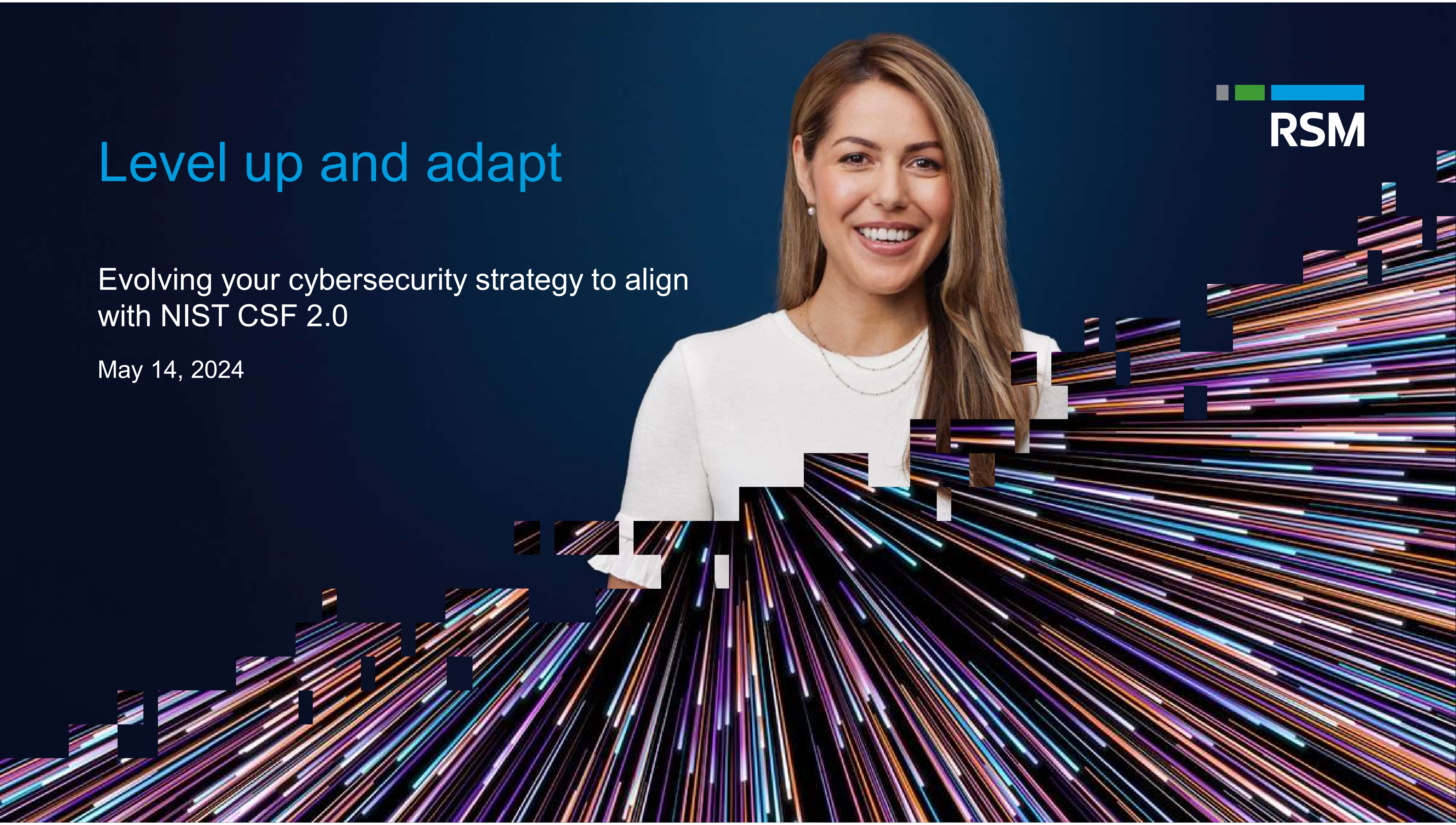
RSM

Level up and adapt

Evolving your cybersecurity strategy to align with NIST CSF 2.0

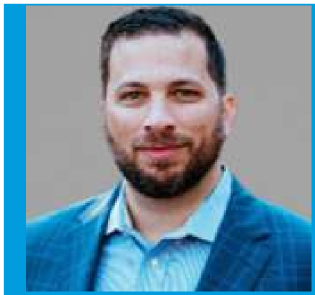
May 14, 2024



Agenda

4	Historical breach numbers
5	Proactive defense
8	Evolving landscape and need for adaptation
12	Dive into NIST CSF 2.0
13	Risk integration and coordination
16	Aligning your strategy with NIST CSF 2.0
20	Benefits of adapting with NIST CSF 2.0
22	Wrap-up

With you today



Chip Stewart Director

Chip.Stewart@rsmus.com

Chip supports the RSM security and privacy risk consulting services practice by integrating his real-world experiences as both a customer and consultant with his technical knowledge and leadership skills. With over 20 years of consulting experience within the information technology and cybersecurity field, his combination of technical, business, and political capabilities allow him to provide unique perspective and support. Most of Chip's experience has focused on developing and operationalizing large-scale programs in both the public and private sectors.

