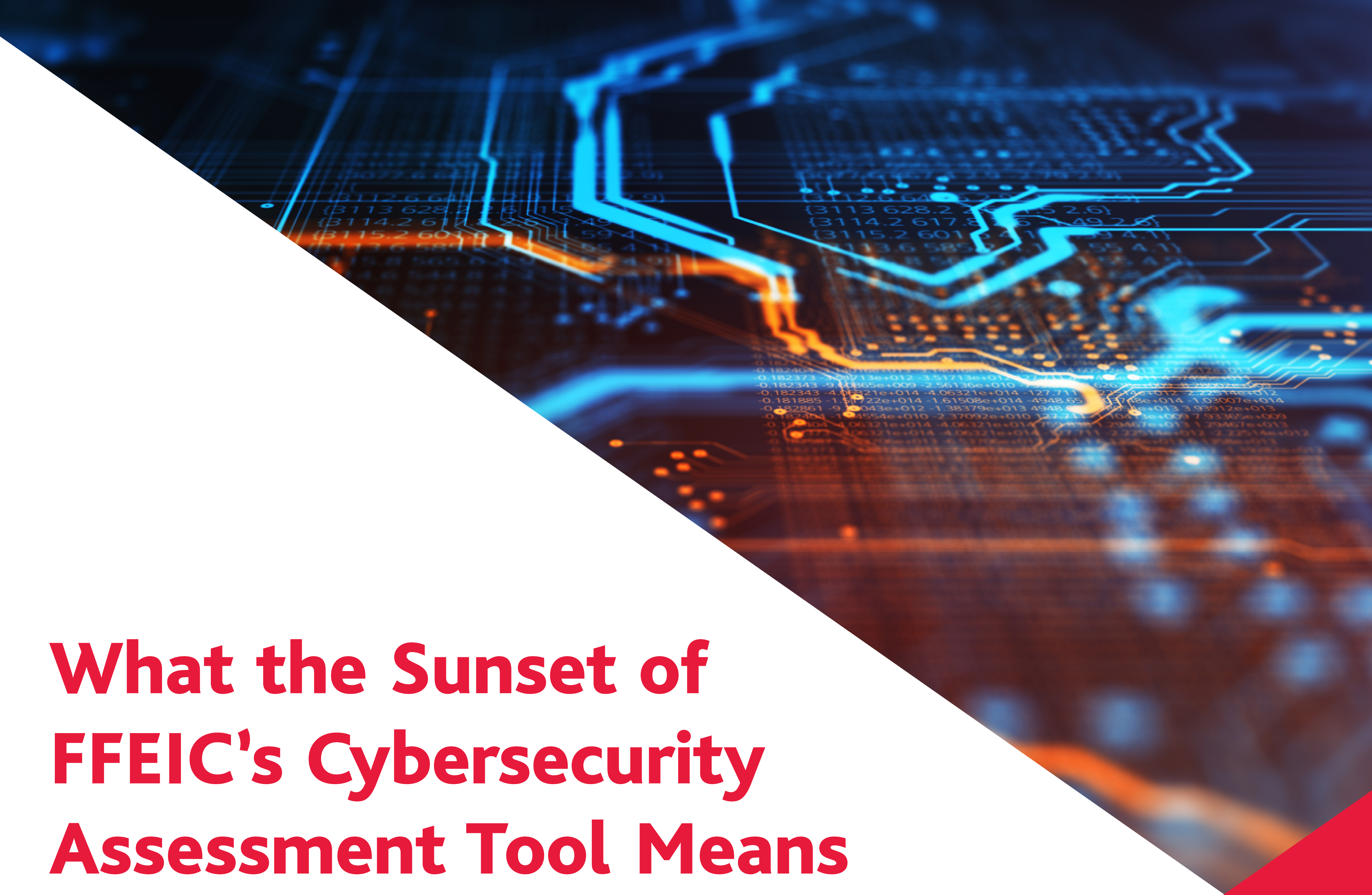
