Crowe

Smart decisions. Lasting value. ™

Credit Union Outlook 2022

Considerations for the year ahead

Feb. 24, 2022

Agenda

1
Welcome and introduction

2
Accounting topics

3
Regulatory update

4
Consumer compliance

5
Cybersecurity topics

6
Wrap-up

Niall Twomey
Principal
+1 630 574 1806
niall.twomey@crowe.com

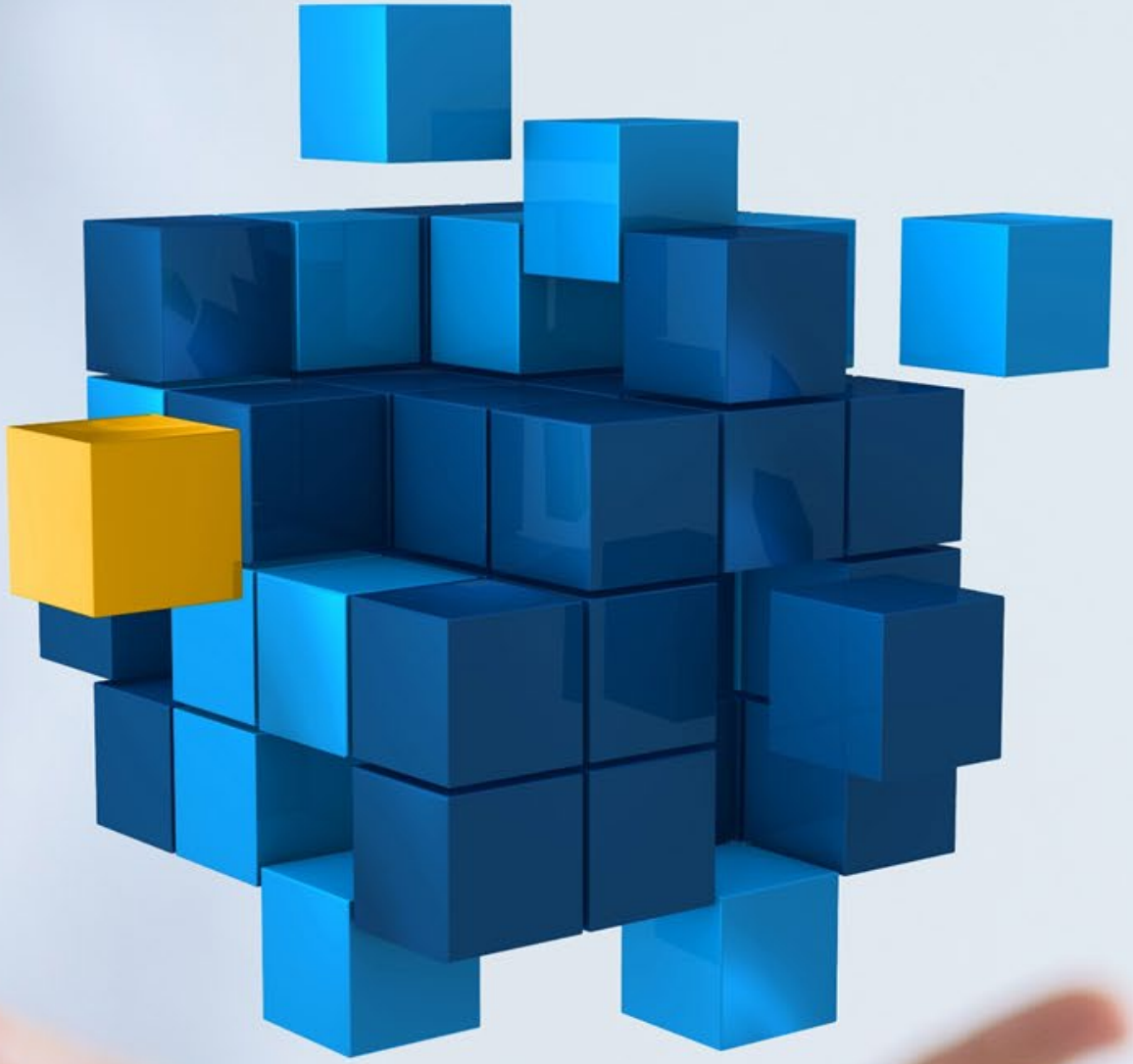
Rob Blanchard
Managing Director
+1 614 469 4003
rob.blanchard@crowe.com