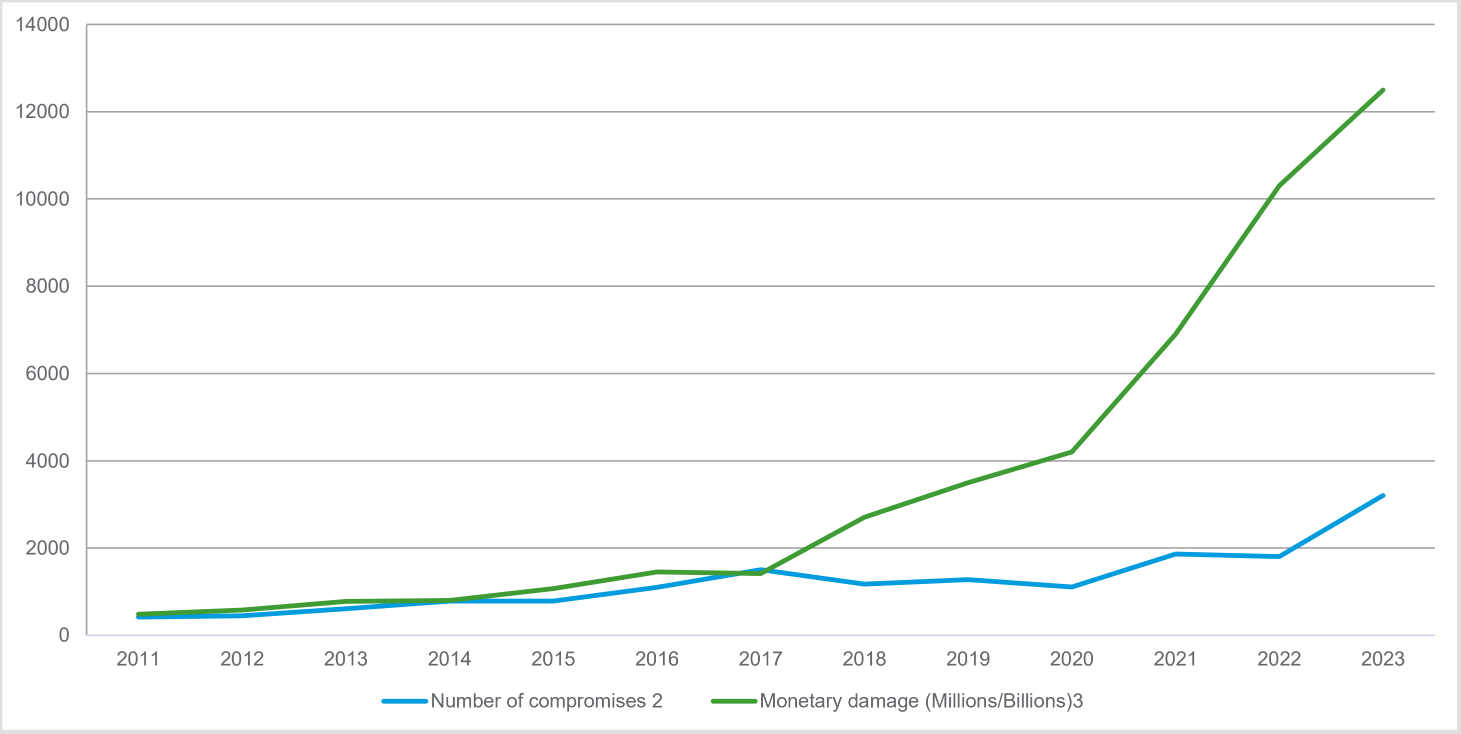
Chip served as the state chief information security officer in Maryland from 2019 until 2023, where he was responsible for building a cybersecurity program from the ground up. In this role, he leveraged his technical abilities to implement legislative changes to Maryland law, including the codification of the state CISO role, creating a legislative mandate for the Maryland Information Sharing and Analysis Center, a requirement for bi-annual security assessments for government agencies, and mandatory incident reporting requirements. In addition, Chip led the charge to create the executive orders establishing Maryland's first state chief privacy officer and state chief data officer.

Jason Broz Director

Jason.Broz@rsmus.com

Jason assists clients with executive management decisions surrounding information security and other complex projects that align with an organization's core business values. He has worked with organizations spanning many industries, including retail, telecommunications, health care, technology, utilities, logistics, insurance and education. Jason applies his multi-industry business expertise and years of technical knowledge to deliver customized solutions that reduce risk, achieve compliance and ensure data security.

Historical breach numbers and associated costs



Breaches by the numbers

3,205[2]

Total compromises 2023

4.45 Million[1]

Average cost of a data breach 2023

15.3%[2]

Cost increase since 2020

39%[2]

Breaches that spanned multiple environments

SOURCES:

[1] *IBM Security: Cost of a Data Breach Report 2023; https://www.ibm.com/downloads/cas/E3G5JMBP*

[2] *ITRC 2023 Data Breach Report; https://www.idtheftcenter.org/publication/2023-data-breach-report/*

[3] *Federal Bureau of Investigation: Internet Crime report 2023; https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf*

Proactive defense

What is it and why is it important?