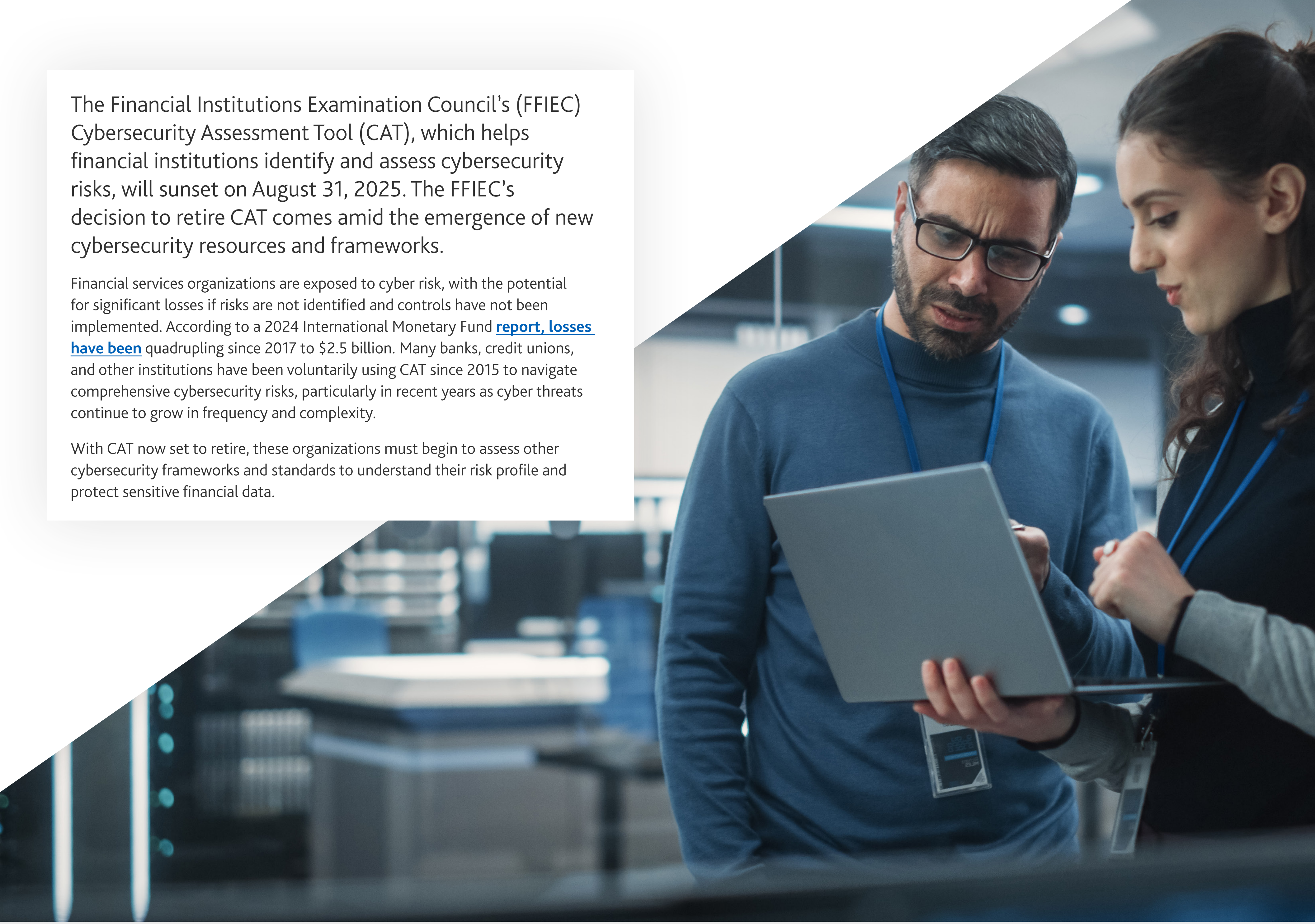