Dennis Hild
Managing Director
+1 202 552 8086
dennis.hild@crowe.com

Jason Naber
Senior Manager
+1 616 242 6124
jason.naber@crowe.com

Megan Rangen
Senior Manager
+1 630 575 4275
megan.rangen@crowe.com

Accounting topics



FASB updates

Accounting standards update

Troubled Debt Restructurings (TDRs) and Vintage Disclosures

- Result of the post-implementation review (PIR) of the CECL standard (ASU 2016-13)
- At its February 2, 2022, meeting, the FASB voted to:
  - Eliminate TDR accounting for entities that have adopted the CECL standard
  - Require new disclosures for modifications to borrowers experiencing financial difficulties
  - For the vintage table, require gross charge-off information by year of origination
    - Note: vintage table is only required for public business entities (PBEs)
  - Prospective adoption
  - Effective for fiscal years beginning after December 15, 2022, with early adoption permitted for those who have already adopted CECL
- Final ASU – expected soon

FASB project

Identifiable Intangible Assets and Subsequent Accounting for Goodwill

- FASB project currently in process to revisit the subsequent accounting for goodwill and identifiable intangible assets
- Would apply more broadly to all entities (not just those entities that qualify for the private company alternative)
- Considering an impairment-with-amortization model
- FASB is currently gathering additional information and performing outreach to assist with their discussions on the details of the what the new ASU would include

CECL

Polling question

Where are you in your CECL implementation process?

A. CECL model developed and running parallel – we're ready to adopt
B. CECL model developed and hoping to run parallel soon
C. CECL implementation plan established – working through the details
D. In the process of developing CECL implementation plan
E. Have not started on CECL implementation yet

CECL

ASU No. 2016-13, "Financial Instruments – Credit Losses (Topic 328)"

The effective date is for fiscal years beginning after Dec. 15, 2022 (after a delay). All credit unions should expect to adopt in the subsequent year (effective Jan. 1, 2023).

Regulatory capital impact – Phase-in over 3 years starting with the adoption date impact amount

AICPA Audit & Accounting Guide: Credit Losses (November 2021)

Provides insights and observations from nearly 150 financial institutions that already adopted CECL

Chapters include internal controls and governance, audit objectives and procedures, comments on accounting issues, presentation and disclosure, and communications with others

Link to AICPA website: Audit and Accounting Guide: Credit Losses

CECL

Best practices and observations

- Expect an increase in the reserve as a result of the adoption of CECL – magnitude of increase may depend on composition of the loan portfolio
- Most have used a third-party application or provider to assist with their CECL model (expectations for model validation)
- Still there – adjustments for current conditions (qualitative factors)
- Consider a CECL methodology that is appropriate for the complexity of your loan portfolio and the resources available at your credit union
- Advantages of running parallel prior to adoption
- Involve your auditors early and often in the implementation process

Leases

Leases

ASU No. 2016-02, "Leases (Topic 842)"

Standard requires leases with a term greater than 12 months (original term) to be recorded on the balance sheet.

- Right-of-use (ROU) asset
- Lease liability
  - Lease term
  - Lease payment (net of any incentives known)
  - Discount rate

Leases that include rent escalations, lease incentive or initial direct costs could result in a ROU asset and lease liability being different.

At initial adoption, differences run through opening equity balance.

The effective date is for fiscal years beginning after Dec. 15, 2021 (after a delay). All credit unions should adopt in the current year (effective Jan. 1, 2022).

Leases

Best practices and observations

Most entities did not use the comparative transition option of applying the transition requirements.

Renewal periods should only be included in lease term if it is reasonably certain you will exercise the renewal option.

Items such as free rent period or tenant allowances will have an impact on the calculation and often result in differing ROU asset and lease liability.

There are challenges in estimating the incremental borrowing rate. There is also a practical expedient to elect the use of a risk-free rate if an incremental borrowing rate is not present.