Proactive defense The ability to anticipate future issues, needs, or changes through implementing continual processes and key activities with the intent to identify and reduce or prevent threats from materializing.

Examples of proactive activities:

- Threat Hunting/Intelligence
- Penetration Testing/Vulnerability Scanning
- Proactive monitoring
- Cybersecurity Awareness training
- Behavior based analytics

Why is it important?

- Better control over risk management
- Help prevent threats
- Enhance reactive security
- Track evolving risks
- Implement continual improvement
- Facilitate compliance
- Enhance trust

Benefits of Proactive Defense

1.68 M	33%	1.49 M
Cost savings of High DevSecOps adoption	Percentage of breaches identified by an organizations own security team or tools	Cost savings of High level of IR planning

SOURCE: IBM Security: Cost of a Data Breach Report 2023; https://www.ibm.com/downloads/cas/E3G5JMBP

Your role in Proactive defense

What is your role in Proactive defense?

Role	***Proactive activity***
Enterprise Leadership	• Develop Written Information Security Program • Develop cybersecurity focused policies to drive proactive behavior • Install quarterly reporting (minimum) of security activities and incidents to security/risk steering committee or Board • Require all employees, contractors/vendors, interns, and volunteers with credentials complete security awareness training
Organization Level Managers	• Define acceptable tolerance based on risk appetite statement • Implement proactive standard operating procedures • Develop a plan or work with the steering committee to plan business as usual security activities, such as penetration testing, security assessments • Enforce security awareness training completion and encourage security focused training • Conduct phishing campaigns to test security awareness program effectiveness
Practitioner	• Execute on business-as-usual activities per defined schedule • Conduct or obtain threat intelligence reports and review • Identify and implement security controls to reduce the risk • Remediate issues identified from penetration testing/vulnerability scanning

Evolving landscape and need for adaptation

Key changes in the landscape

Expanding attack surface

Technology resources with interdependent complexity are interwoven and distributed across multiple environments and providers.

Sophistication of threats

Sophisticated threat actors are leveraging advanced toolkits and capabilities to launch attacks.

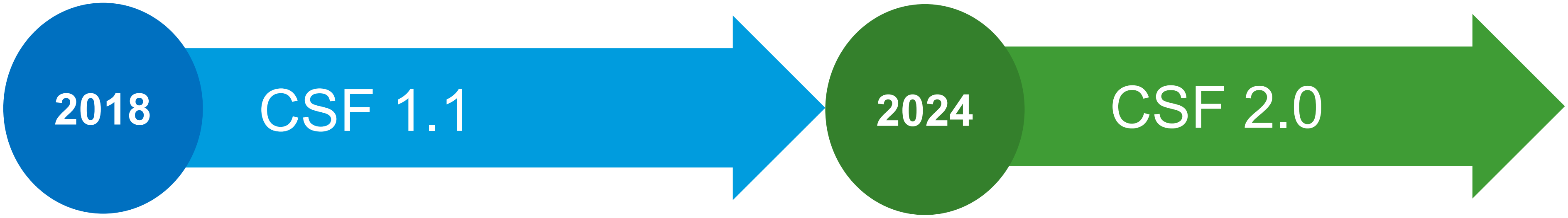
Unsophisticated threat actors are leveraging commoditized products to carry out attacks.

Increased reliance on technology

Businesses are increasingly reliant on technology across all areas of business and frequently do not have non-technology-dependent mechanisms to conduct operations.