What the Sunset of FFEIC's Cybersecurity Assessment Tool Means for Financial Institutions

The Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool (CAT), which helps financial institutions identify and assess cybersecurity risks, will sunset on August 31, 2025. The FFIEC's decision to retire CAT comes amid the emergence of new cybersecurity resources and frameworks.

Financial services organizations are exposed to cyber risk, with the potential for significant losses if risks are not identified and controls have not been implemented. According to a 2024 International Monetary Fund **report, losses have been** quadrupling since 2017 to $2.5 billion. Many banks, credit unions, and other institutions have been voluntarily using CAT since 2015 to navigate comprehensive cybersecurity risks, particularly in recent years as cyber threats continue to grow in frequency and complexity.

With CAT now set to retire, these organizations must begin to assess other cybersecurity frameworks and standards to understand their risk profile and protect sensitive financial data.



Background of CAT

Due to its comprehensive nature, CAT has been a popular resource for financial institutions, enabling several critical functions, including:

Evaluating the institution's risk profile based on its **size, complexity,** and **operational environment.**

Assessing **cybersecurity maturity** across various domains, including **governance, risk management**, and **incident response.**

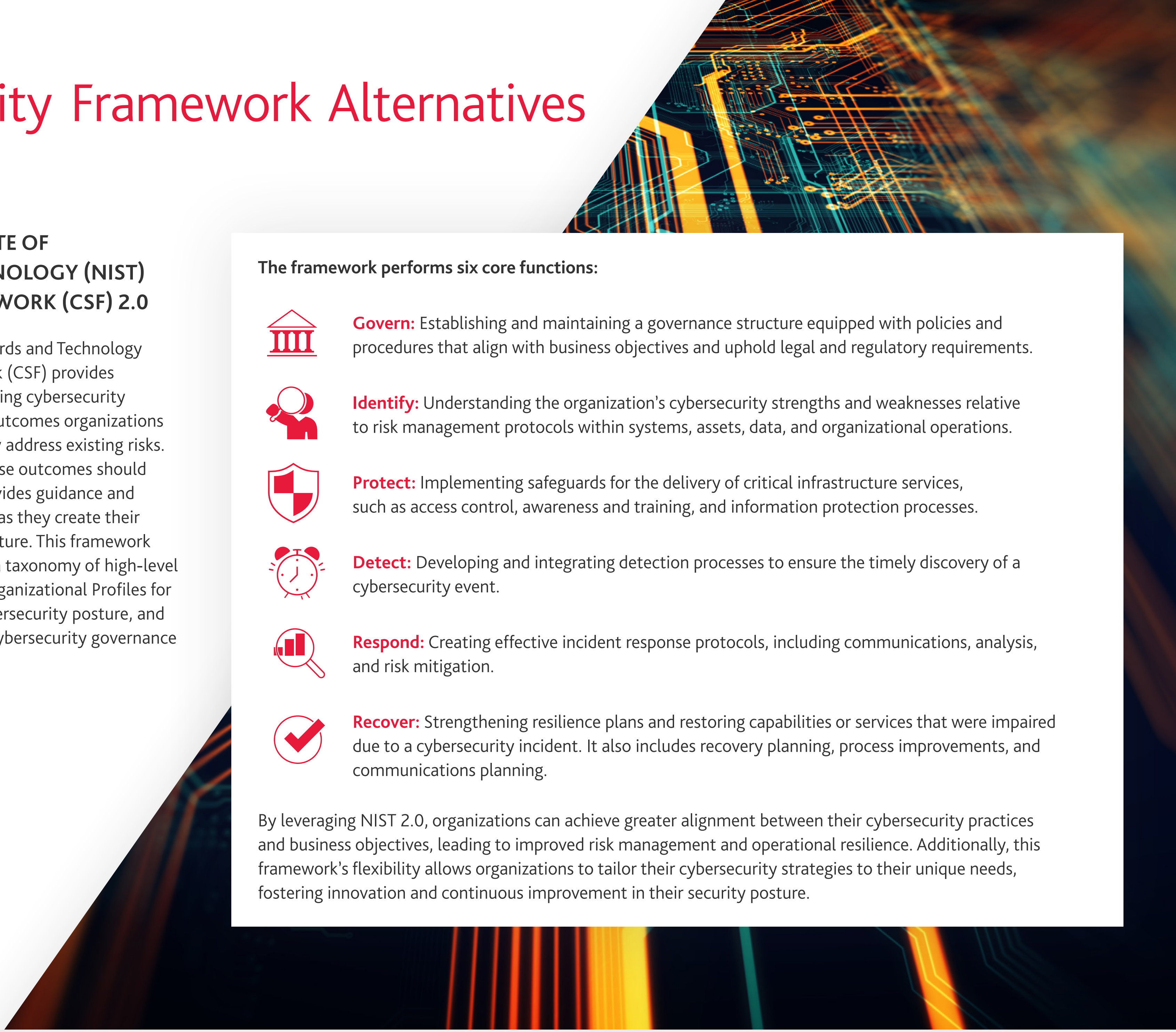
Providing a **structured assessment process**, including detailed questions and criteria, to help institutions **thoroughly understand their cybersecurity capabilities.**

