**SBS CyberSecurity**
700 S. Washington Avenue, Suite 200
Madison, SD 57042

July 19, 2026

Executive Secretary
Federal Financial Institutions Examination Council
L. William Seidman Center
Mailstop: E-2035-c
3501 Fairfax Drive
Arlington, VA 22226-3550

**Re: Uniform Financial Institutions Rating System — Docket ID OCC-2026-0562**

To the Federal Financial Institutions Examination Council:

SBS CyberSecurity appreciates the opportunity to comment on the Federal Financial Institutions Examination Council's proposed revisions to the Uniform Financial Institutions Rating System, commonly known as CAMELS. SBS supports the FFIEC's goals of improving transparency, consistency, and predictability in the examination process. Financial institutions should understand how supervisory ratings are determined, and ratings should be tied to meaningful risk rather than examiner discretion or documentation requirements that are not indicative of material risk.

At the same time, SBS is concerned that removing the special consideration historically given to the Management component may unintentionally reduce supervisory emphasis on technology governance, cybersecurity governance, third-party risk management, operational resilience, independent testing, and a well-managed Information Security Program. Those areas are not secondary concerns in modern banking. They are core safety-and-soundness issues, as well as critical elements to the resilience and continued operations of the financial sector as a whole. While SBS supports the FFIEC's effort to focus ratings on material financial risk, we believe technology governance, cybersecurity, and independent testing should be viewed as leading indicators of material risk rather than process-oriented considerations.

SBS works with approximately 24% of FDIC-insured banks, as well as credit unions and other non-bank financial institutions across the country. For more than 22 years, we have helped institutions manage Information Security Programs, conduct risk assessments, govern third-party risk, test people, process, and technology, and improve operational resilience. Our concern is simple: cybersecurity and technology failures often begin as governance, implementation, or validation failures long before they appear as capital, earnings, liquidity, or asset-quality problems.

> **SBS's core concern:** The supervisory framework should not unintentionally encourage institutions to underweight governance weaknesses, technical control gaps, or insufficient independent testing simply because those weaknesses have not yet produced observable financial deterioration.

## Technology Risk Has Changed Since the Last Major CAMELS Revision

Financial institutions are more dependent on technology today than at any point in the history of banking. Core processing, digital banking, payment systems, cloud platforms, APIs, fintech integrations, managed service providers, and other third-party technology relationships are now essential to delivering financial services.

SBS often teaches financial institutions to think of themselves as technology companies. That does not mean every bank or credit union needs to become a software company. It means technology is now central to how institutions serve customers, move money, protect data, remain available, and compete. When technology fails, the institution's operations and customers are directly affected, which we can all agree is not good for our financial institutions, their customers, the industry, or our country.

A ransomware incident, core processing outage, cloud misconfiguration, vendor disruption, data breach, or digital banking outage can affect customer confidence, liquidity, earnings, compliance, and institutional stability. These are not merely technical events. They are business events, operational events, and safety-and-soundness events.

## Governance, Implementation, and Independent Testing All Matter

The proposal's focus on material financial risk is understandable. However, in cybersecurity and technology risk management, many of the most important warning signs appear before a measurable financial loss occurs. Cybersecurity weaknesses frequently serve as leading indicators of future operational, reputational, and financial risk. That is the purpose of risk management: to identify and mitigate risk before it becomes a loss event.

SBS believes effective technology and cybersecurity risk management requires three connected disciplines. First, institutions must establish governance through board oversight, risk assessment, strategy, policies, reporting, and accountability. Second, institutions must implement technical and operational controls that reflect those risk-based decisions. Third, institutions must independently test people, process, and technology to validate whether those controls are actually working. Independent testing identifies weaknesses before they become material incidents, regulatory findings, or financial losses.

Weaknesses such as poor board reporting, incomplete asset inventories, weak vendor oversight, failed patch management, insufficient logging and monitoring, weak access controls, aging audit findings, incomplete penetration testing, insufficient incident response testing, or an outdated Information Security Program may not immediately affect capital, earnings, liquidity, or asset quality. But these weaknesses often represent the conditions that allow a material incident to occur later.

## The Management Component Has Served an Important Safety-and-Soundness Function

The Management component has historically provided a mechanism for examiners to evaluate whether the board of directors and management are effectively identifying, measuring, monitoring, and controlling risk. For technology and cybersecurity, this has been especially important because many technology risks are governance risks first, making governance a critical leading indicator of future operational and financial concerns.

If the proposal removes special consideration for Management while also narrowing the impact of specialty review findings, the result could be a weaker supervisory signal around the governance, technical control, and independent testing practices that prevent technology failures and cybersecurity incidents. Cybersecurity remains one of the most significant operational and strategic risks facing financial institutions. A diminished focus on cybersecurity within the supervisory framework and examinations will undoubtedly lead to a diminished focus on cybersecurity at the board level (already a struggle) and more importantly, diminished cybersecurity budgets and support.