Evolving landscape and need for adaptation

Business drivers for change



2018

CSF 1.1

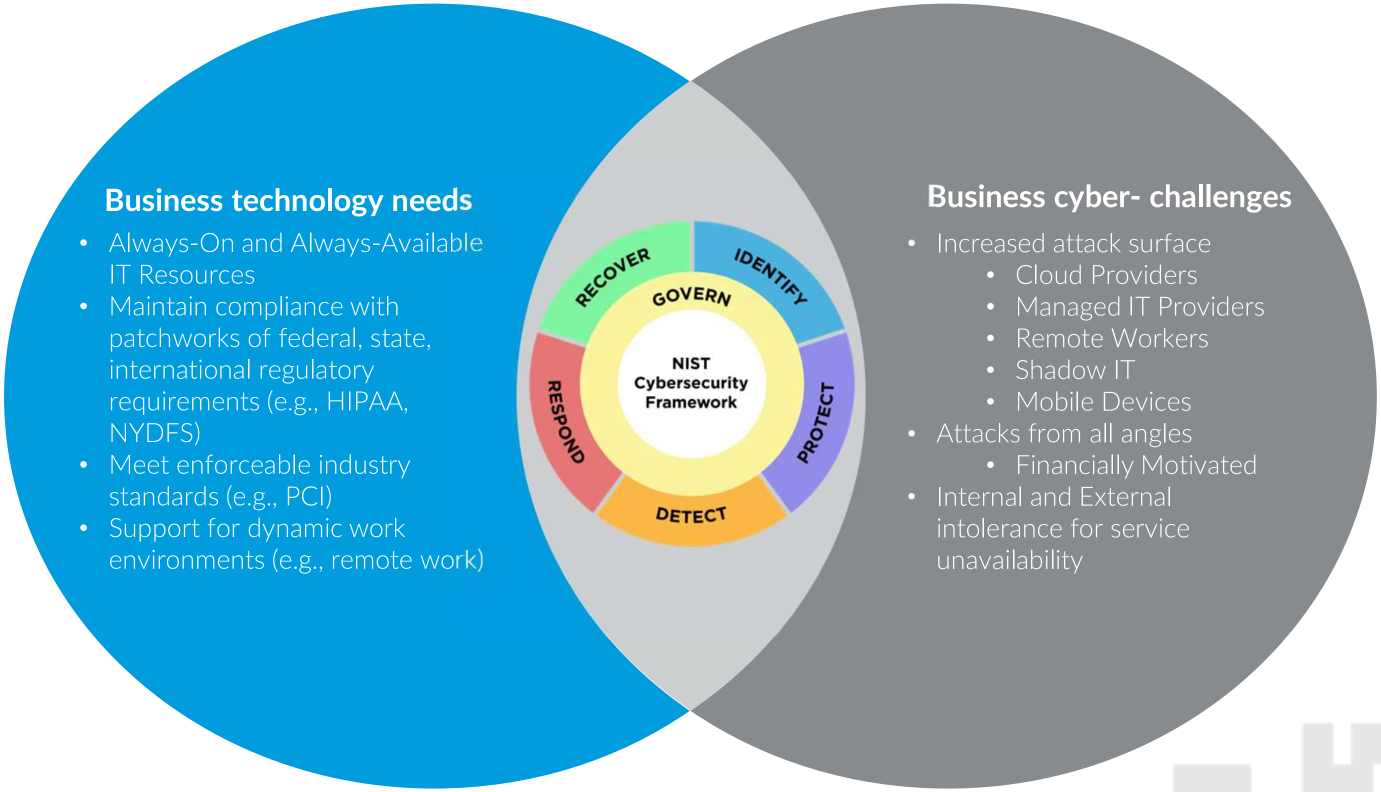
2024

CSF 2.0

- Most businesses rely on technology for all aspects of their operation
- Increased interconnectedness between businesses
- Greater reliance on partners and suppliers
- Increasingly distributed workforce
- More regulatory pressure across a broader range of business

Evolving landscape and need for adaptation

Convergence of change drives adapting strategies



Business technology needs

- Always-On and Always-Available IT Resources
- Maintain compliance with patchworks of federal, state, international regulatory requirements (e.g., HIPAA, NYDFS)
- Meet enforceable industry standards (e.g., PCI)
- Support for dynamic work environments (e.g., remote work)

Business cyber- challenges

- Increased attack surface
  - Cloud Providers
  - Managed IT Providers
  - Remote Workers
  - Shadow IT
  - Mobile Devices
- Attacks from all angles
  - Financially Motivated
- Internal and External intolerance for service unavailability

Dive into NIST CSF 2.0

What’s different?

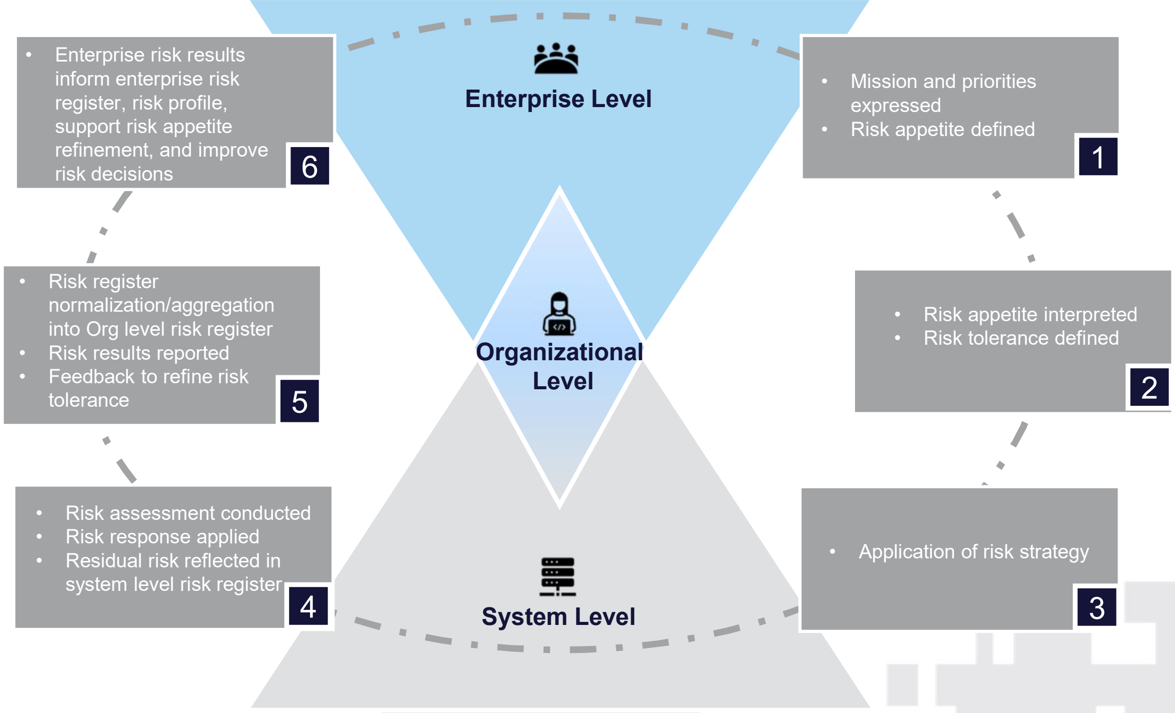
Functions	Subcategories/Controls	Scope/Focus	Additional resources
• New Govern Function	• Alignment of Governance Functions under 1 heading • Enhanced Supply-Chain Risk Management controls	• Applicable to all industries, size, and complexity of companies	• Alignment to other frameworks/standards • Implementation examples • Quick Start Guides (QSG) • Community and organizational Profile Templates