Enhancing regulatory compliance by enabling institutions to **align their cybersecurity practices** with expectations outlined in CAT, thereby demonstrating their **cyber-risk management program.**

Through CAT, financial institutions have tailored their cybersecurity strategies commensurate with the risks they face and their specific vulnerabilities, allowing for a customized and streamlined approach to strengthening cyber defenses.

Looking ahead, organizations will need to select an alternative cybersecurity framework that provides a strong foundation they can build upon to address specific risk areas. There are several frameworks that financial institutions may consider. At a high level, organizations should look for a framework that covers multiple areas of cybersecurity, pinpoints problem areas that require enhancement, and helps stand up effective compliance programs. Selecting a framework will depend on the organization's needs as different guidance solutions offer unique capabilities and benefits. By using frameworks to identify gaps, institutions can allocate resources more efficiently and implement more targeted measures to bolster their cybersecurity posture.

Cybersecurity Framework Alternatives



THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) CYBERSECURITY FRAMEWORK (CSF) 2.0

The National Institute of Standards and Technology (**NIST**) Cybersecurity Framework (CSF) provides a structured approach to improving cybersecurity programs by outlining specific outcomes organizations can expect to achieve when they address existing risks. Rather than prescribing how those outcomes should be achieved, the framework provides guidance and resources for institutions to use as they create their own internal cybersecurity structure. This framework includes the CSF Core, which is a taxonomy of high-level cybersecurity outcomes, CSF Organizational Profiles for describing an organization's cybersecurity posture, and CSF Tiers to assess the rigor of cybersecurity governance and management practices.

The framework performs six core functions:

Govern: Establishing and maintaining a governance structure equipped with policies and procedures that align with business objectives and uphold legal and regulatory requirements.

Identify: Understanding the organization's cybersecurity strengths and weaknesses relative to risk management protocols within systems, assets, data, and organizational operations.

Protect: Implementing safeguards for the delivery of critical infrastructure services, such as access control, awareness and training, and information protection processes.

Detect: Developing and integrating detection processes to ensure the timely discovery of a cybersecurity event.

Respond: Creating effective incident response protocols, including communications, analysis, and risk mitigation.

Recover: Strengthening resilience plans and restoring capabilities or services that were impaired due to a cybersecurity incident. It also includes recovery planning, process improvements, and communications planning.

By leveraging NIST 2.0, organizations can achieve greater alignment between their cybersecurity practices and business objectives, leading to improved risk management and operational resilience. Additionally, this framework's flexibility allows organizations to tailor their cybersecurity strategies to their unique needs, fostering innovation and continuous improvement in their security posture.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S (CISA)'S CYBERSECURITY PERFORMANCE GOALS (CPGS)