That outcome would be inconsistent with the way modern financial institutions operate. Technology governance, cybersecurity operations, vendor dependency, resilience planning, and independent validation are not peripheral to the condition of a financial institution. They are leading indicators of an institution's ability to serve customers safely and reliably and to avoid future safety-and-soundness concerns.

## Information Security Programs Should Be Living Management Systems

SBS believes a valuable Information Security Program should help an institution make better decisions. A strong program begins with risk assessments, documents risk-based decisions, operationalizes controls, tests whether those controls are working, reports meaningful information upstream, and improves over time.

This risk-management cycle is not a compliance exercise. It is how institutions protect customer information, manage technology risk, oversee third parties, maintain operational resilience, and create accountability. Technology risk management deserves the same rigor, visibility, and board-level oversight traditionally applied to loan risk management. Both disciplines exist to help institutions make informed decisions about critical business risks.

Reducing the practical supervisory weight of Management without elevating technology and operational resilience as a standalone category may make it more difficult for cybersecurity and technology leaders to obtain the attention and resources necessary to maintain these programs effectively.

What gets measured gets managed. What gets examined gets funded. If technology governance, cybersecurity operations, and independent testing are perceived as less likely to affect supervisory ratings, institutions may naturally shift attention and investment elsewhere. Allowing financial institutions to reduce cybersecurity budgets, stretch independent assessment timelines, and generally be less safe and sound from a technology standpoint in today's constantly evolving threat landscape would be an unintended, harmful, and avoidable outcome for the industry.

## Support for Considering a Technology & Operational Resilience Component

SBS strongly appreciates the public comment submitted by Vincent J. Buono, CISA, CISM, retired OCC Bank IT Analyst, recommending that the FFIEC consider adding a distinct Technology & Operational Resilience component to the rating framework. His proposed **CAMELTS** structure recognizes that technology failures, cyber events, operational outages, third-party dependencies, and data integrity issues can directly affect safety and soundness.

SBS does not suggest that every detail of a new Technology & Operational Resilience component can or should be finalized within this comment. However, the direction is appropriate and merits serious consideration. Technology risk is no longer merely a subset of Management risk. Technology and operational resilience are now foundational to how financial institutions function.

SBS recommends that the FFIEC evaluate a Technology & Operational Resilience component that bridges familiar regulatory and industry concepts rather than creating an entirely unfamiliar taxonomy. The component should align to the NIST Cybersecurity Framework 2.0 functions, the FFIEC IT Examination Handbook, and the former FFIEC Cybersecurity Assessment Tool domains while explicitly distinguishing governance, implementation, resilience, and independent validation.

## Recommended Technology & Operational Resilience Evaluation Domains

SBS recommends the following nine-domain structure, which keeps most of Mr. Buono's core concepts intact, includes a few additional domains SBS sees as critically important to a modern Information Security Program, and uses language that should be familiar to financial institutions, examiners, auditors, and cybersecurity practitioners.

| Domain | Relevance Statement | NIST CSF 2.0 Alignment | FFIEC IT Handbook Alignment | Former FFIEC CAT Alignment |
|---|---|---|---|---|
| **1. Technology Governance & Risk Management** | Board and management oversight determines whether technology and cybersecurity risks are understood, prioritized, funded, monitored, and remediated. | Govern | IT Management; AIO governance concepts | Cyber Risk Management & Oversight |
| **2. Information Security Program Management** | A living Information Security Program translates risk assessments into documented decisions, accountability, controls, reporting, and continuous improvement. | Govern; Identify | Information Security; IT Management | Cyber Risk Management & Oversight; Cybersecurity Controls |
| **3. Cybersecurity Operations & Technical Controls** | Technical safeguards such as identity management, vulnerability management, monitoring, logging, endpoint protection, and network security reduce the likelihood and impact of cyber events. | Protect; Detect | Information Security; AIO | Cybersecurity Controls |
| **4. Third-Party & Cloud Risk Management** | Third-party providers, cloud platforms, fintech partners, and service providers create concentration, operational, security, and dependency risks that remain the institution's responsibility. | Govern; Identify | IT Management; Information Security; AIO; Technology service provider guidance | External Dependency Management |
| **5. Technology Operations & Infrastructure Management** | Stable, resilient, and well-managed technology operations are necessary to maintain availability, reliability, and secure delivery of critical financial services. | Protect; Detect | AIO; Information Security | Cybersecurity Controls; External Dependency Management |
| **6. Incident Response & Cyber Recovery** | The ability to rapidly detect, contain, eradicate, recover from, and learn from cyber incidents directly influences safety-and-soundness outcomes. | Detect; Respond; Recover | Information Security; BCM | Cyber Incident Management & Resilience |
| **7. Business Continuity & Operational Resilience** | Institutions must sustain critical operations and recover essential services during disruptions affecting technology, facilities, personnel, vendors, or external events. | Recover | BCM; AIO | Cyber Incident Management & Resilience; External Dependency Management |
| **8. Independent Testing & Assurance** | Independent audits, assessments, exercises, vulnerability assessments, penetration tests, and social engineering tests validate whether people, process, and technology controls are actually working as intended. | Govern; Protect; Detect; Respond; Recover | Information Security; BCM; AIO; Audit-related examination procedures | Cybersecurity Controls; Cyber Incident Management & Resilience |
| **9. Emerging Technology & Digital Innovation Risk** | AI, APIs, automation, digital banking, fintech integration, and future technologies introduce new opportunities and new sources of operational and cybersecurity risk. | Govern; Identify | AIO; IT Management; Information Security; DA&M concepts | Cyber Risk Management & Oversight; External Dependency Management |

