DHG

PERSPECTIVES

December 2021

IOSCO Releases New Guidance on Operational Resilience for Third-Party Outsourcing

On October 27th, 2021, The Board of the International Organization of Securities Commissions (IOSCO) published a set of updated outsourcing principles for regulated entities that outsource tasks to service providers. The updated Principles on Outsourcing[1] are based on the earlier Outsourcing Principles for Market Intermediaries in 2005 and Markets in 2009, but their application has been expanded and now includes trading venues, intermediaries, market participants acting on a proprietary basis, and credit rating agencies (CRAs).

The guidance also comprises a set of fundamental precepts such as the definition of outsourcing, the assessment of materiality and criticality, their application to affiliates, the treatment of sub-contracting and outsourcing on a cross-border basis.

IOSCO's newly formed Operational Resilience Group has been tasked with considering and reporting on issues raised by the COVID-19 pandemic relating to operational resilience, business continuity planning, and cyber security risks. The Group has expanded its seven Principles on Outsourcing, outlined below, to encompass these emergent challenges and how regulated entities can best equip themselves to handle evolving relationships with their third-party suppliers and service providers.

IOSCO OUTSOURCING PRINCIPLE	DESCRIPTION	EXPANDED CONSIDERATIONS
PRINCIPLE 1 Due diligence in the selection and monitoring of a service provider and the service provider's performance	A regulated entity should conduct suitable due diligence processes in selecting an appropriate service provider and in monitoring its ongoing performance.	Consider the service level provisions that apply to the service providers depending on whether the staff is working onsite or remotely, and whether service providers and regulated entities have identified their dependencies and taken steps to mitigate the associated risks.
PRINCIPLE 2 The contract with a service provider	A regulated entity should enter into a legally binding written contract with each service provider, the nature and detail of which should be appropriate to the materiality or criticality of the outsourced task to the business of the regulated entity.	

© 2021 Dixon Hughes Goodman LLP. All rights reserved. DHG is registered in the U.S. Patent and Trademark Office to Dixon Hughes Goodman LLP.

IOSCO OUTSOURCING PRINCIPLE	DESCRIPTION	EXPANDED CONSIDERATIONS
PRINCIPLE 3 Information security, business resilience, continuity and disaster recovery	A regulated entity should take appropriate steps to ensure both the regulated entity and any service provider establish procedures and controls to protect the regulated entity's proprietary and client-related information and software, and to ensure a continuity of service to the regulated entity, including a plan for disaster recovery with periodic testing of backup facilities.	With respect to cyber security and resilience issues, consider the challenges posed by a remote working environment, the increased use of technology and the evolving threat landscape. Ensure that the third-party's testing of backup facilities uses severe but plausible scenarios which encapsulate multiple concurrent events. Consider the continuity and quality of outsourced tasks where the regulated entities' and third-party service providers' work forces are working remotely. This could include considering additional capabilities to safeguard the security and the accessibility of the remote network connection used by staff, as well as establishing procedures in business continuity plans and performing adequate testing to validate this capability.
PRINCIPLE 4 Confidentiality Issue	A regulated entity should take appropriate steps to ensure that service providers protect confidential information and data related to the regulated entity and its clients, from intentional or inadvertent unauthorized disclosure to third parties.	
PRINCIPLE 5 Concentration of outsourcing arrangements	A regulated entity should be aware of the risks posed, and should manage them effectively, where it is dependent on a single service provider for material or critical outsourced tasks or where it is aware that one service provider provides material or critical outsourcing services to multiple regulated entities including itself.	Assess and understand concentration risk from a technology and infrastructure perspective (e.g., cloud service providers), including the relationship between concentration risk and the physical location of the service provider.
PRINCIPLE 6 Access to data, premises, personnel, and associated rights of inspection.	A regulated entity should take appropriate steps to ensure that its regulator, its auditors, and itself are able to obtain promptly, upon request, information concerning outsourced tasks that is relevant to contractual compliance and/or regulatory oversight including, as necessary, access to the data, IT systems, premises and personnel of service providers relating to the outsourced tasks.	Consider the possibility of obtaining information regarding a third-party service provider from the regulated entity's or service provider's home country regulator, where there are difficulties arranging on-site inspections or otherwise obtaining information from the regulated entity itself.

IOSCO OUTSOURCING PRINCIPLE	DESCRIPTION	EXPANDED CONSIDERATIONS
PRINCIPLE 7 Termination of outsourcing arrangements	A regulated entity should include written provisions relating to the termination of outsourced tasks in its contract with service providers and ensure that it maintains appropriate exit strategies.	In addition to including termination provisions within service providers' contracts, a regulated entity should actively understand its contingency planning processes and incorporate appropriate exit strategies.

The updated principles aim to promote sound outsourcing practices across the Third-Party Risk Management (TPRM) Lifecycle while maintaining operational resilience across the organization. Organizations should consider the following action items while incorporating the additional guidance:

- Determine the applicability of these Principles to your Third-Party Risk Management Program, taking into consideration the scope and complexity of your third-party outsourcing arrangements
- Consider how the above guidance might translate to or reshape existing roles and responsibilities across your organization's first line of defense (operationalization of due diligence and monitoring requirements) and second line of defense (oversight and program governance)
- Update relevant policies, standards, and procedures to incorporate IOSCO's considerations for operational resilience as appropriate for your organization's risk appetite
- Review your TPRM Lifecycle to assess what is currently being done at each phase, identifying any bottlenecks, pain points, and gaps
- Include third-party contract provisions as appropriate to address the additional risks and/or material deviations in service level agreements resulting from the service provider being partially or wholly remote
- The report also briefly addresses how outsourcing integrates with cloud computing, how CRAs use and incorporate outsourcing, and how cloud computing is integrated into organizational strategies and structures.

HOW DHG CAN HELP

DHG Advisory provides services to clients for all aspects of third-party risk management, including framework development and implementation, risk assessment, and lifecycle development and monitoring. Our dedicated domain professionals are prepared to advise on the complexities of third-party risk and achieve strategic business objectives. For more information, please contact us at dhgadvisory@dhg.com.

YOUR CONTACTS

Prashant Panavalli
Principal, DHG Advisory
prashant.panavalli@dhg.com

Michael Rosen
Senior Manager, DHG Advisory
michael.rosen@dhg.com

Contributing Authors:
Ben Kornegay, Alex Monk

SOURCES

1 FR07/2021 Principles on Outsourcing (iosco.org)

The information set forth in this article contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by DHG or the author(s) as to any individual situation as situations are fact specific. The reader should perform its own analysis and form its own conclusions regarding any specific situation. Further, the author(s) conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2021 Dixon Hughes Goodman LLP. All rights reserved. DHG is registered in the U.S. Patent and Trademark Office to Dixon Hughes Goodman LLP.