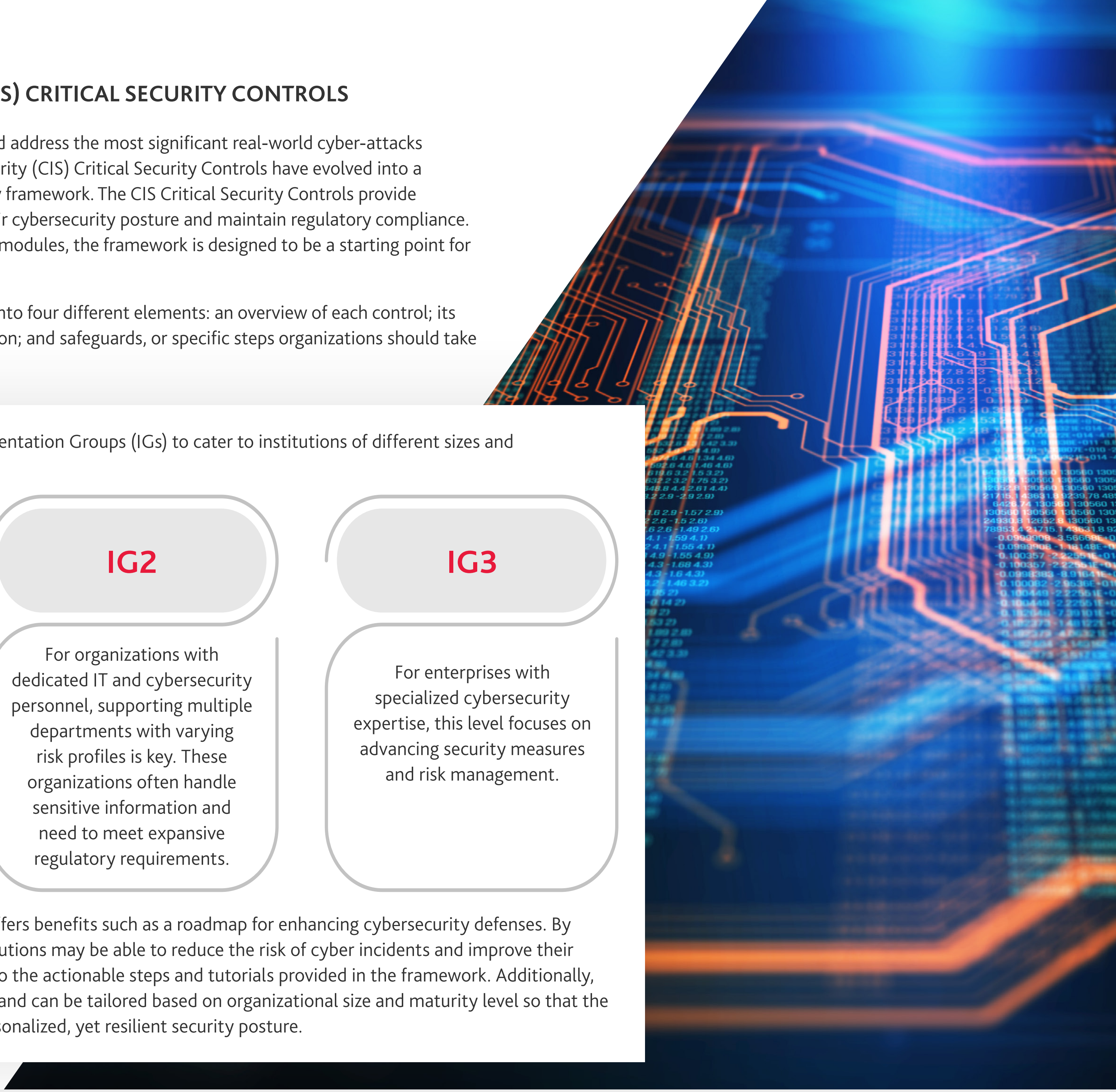
The Cybersecurity and Infrastructure Security Agency (CISA)'s Cybersecurity Performance Goals (CPGs) are voluntary guidelines designed to help businesses and critical infrastructure owners protect against cyber threats. While not exhaustive, the CPGs offer a core set of best practices with risk-reduction benefits applicable across industries. These guidelines prioritize high-impact security actions based on the current threat landscape and are organized into several categories such as asset identification, system protection, threat detection, incident response, and cyberattack recovery.

Using CISA's CPGs provides several advantages, including enhanced preparedness against cyber threats and a structured approach to implementing security measures. By adopting these guidelines, organizations can better prioritize critical security actions and execute efficiently. Additionally, CISA CPGs foster collaboration and information sharing across industries, which may help organizations learn from collective insights and experiences.