Identify embedded leases; consider materiality of leases to the credit union.

Leases

Required disclosures

Nature of leases	Not-yet commenced leases	Significant judgments and assumptions
Composition of total lease cost	Weighted average lease term and discount rate	Sub-lease arrangements
Maturity analysis of lease liabilities	Related-party leases	Practical expedients

https://www.crowe.com/insights/asset/2/2021-illustrative-financial-statements-for-financial-institutions

Practice issue

Other topics

Collateral assignment split-dollar policy

Typical collateral assignment arrangement

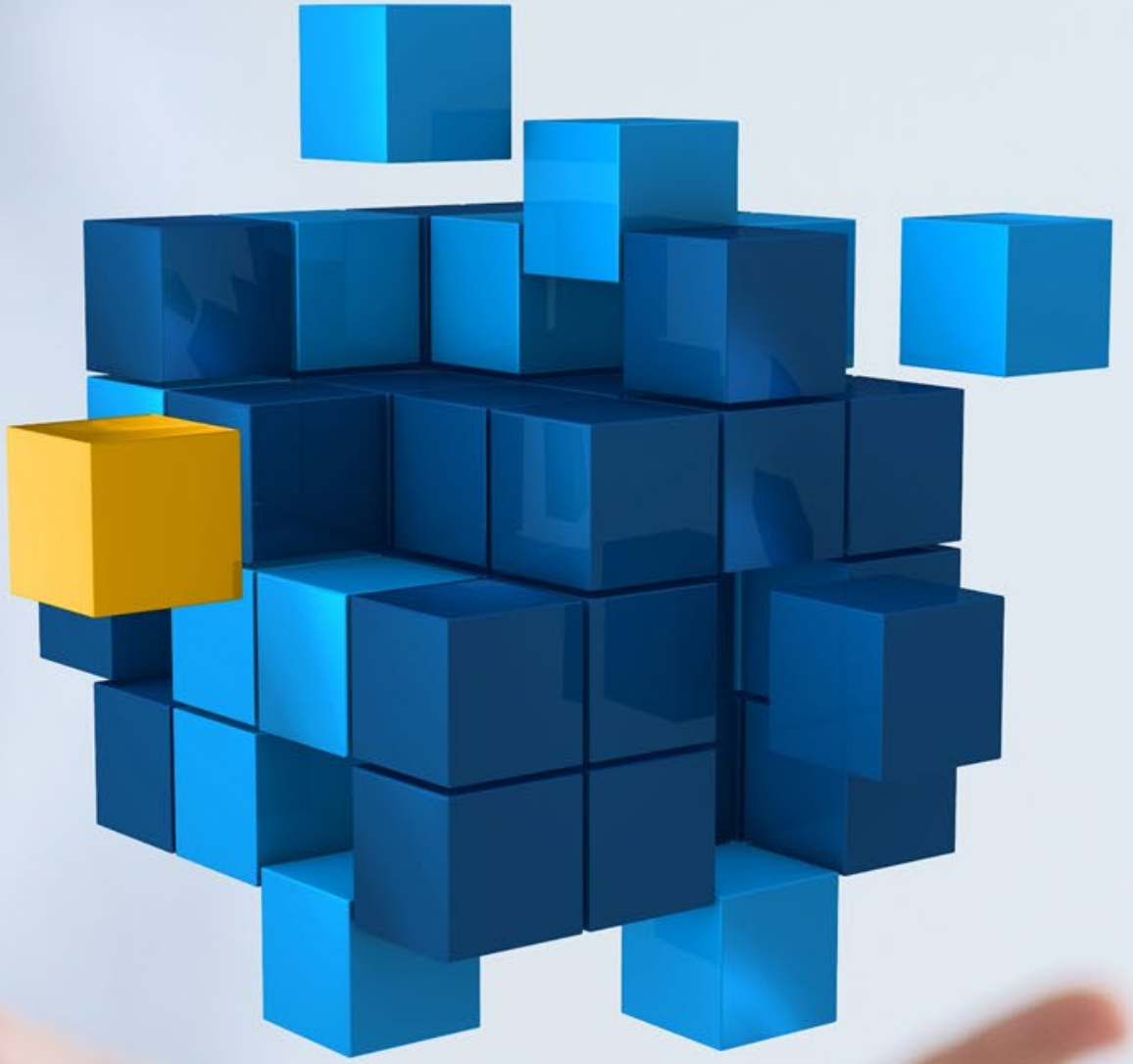
- Credit union has a non-recourse loan to an employee, collateralized by cash surrender value (CSV).
- Employee owns life insurance policy and endorses death benefits to CU equal to the loan amount plus accrued interest.

