

What does the new interagency guidance mean for bank third-party risk management programs?



Evolved regulatory guidance aligns

with evolved third-party risk

In June 2023, the primary federal banking regulators responsible for overseeing third-party risk management (TPRM) programs in the banking industry issued new guidance, "Interagency Guidance on Third-Party Relationships: Risk Management."

The new guidance replaces existing TPRM guidance from all three agencies: the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corp. (FDIC), and the Board of Governors of the Federal Reserve System (Fed).



The agencies' goal is to create alignment and help banking organizations manage risks associated with third-party relationships, including fintechs.¹

Based on our TPRM specialists' review of the interagency guidance, we have several broad takeaways:

- In response to the ongoing rise in third-party incidents and cybersecurity breaches, the agencies seek to clarify their expectations regarding how banks manage third-party risk.
- The new guidance attempts to align the level of regulatory expectation more accurately with the level of risk regardless of a banking organization's asset size or primary regulator.
- The interagency guidance addresses the significant changes in outsourcing relationships with third parties since the previous TPRM guidance was published. Banking organizations now outsource more bank processes than ever before, and the industry has experienced a rapid spike in banking as a service (BaaS) relationships.

Many leaders in the banking industry are wondering: What does the new guidance mean for our organization's TPRM program?

Below is a high-level summary of expected changes based on a banking organization's current regulator.

FDIC and Fed

Banking organizations regulated by the FDIC and Federal Reserve System will see the most change and should anticipate significant – although risk-adjusted – enhancements to regulatory requirements across many different areas.

Smaller organizations with complex, risky third-party relationships should expect the biggest impact.

Areas of change:

- The list of due diligence topics to be covered under a third-party assessment has become significantly more extensive in the guidance.
- The guidance expands the level of detail in many areas, especially those related to oversight and accountability.
- Terminations of third parties and ongoing monitoring are now covered in a stand-alone section that organizations must address.
- (Fed only) The scope of the relationships covered under the guidance is expanded. Previously, the guidance had covered only traditional outsourcing relationships.

OCC

For banking organizations regulated by the OCC, the new guidance contains some minor clarifications and small enhancements, but most areas remain materially the same.

Areas of change:

- The definition of critical vendors has been enhanced to provide more guidance.
- The guidance is slightly more prescriptive in areas such as contract negotiation, business continuity, and responsibilities for providing, receiving, and retaining information.





Crowe third-party risk management specialists have reviewed the interagency guidance and created a visual guide to illustrate the anticipated changes from existing TPRM guidance. The tables on the following pages summarize the degree of change in various stages of the risk management life cycle for each regulatory agency.

Stage of risk management life cycle	осс	Fed	FDIC
Planning		•	•
Due diligence and third-party selection		•	•
Strategies and goals		•	
Legal and regulatory compliance		•	•
Financial condition			•
Business experience		•	•
Qualifications and backgrounds of company principals		•	
Risk management		•	•
Information security		•	
Management of information systems		•	•
Operational resilience		•	
Incident reporting and management programs		•	•
Physical security		•	
Reliance on subcontractors		•	
Insurance coverage	•	•	
Contractual arrangements with other parties		•	•

Substantially the same as previous
 Somewhat enhanced
 Materially expanded or did not exist in previous guidance

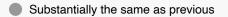
Stage of risk management life cycle	осс	Fed	FDIC
Contract negotiation	•	•	•
Nature and scope of arrangement	•	•	•
Performance measures or benchmarks	•	•	
Responsibilities for providing, receiving, and retaining information	•		•
The right to audit and require remediation	•	•	
Responsibility for compliance with applicable laws and regulations	•	•	•
Cost and compensation	•	•	
Ownership and license	•	•	
Confidentiality and integrity	•	•	
Operational resilience and business continuity	•	•	
Indemnification and limits on liability	•	•	
Insurance	•	•	•
Dispute resolution	•	•	
Customer complaints	•	•	
Subcontracting	•		•
Foreign-based third parties	•	•	
Default and termination	•	•	
Regulatory supervision			

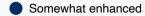


Materially expanded or did not exist in previous guidance



Stage of risk management life cycle	occ	Fed	FDIC
Ongoing monitoring			
Termination	•		
Governance			
Oversight and accountability			•
Independent reviews	•		•
Documentation and reporting	•		•
Supervisory reviews of third-party relationships			•





Materially expanded or did not exist in previous guidance



Have more questions? Want a detailed analysis of the new interagency guidance, tailored to your organization?

Reach out to our third-party risk management team, and we can provide an in-depth breakdown of the effects of the regulatory changes based on your specific situation and regulator. We can also answer any questions you might have and talk about how to optimize your third-party risk management program to prepare for the changes.



Jill Czerwinski
Principal
Third-Party Risk
Management Leader
+1 630 575 4317
jill.czerwinski@crowe.com



Morgan Strobel

Financial Services Consulting +1 312 966 3062 morgan.strobel@crowe.com

Learn more about our TPRM services at crowe.com



"Crowe" is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. "Crowe" may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S. member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. © 2023 Crowe LLP.