CENTER FOR INTERNET SECURITY (CIS) CRITICAL SECURITY CONTROLS

What started as a grassroots effort to identify and address the most significant real-world cyber-attacks affecting enterprises, the Center for Internet Security (CIS) Critical Security Controls have evolved into a comprehensive, globally recognized cybersecurity framework. The CIS Critical Security Controls provide actionable steps for organizations to improve their cybersecurity posture and maintain regulatory compliance. Supported by an ecosystem of tools and training modules, the framework is designed to be a starting point for businesses across various sectors.

The CIS Critical Security Controls are structured into four different elements: an overview of each control; its criticality; procedures and tools for implementation; and safeguards, or specific steps organizations should take to implement the control.



The framework is also organized into Implementation Groups (IGs) to cater to institutions of different sizes and cybersecurity maturity levels:

IG1

For small to medium-sized enterprises with limited IT and cybersecurity expertise, this level focuses on maintaining business operations and protecting low-sensitivity data.

IG2

For organizations with dedicated IT and cybersecurity personnel, supporting multiple departments with varying risk profiles is key. These organizations often handle sensitive information and need to meet expansive regulatory requirements.

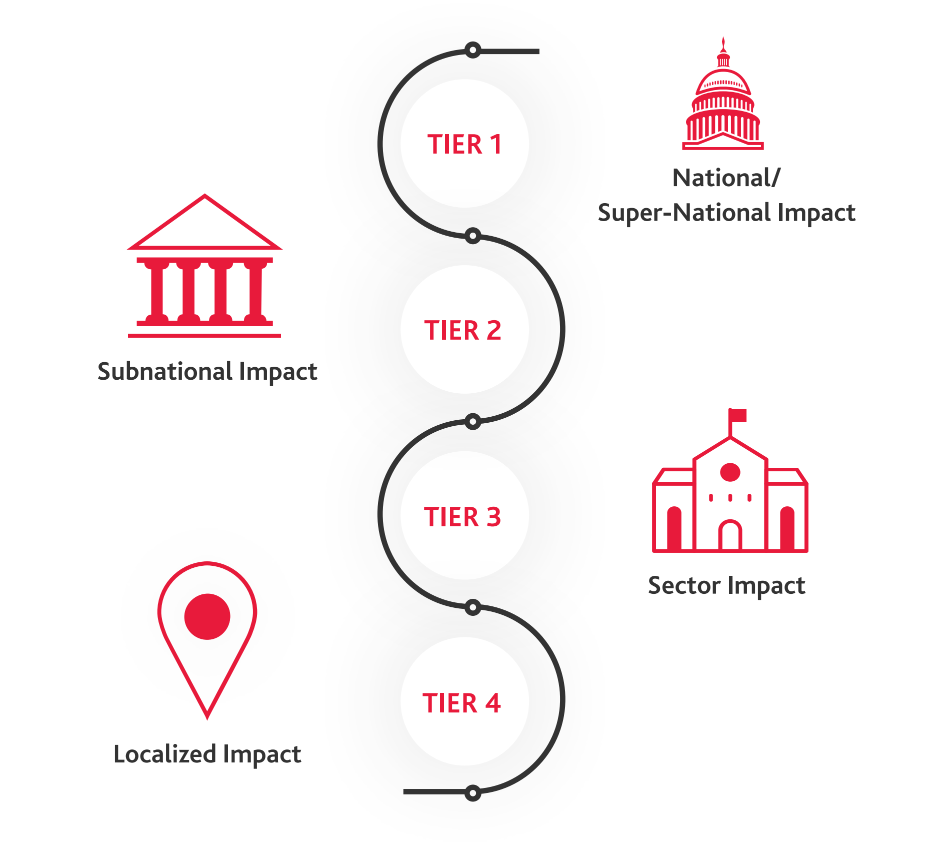
IG3

For enterprises with specialized cybersecurity expertise, this level focuses on advancing security measures and risk management.

Adopting the CIS Critical Security Controls offers benefits such as a roadmap for enhancing cybersecurity defenses. By implementing this framework, financial institutions may be able to reduce the risk of cyber incidents and improve their ability to detect and respond to threats due to the actionable steps and tutorials provided in the framework. Additionally, the controls in this framework are adaptable and can be tailored based on organizational size and maturity level so that the resulting cybersecurity strategy fosters a personalized, yet resilient security posture.