Question: What is necessary if the CSV is less than the loan amount?

Answer: The loan is written down to CSV (EITF 06-10) and a loss taken through the income statement.

Loans taken against the policy may also impact the CSV.

Regulatory update



NCUA supervisory priorities

Examinations primarily continuing off-site with heavy emphasis on:

- **Credit risk management**
  - Concentration risk
  - Real estate loans / member business loans
  - Examiners focusing reviews on policies related to workout strategies and risk management practices
- **Cybersecurity risk**
- **BSA / AML & terrorist financing**
- **Third-party risk management**

Polling question

What do you expect to be the biggest regulatory compliance challenge for your institution during 2022?

A. BSA/AML compliance
B. Climate financial risk management
C. Cybersecurity
D. Consumer compliance / fair lending
E. Third-party risk management
F. Other / don't know

NCUA supervisory priorities

- **Cybersecurity risk management**
  - Ransomware, third-party/supply chain risks
  - NCUA developing refined exam procedures around info security – piloting in 2022 and finalizing later in the year
  - October 2021: NCUA released the Automated Cybersecurity Evaluation Toolbox (ACET) – aligns with FFIEC self-assessment tool / used to measure cybersecurity preparedness
  - NCUA cybersecurity resources

    https://www.ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources

NCUA supervisory priorities

BSA / AML & terrorist financing

- AML Act of 2020 and CTA will prompt updates for BSA/AML policies and procedures
- Interagency efforts to improve SAR and CTR filings
- Watch for further updates to FFIEC BSA/AML exam manual
- NCUA BSA Resource Center https://www.ncua.gov/regulation-supervision/regulatory-compliance-resources/bank-secrecy-act-resources

NCUA supervisory priorities

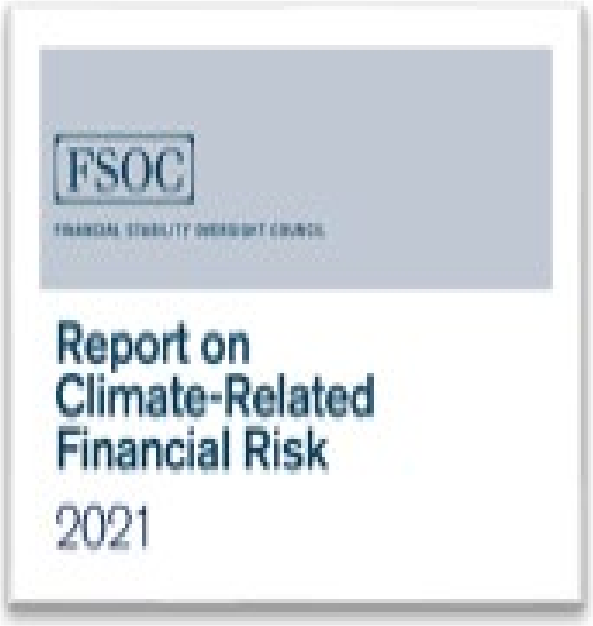
Third-party risk management / heavy emphasis on fintechs

- NCUA created Office for Financial Technology and Access
- NCUA statement on digital assets / crypto relationships
  - https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/relationships-third-parties-provide-services-related-digital-assets
- **PWG report on Stablecoins**
  - https://home.treasury.gov/news/press-releases/jy0454

NCUA supervisory priorities

Developing climate financial risk supervisory policy

- **Financial Stability Oversight Council report**
  - https://home.treasury.gov/system/files/261/FSOC-Climate-Report.pdf
- "*As a regulator and insurer, the NCUA will continue to work to ensure that the institutions it oversees remain resilient against all material risks, including climate financial risk.*"
  – NCUA Chairman Harper, Nov. 18, 2021, statement on NCUA strategic plan for 2022-2026