Middle Market Impact

- Not a “one size fits all” model
- Implementation guides
- Quick start guides
- Profile templates

Risk integration and coordination activities

NIST Special Publication 800-221 provides alignment of Cybersecurity Risk Management (CSRM) to Enterprise Risk Management (ERM) through Information and Communications Technology (ICT)



1
- Mission and priorities expressed
- Risk appetite defined

2
- Risk appetite interpreted
- Risk tolerance defined

3
- Application of risk strategy

4
- Risk assessment conducted
- Risk response applied
- Residual risk reflected in system level risk register

5
- Risk register normalization/aggregation into Org level risk register
- Risk results reported
- Feedback to refine risk tolerance

6
- Enterprise risk results inform enterprise risk register, risk profile, support risk appetite refinement, and improve risk decisions

Enterprise Risk Management integration and coordination (NIST SP 800-221)

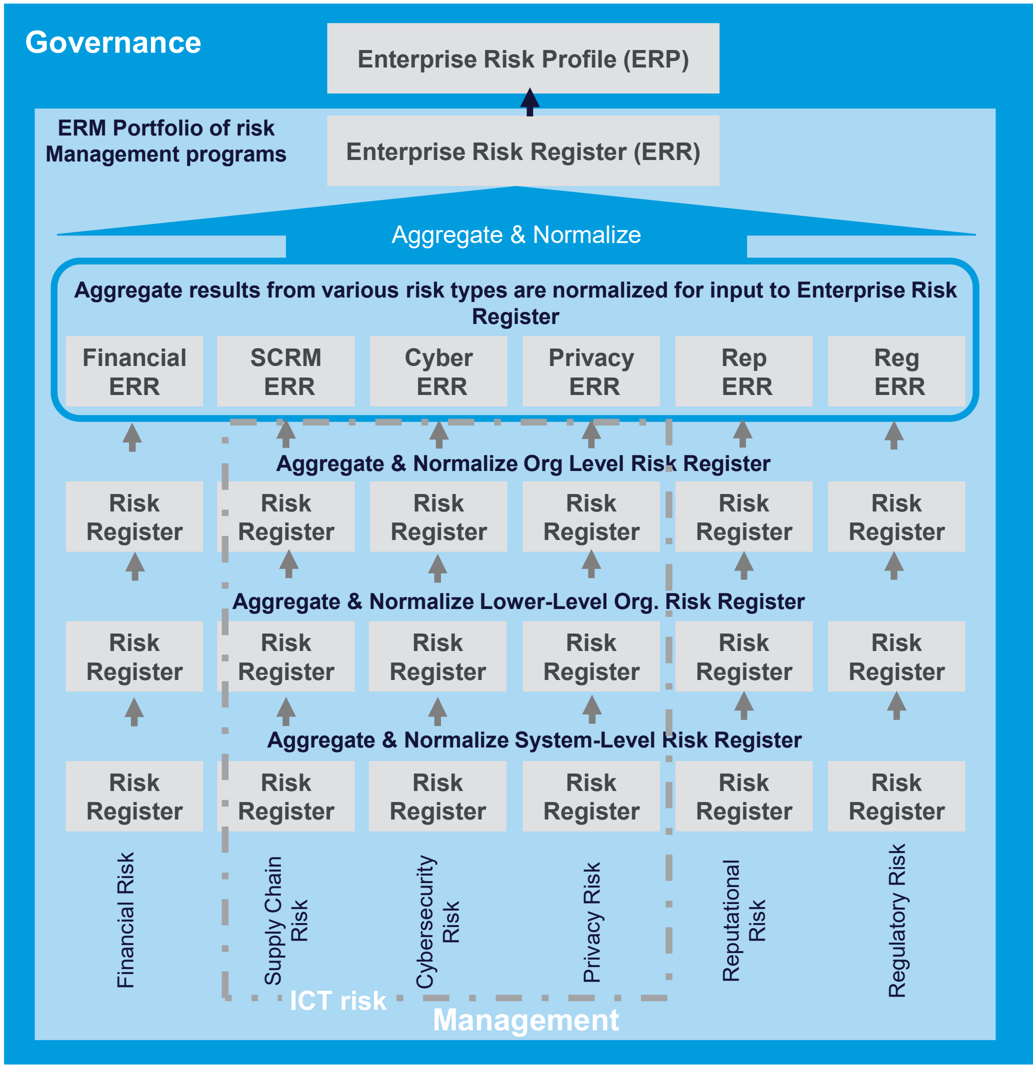
Risk management workflow

Enterprise risk management and information and communications technology risk (ICTRM)