CYBER RISK INSTITUTE CYBER PROFILES

Created by and for the financial sector, the Cyber Risk Institute (CRI) Profile serves as a benchmarking tool for the financial services industry. It is specifically designed to help financial organizations understand their cybersecurity maturity, as well as provide consistency across the industry. Notably, the CRI categorizes institutions into four tiers based on their impact to the financial services sector and economy. Each tier descends from most widespread to localized impact as follows:



The profile is based on the NIST CSF with a significant addition: diagnostic statements. These statements "knit together 2,500 regulatory expectations in 318 control objectives" to give financial institutions prescriptive guidance for complex cyber-risk management. By understanding the macro impacts of a cybersecurity incident based upon their tier, financial firm leaders can better gauge the criticality of cyber upgrades and appropriate resource allocation.

Employing the CRI Cyber Profiles provides numerous advantages, such as improved clarity and accuracy in evaluating cybersecurity maturity and preparedness. By using these profiles, financial institutions can better align with regulatory requirements and industry standards, which helps to promote uniform cybersecurity best practices throughout the sector. Since the tiered structure of this framework enables organizations to focus their cybersecurity initiatives or investments according to their potential impact, it also allows for more targeted and effective risk management.

CYBERSECURITY CAPACITY MATURITY MODEL

The Cybersecurity Capacity Maturity Model (C2M2) 2022 is another promising alternative. While C2M2 is primarily focused on operational technology (OT) environments, it can be adapted for use in non-industrial settings. This model offers a comprehensive framework for assessing and enhancing cybersecurity capabilities across various domains, making it particularly relevant for organizations seeking to strengthen their cyber defenses and interested in a possible option in the wake of CAT's sunset. However, using C2M2 would require modifications so that the model appropriately addresses the cybersecurity needs of banks and financial institutions and their non-industrial environments.

Some key features of C2M2 include the following:

- **Cross-dimensional Approach:** C2M2 2022 emphasizes the development of cybersecurity capabilities across five dimensions: policy and strategy, culture and awareness, education and training, legal and regulatory frameworks, and technical capabilities. This holistic approach often leads to well-rounded cybersecurity programs.
- **Maturity Levels:** The model provides a structured pathway for organizations to assess their cybersecurity maturity. By identifying current capabilities and areas for improvement, institutions can prioritize initiatives based on what will enhance their security posture most effectively.
- **Customizable Framework:** C2M2 2022 is designed to be highly adaptable to the unique needs of each organization. Financial institutions can tailor the model to align with their specific risk profiles, operational environments, and strategic objectives, making cybersecurity efforts both bespoke and efficient.
- **Collaborative Approach:** The model encourages collaboration between different sectors and stakeholders, fostering a shared understanding of cybersecurity challenges and solutions. This collaborative approach can help institutions leverage collective expertise and resources to address complex cyber threats.

The C2M2 2022 model's emphasis on continuous improvement and adaptability allows institutions to respond to evolving cyber threats with confidence and maintain resilience in the face of uncertainty.