NCUA supervisory priorities

Capital adequacy and risk-based capital rule implementation

- Complex credit unions (over $500 million in assets)
- NCUA webinars on Call Report changes effective on March 31, 2022

CAMELS ratings

- "S" component added for sensitivity to market risk (Oct. 2021 final rule)
- Effective for exams starting April 1, 2022

Proposed succession planning rules (January 2022)

https://www.federalregister.gov/documents/2022/02/03/2022-02038/succession-planning

- Comment period closes April 4, 2022

Consumer compliance

Regulatory focus

NCUA will continue to examine for compliance with applicable consumer financial protection laws and regulations during every federal credit union examination.

Fair lending programs

- Risk assessment
- Monitoring and analysis
- Vendor and model-related risk
- Complaints
- Servicing and loss mitigation

Recent NCUA webinar indicated they were identifying quite a few results within the HMDA data presenting potential fair lending disparate impacts based upon marital status and gender.

Do you know what your data will reflect?

Regulatory focus

Headlines over the last three months have shed light on the Overdraft topic by the regulators. Have you considered the ramifications of maintaining the status quo?

Overdraft programs

- Consider fee amounts and limits, including a de minimis amount and daily limit. Are you in line with your geographic peers?
- Consider a certain account that has overdraft privilege.
- Monitor complaints to be proactive.
- Monitor returned fees for disparate impact/treatment.

Do you know what your data will reflect?

Regulatory focus

NCUA will continue to examine for compliance with applicable consumer financial protection laws and regulations during every federal credit union examination.

Fair Credit Reporting Act

- Did we handle our members' data according to the CARES Act requirements?
- When the dust settles from the last couple years, are we confident that have been reporting timely and accurately?
- Have we tested the integrity of our Metro 2 reporting?
- Are we monitoring complaints for FCRA-related complaints?
- Is our dispute process handled centrally, or is it decentralized? Are we confident it is handled consistently? (e.g., operational procedures and guidance in the first line)

Do you know what your data will reflect?

Regulatory focus

What else should we be thinking about?