- ICTRM is an important subset of the broader portfolio of ERM
- Enterprise risk register (ERR) is prioritized by those with fiduciary and oversight responsibilities by creating an Enterprise risk profile (ERP)
  - Takes into consideration enterprise risks through comparison to objectives as outlined in the organizational strategic plan
    - Per OMB Circular A-123, ERP includes four (4) objectives
      - Strategic
      - Operations (effectiveness and efficiency)
      - Reporting (reporting reliability)
      - Compliance (with applicable laws and regulations)
- Effective ERM balances maximizing resources with achieving objectives

Typical ICTRM approach shortcomings

- Increasing system and ecosystem complexity
- Lack of standardized measures
- Informal analysis methods
- Overly focused on system level
- Gap between ICTRM output and ERM Input
- Losing the context of the positive risk



Governance

Enterprise Risk Profile (ERP)

ERM Portfolio of risk Management programs

Enterprise Risk Register (ERR)

Aggregate & Normalize

Aggregate results from various risk types are normalized for input to Enterprise Risk Register

Financial ERR | SCRM ERR | Cyber ERR | Privacy ERR | Rep ERR | Reg ERR

Aggregate & Normalize Org Level Risk Register

Risk Register | Risk Register | Risk Register | Risk Register | Risk Register | Risk Register

Aggregate & Normalize Lower-Level Org. Risk Register

Risk Register | Risk Register | Risk Register | Risk Register | Risk Register | Risk Register

Aggregate & Normalize System-Level Risk Register

Risk Register | Risk Register | Risk Register | Risk Register | Risk Register | Risk Register

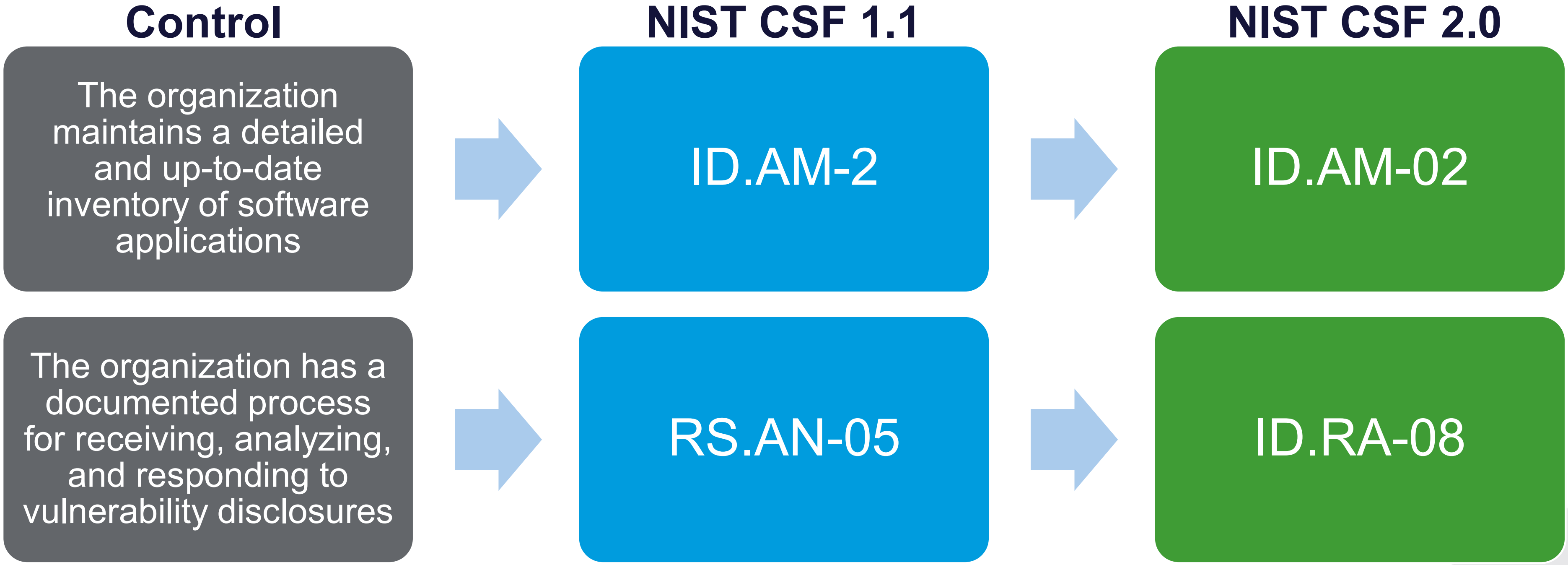
Financial Risk | Supply Chain Risk | Cybersecurity Risk | Privacy Risk | Reputational Risk | Regulatory Risk