## Recommendations

1. **Preserve a strong connection between governance and composite ratings.** Governance weaknesses can be meaningful safety-and-soundness concerns even before financial deterioration is observable.
2. **Explicitly recognize technology and cybersecurity risk as safety-and-soundness issues.** Technology resilience, cybersecurity governance, vendor dependency, digital banking availability, and technical control implementation are fundamental to modern financial institution stability.
3. **Ensure specialty technology and cybersecurity findings continue to influence supervisory outcomes.** Such findings should matter when they demonstrate elevated risk, weak governance, significant control gaps, poor remediation discipline, or insufficient independent validation, not only after a financial loss occurs.
4. **Evaluate a dedicated Technology & Operational Resilience component.** The FFIEC should seriously consider Mr. Buono's recommendation for a separate component or an equivalent mechanism that gives technology risk appropriate visibility.
5. **Use familiar regulatory language and framework mappings.** A Technology & Operational Resilience component should bridge NIST CSF 2.0, FFIEC IT Handbook concepts, and the former FFIEC CAT domains so institutions and examiners can build on familiar expectations, including governance, implementation, resilience, and independent testing.
6. **Use both leading and lagging indicators.** Risk assessments, governance, technical control maturity, testing, incident readiness, vendor oversight, and remediation discipline should be considered alongside financial performance and material loss events.
7. **Encourage institutions to maintain living Information Security Programs.** An effective Information Security Program should document decisions, operationalize controls, support testing, inform board reporting, and drive continuous improvement.
8. **Explicitly recognize independent testing as a required validation discipline.** Annual and independent testing of people, process, and technology should be considered a core indicator of whether the institution's risk management program is functioning as intended.

## Conclusion

SBS supports the FFIEC's effort to improve clarity, consistency, and transparency in the CAMELS rating framework. However, modernization should not come at the cost of reducing emphasis on cybersecurity governance, technology oversight, third-party risk management, operational resilience, technical control implementation, or independent testing.

Financial institutions are more technology-dependent today than at any point in the history of banking. Strong cybersecurity governance is not a paperwork exercise. Technical controls are not optional implementation details. Independent testing is not a secondary activity. Together, these disciplines help institutions identify risk, implement controls, validate effectiveness, and improve over time.

That is not separate from safety and soundness. In modern banking, that is safety and soundness.

SBS respectfully encourages the FFIEC to ensure that any final revisions preserve strong supervisory emphasis on governance and to consider whether technology and operational resilience should receive explicit treatment within the rating framework, using a familiar structure that connects to NIST CSF 2.0, the FFIEC IT Examination Handbook, and the former FFIEC Cybersecurity Assessment Tool domains.

Respectfully submitted,

**Jon Waldman**
President and Co-Founder
SBS CyberSecurity

## References


- FFIEC, "Agencies Request Comment on Financial Institutions Rating System," May 19, 2026: https://www.ffiec.gov/news/press-releases/2026/pr-05-19
- Regulations.gov, "Uniform Financial Institutions Rating System," Docket ID OCC-2026-0562, Document OCC-2026-0562-0003: https://www.regulations.gov/document/OCC-2026-0562-0003
- Vincent J. Buono, public comment attachment, OCC-2026-0562-0014: https://www.regulations.gov/comment/OCC-2026-0562-0014
- NIST, "The NIST Cybersecurity Framework (CSF) 2.0," February 26, 2024: https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20
- OCC Bulletin 2016-27, "FFIEC Information Technology Examination Handbook: Revised Information Security Booklet": https://www.occ.gov/news-issuances/bulletins/2016/bulletin-2016-27.html
- OCC Bulletin 2019-57, "FFIEC Information Technology Examination Handbook: Revised Business Continuity Management Booklet": https://www.occ.gov/news-issuances/bulletins/2019/bulletin-2019-57.html
- FDIC FIL-47-2021, "Updated FFIEC IT Examination Handbook – Architecture, Infrastructure, and Operations Booklet": https://www.fdic.gov/news/financial-institution-letters/2021/fil21047.html