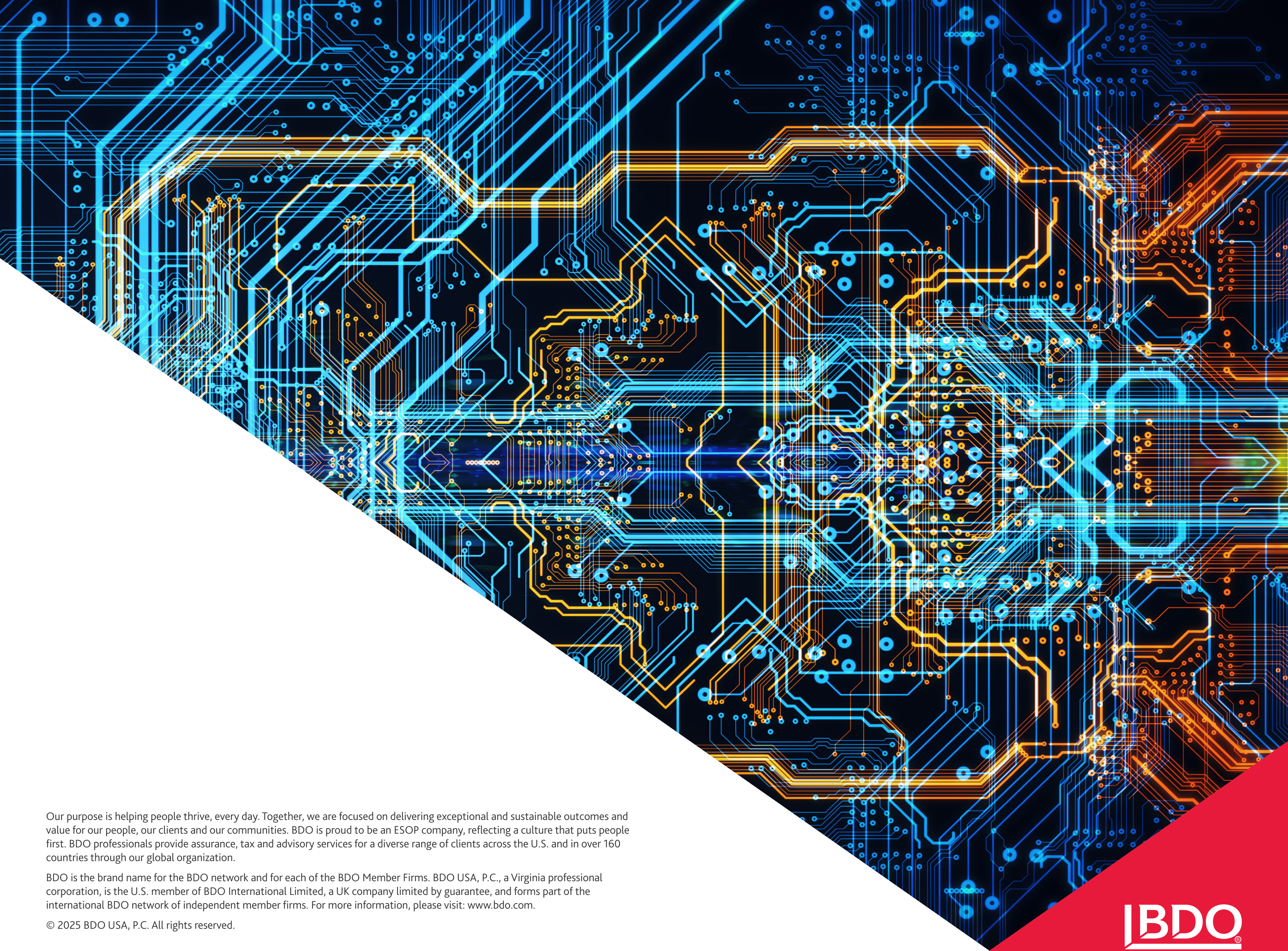
The Future of Cybersecurity for Financial Institutions

The retirement of the FFIEC Cybersecurity Assessment Tool (CAT) underscores the necessity for financial institutions to identify and adopt newer frameworks to help bolster their cybersecurity posture. Chosen tools, controls, and standards should be tailored to address the organization's specific risk profile and complement its existing frameworks and cybersecurity maturity goals.

To prepare defenses amid the ongoing and evolving cyber threats, financial services firms should adopt a comprehensive and iterative approach to cybersecurity management. Protecting sensitive financial data, maintaining the integrity of financial systems, and forecasting potential threats are all cornerstones of an effective cybersecurity program — safeguarding information today and into the future.

BDO's team of IT risk advisory professionals can help stand up a comprehensive program for addressing today's sophisticated cyber threats. BDO professionals can assist financial institutions in strengthening their cybersecurity frameworks and corresponding compliance programs through a variety of services, such as IT risk assessment and cybersecurity audits that evaluate organizational controls and processes to identify where improvements should be made.

READY TO LEARN MORE ABOUT CHOOSING A CYBERSECURITY FRAMEWORK? **CONTACT BDO TODAY.**



Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.