ICT risk

Management

Aligning Your Strategy with NIST CSF 2.0

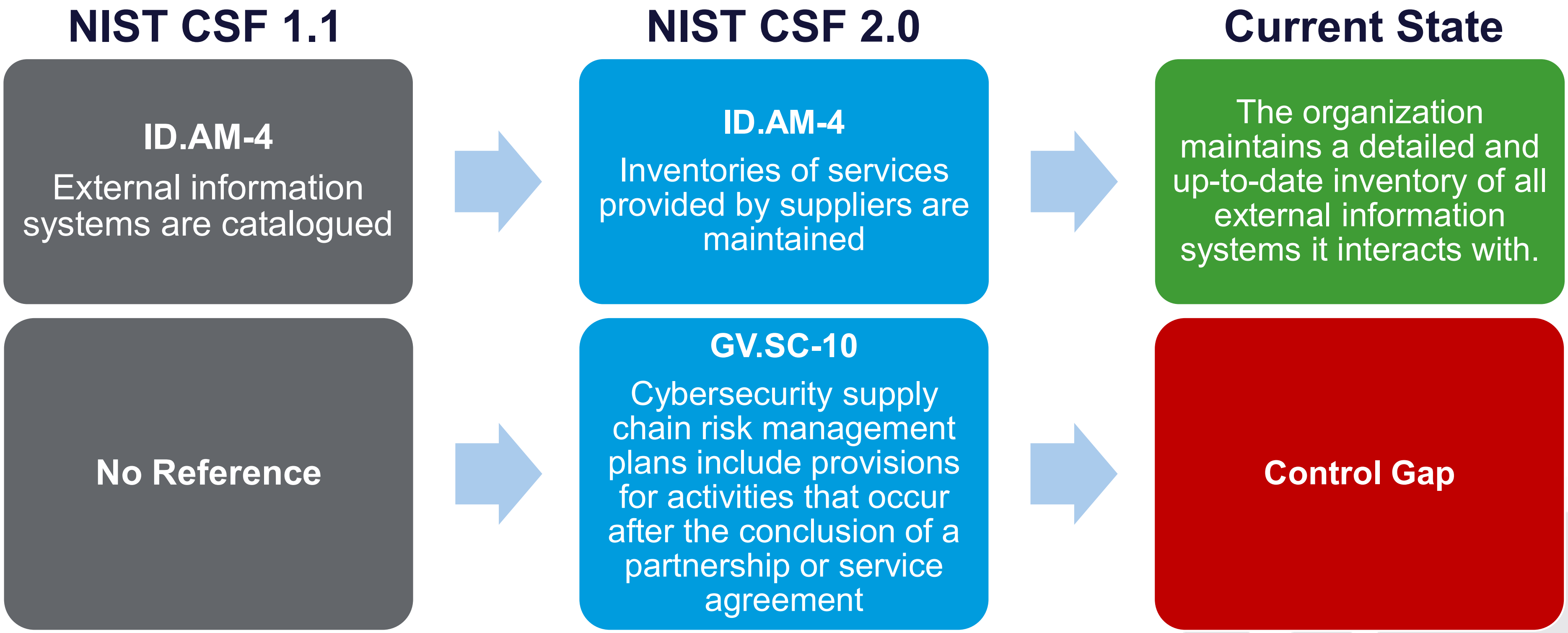
Step-by-Step Approach for adapting to the new framework – Mapping Controls



Control	NIST CSF 1.1	NIST CSF 2.0
The organization maintains a detailed and up-to-date inventory of software applications	ID.AM-2	ID.AM-02
The organization has a documented process for receiving, analyzing, and responding to vulnerability disclosures	RS.AN-05	ID.RA-08

Aligning your strategy with NIST CSF 2.0

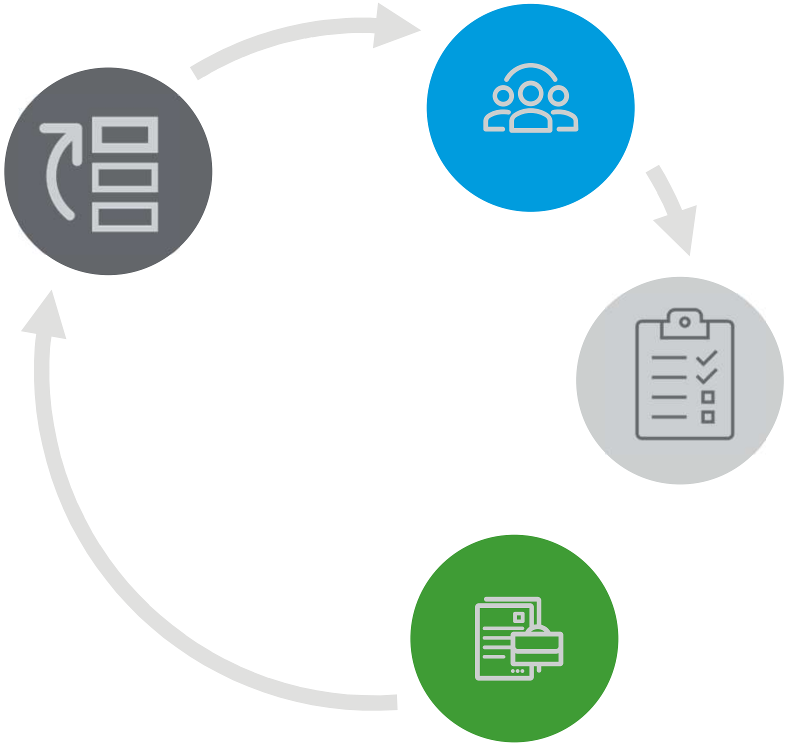
Step-by-step approach for adapting to the new framework – Gap Analysis