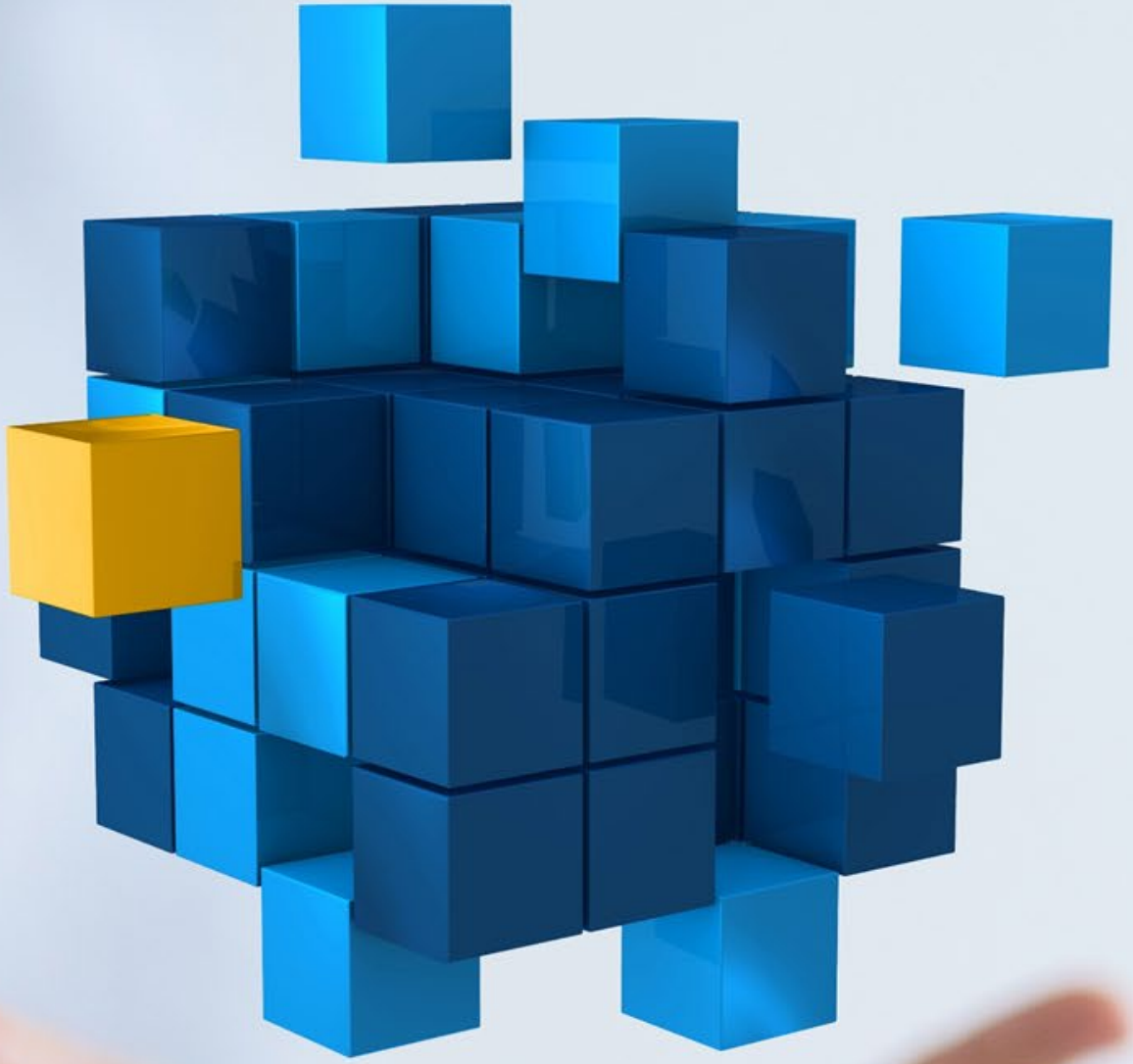
- *Servicemembers Civil Relief Act*
- *Electronic Fund Transfer Act*
- UDAAP-related risk across the enterprise
- Monitoring of vendors (overdraft vendors, mortgage sub-servicers, flood vendors)
- Relationships with fintechs (Are we confident in their compliance program, models, and complaint management?)

Polling question

If you had a little extra time and a little extra budget, where would you spend it?

A. BSA/AML compliance
B. Fair lending program and data analysis
C. Complaint management software
D. Compliance risk assessment and program development
E. Dinner for my team
F. Other / don't know

Cybersecurity topics



Polling question

Is your organization currently using or planning to implement robotic process automation (RPA) in the future?

A. We have bots in production today.

B. We are in the process of developing bots and plan to go live in 2022.

C. We have plans to utilize bots in the next 1-2 years.

D. We would like to implement RPA but don’t know where to start.

E. We do not plan on using RPA.

Financial services continues to observe persistent and ever-present cyber threat actors.

Digital payment fraud
Business email compromise (BEC)
General theft/breach of electronic data
Service interruption/disruption

Social engineering
Malware/ransomware
Third/fourth/fifth-party compromise
Applications (APIs/insecure code)

People continue to be the primary facilitator of successful cyberattacks.

Individuals continue to demonstrate a lack of awareness and/or attentiveness to ongoing attacks, which continuously aim to mislead or misuse a person's trust and access.

Banking data continues to hold value to criminals.

“Bank,” “bank identification number,” “CVV,” “Visa,” and “SSN” are all top terms being actively searched within the dark web (a secure and anonymous platform known to be used to communicate, transfer, exchange, and share information).

Digital transformation and remote working have accelerated the possibility of cyberattacks.

A bank’s attack surface continues to expand as more retail and commercial services/capabilities are made accessible from the internet, mobile devices, and vendors.

Refreshed guidance, frameworks & assessments

January 2021 – The Federal Reserve banks implement a Security and Resiliency Assurance Program that all banks must complete, starting in 2021.

June 2021 – “Architecture, Infrastructure, and Operations” FFIEC handbook introduced.

August 2021 – FFIEC “Authentication and Access to Financial Institution Services and Systems” guidance released.

Risk transference becomes more costly and difficult

Insurance premiums are rising (50%-300%). New coinsurance and sublimited coverages exist, specific to extortion losses (ransomware).

New “minimum security controls,” such as MFA, remote access restrictions, encryption, segmentation, backups, and EDR are requirements.

Managed service providers continue to be prime targets for cyberattacks.

Updated plans, practices & strategy

Are we targeted?

How prepared are we?

Are we doing enough?

Cybersecurity governance and board involvement

Cybersecurity and cyber risk are organizational needs that require attention. This is not “an IT problem.”

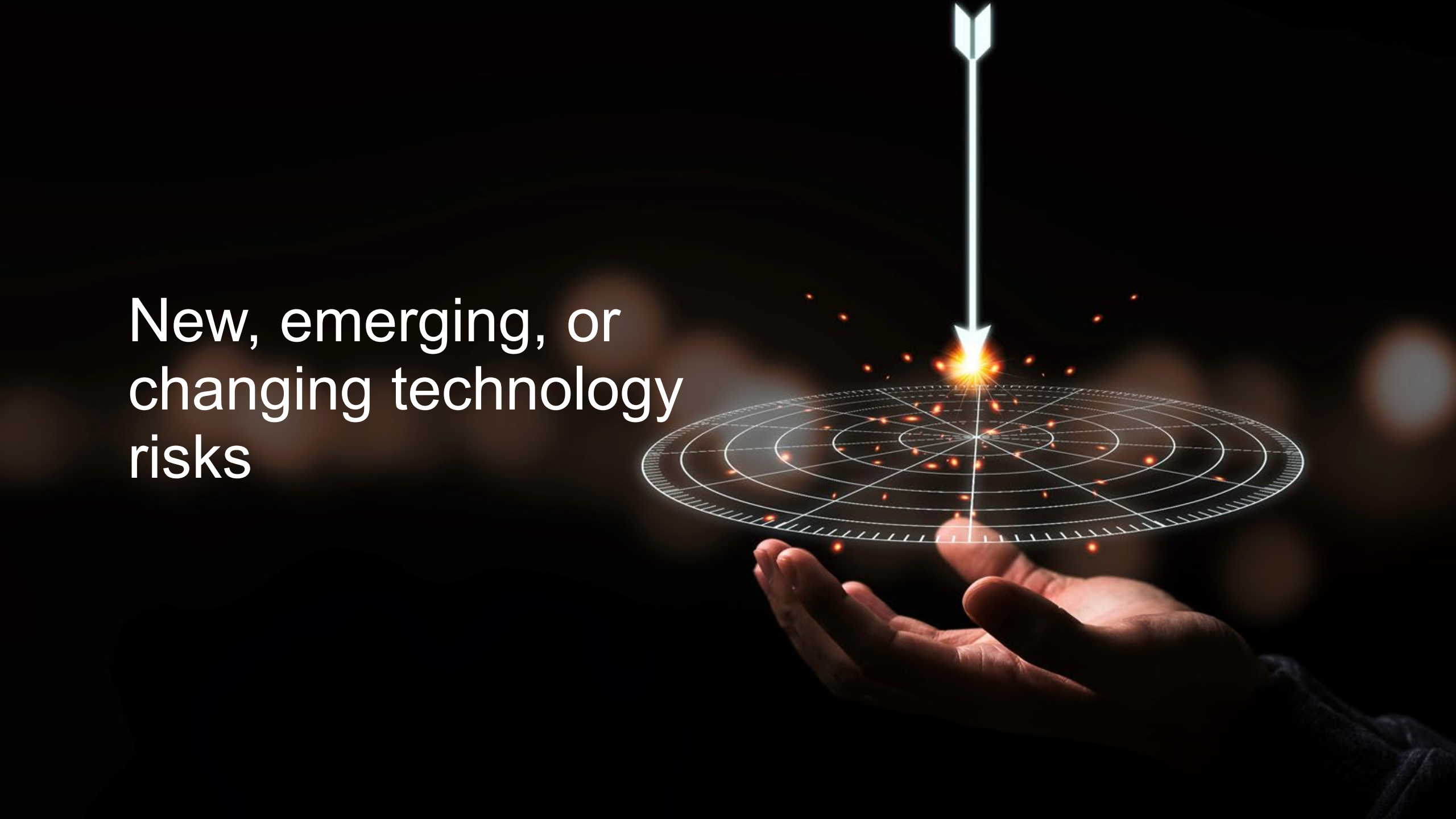
Like other risks, cybersecurity considerations must be incorporated into both operational and strategic decision-making processes (including M&A, transformation, development, and product choices).