NIST CSF 1.1	NIST CSF 2.0	Current State
ID.AM-4 External information systems are catalogued	**ID.AM-4** Inventories of services provided by suppliers are maintained	The organization maintains a detailed and up-to-date inventory of all external information systems it interacts with.
No Reference	**GV.SC-10** Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	**Control Gap**

Aligning your strategy with NIST CSF 2.0

Step-by-step approach for adapting to the new framework – Prioritized remediation roadmap



Conduct a risk assessment

Understanding the risks associated with control non-adherence supports communicating alignment with your organizational risk tolerances and appetite.

Prioritize risks

Considering the likelihood and impact supports the organization making investments to align operational realities with the evolving landscape.

Develop remediation roadmap

Identifying and planning for the changes, including costs, timelines, and organizational change smooths the implementation rollout.

Implement the roadmap

Executing a controlled rollout of the changes, including developing new metrics and measuring performance of the shift facilitates successful implementation.

Benefits of adapting with NIST CSF 2.0

Improved risk management

- Cybersecurity risk management strategy alignment to enterprise risk management strategy
- Enhanced focus on supply-chain risk management
- Facilitate vendor and compliance requirements
- Supports resiliency efforts
- Includes people, process, and technology
- Allows for customization of risk management strategy

Enhanced communications

- Common language used across the organization
- Tools and informative guides on how to get started or resolve issues are actionable
- Identifies organizational risks and provides examples how to mitigate
- Aligned to many NIST developed Special publications, including
  - Workforce framework for cybersecurity SP 800-181;NICE Framework)
  - AI Risk Management framework (AI RMF 1.0)

Supports proactive approach

- Enhanced preparedness for cyber threats.
- Increased resilience in the face of evolving attacks
- Conducting an assessment to identify vulnerabilities
- Identify best practice security tasks that need completed
- Controls designed to foster a proactive approach

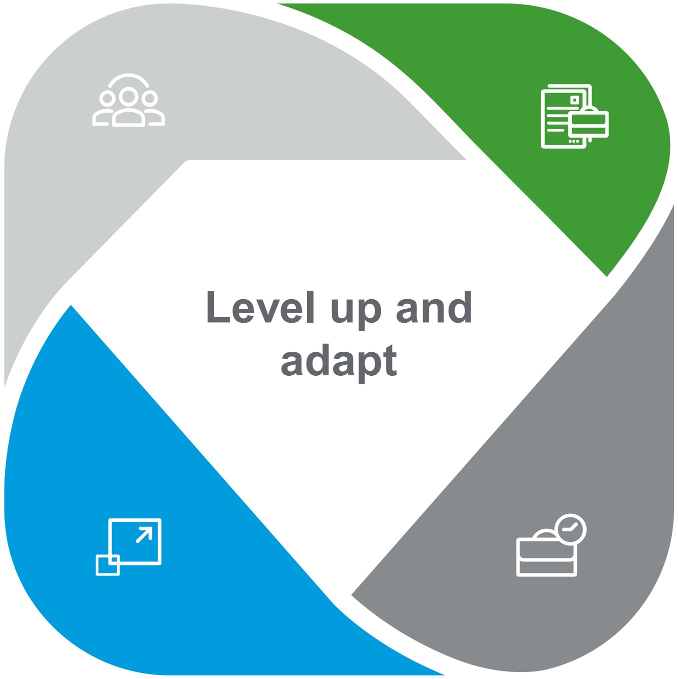
Level up & adapt – Aligning your cybersecurity strategy with the NIST CSF 2.0

Key takeaways and resources

- The intersection of increased technological dependence, a more distributed attack surface, and more sophisticated threats is driving the evolution of cybersecurity programs.
  - Successful implementation of the new framework supports better resilience in the face of new threats and business needs
- The CSF 2.0 increases the applicability for more organizations and clarity of implementation expectations
- Building an achievable roadmap accelerates implementation timeline
  - Implementation metrics facilitate communication across organizational leadership
- The NIST Website includes a wealth of resources on the updated framework
  - Cybersecurity Framework | NIST

Leveling up

Steps you should consider to transition to the new framework



Decide if NIST CSF 2.0 is right for your organization

As a non-mandatory framework, the NIST CSF is a great fit for many organizations, but not all.

Conduct an assessment and gap analysis

Having a clear picture of your current posture and an understanding of the gaps in your current controls informs the needs and priorities required to get to the next level.

Develop your remediation strategy

Building out an implementation strategy that including timelines, costs, and metrics facilitates shared expectations and a successful rollout.

Level up

Implementing new controls may require additional expertise, reskilling staff, and new tools. Plan to level up people, process, technology, and partners.

RSM

Thank you for your time and attention

RSM

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute assurance, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent assurance, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.