Organizational alignment, cooperation, and appropriate governance

Functions that support cybersecurity initiatives must be adequately staffed, funded, and monitored. Clear roles and responsibilities are established between operational, risk management, and audit roles that touch on cybersecurity. The board of directors should seek opportunities to build upon its existing knowledge on IT/cybersecurity as it aligns to the bank’s portfolio and digital goals. Cybersecurity should be a routine agenda topic during full board meetings and the board should recruit or contract cybersecurity expertise for guidance and consultation as necessary.

Understand effects of cybersecurity on <u>your</u> business objectives > **Obtain adequate representation and diverse expertise** > **Comprehend/establish <u>your</u> organization’s risk posture and cyber appetite.**

New, emerging, or changing technology risks



New, emerging, or changing technology risks

Targeted network-based penetration testing

Overview: Clients continue to seek new and innovative ways to test and challenge their controls, processes, and employees by performing targeted attacks against their own networks and systems. Crowe continues to execute penetration tests for most of our clients. In order to dig a bit deeper and/or evaluate more specific possible weaknesses, more advanced levels of testing may be valuable. These types of tests are referred to as "Red Team," "Purple Team," and/or "simulation tests," where we narrow the focus of a test and increase depth, length of testing, and/or collaboration with those being tested.

Continued exploration in robotic process automation

Overview: Clients (or their vendors) continue to deploy robotic process automation (RPA), which drives lower costs and higher efficiency. Areas where banks are investing include loan applications and servicing, deposit account creation, account closure, customer service, know your customer (KYC) standards, quality assurance (QA) processing, and regulatory monitoring.

New, emerging, or changing technology risks (continued)

Sustained remote worker arrangements

Overview: Clients continue to oscillate between on-site, off-site, and hybrid work arrangements. Technology that enables sustained connectivity and access to banking applications has mostly been implemented, yet refinements around usability, security, and access will persist.

Data

Overview: Clients continue to explore meaningful ways to correlate customer data and recognized patterns/trends to drive business decision-making, customer targeting, and increased revenue. Amassing data, data sharing/selling, and computing outcomes requires increased access controls, monitoring, distinguished roles, and defined data structures. Data governance continues to be a focus of examiners.

New, emerging, or changing technology risks (continued)

Pandemic planning

Overview: Adjustments to how our clients' employees and systems are accessible and utilized (due to COVID-19 and U.S. weather events) drove needed changes in multiple supporting operations and respective documentation, including disaster recovery, business continuity, and third-party risk management.

Migration to the cloud

Overview: The last 2 years saw a tremendous acceleration of cloud migrations, mostly due to the need to sustain employee connectivity. This primarily includes Microsoft 365, Microsoft Azure, Amazon AWS, and Google Cloud Platform in technology but also includes Fiserv, JHA, Oracle, SAP, and Salesforce for operational areas.

Peer groups

Interested in diving deeper into these topics and discussing with your peers?

Crowe hosts semi-annual credit union peer groups for risk and finance individuals. Sign up for emails from Crowe and look for our invitations in the spring and fall.

https://www.crowe.com/registration

Thank you

Niall Twomey
Principal
+1 630 574 1806
niall.twomey@crowe.com

Rob Blanchard
Managing Director
+1 614 469 4003
rob.blanchard@crowe.com

Dennis Hild
Managing Director
+1 202 552 8086
dennis.hild@crowe.com

Jason Naber
Senior Manager
+1 616 242 6124
jason.naber@crowe.com

Megan Rangen
Senior Manager
+1 630 575 4275
megan.rangen@crowe.com