riskrecon™
Control your third party risk reality.

You Can't Outsource Risk

A regulatory guide to third-party cyber security risk management

INTRODUCTION

Third parties are integral to the value chain—any given organization can have up to hundreds of vendors, depending on its size. Along with business process, IT bandwidth and application functionality, data also flows through that chain. While you can outsource systems and services, you cannot outsource your risk associated with that data and how it's managed. Regulators have been consistently and clearly giving that message for years, in writing and in practice.

For instance, the Federal Deposit Insurance Corporation (FDIC) issued this formal guidance in 2008: *"An institution's board of directors and senior leadership are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution" (*www.fdic.gov*).* That's pretty clear direction.

The same is true across regulated industries, where rules are set by a breadth of governing entities such as the FDIC, the Office of the Comptroller of the Currency, the Department of Health and Human Services, the Securities and Exchange Commission, the National Association of Insurance Commissioners, the New York Department of Financial Services, and even the European Union for those whose business ventures abroad. Add to that forty seven U.S. states have unique data privacy regulations on their books. It's a lot to track.

These regulators know that good risk management requires full transparency, which enables accountability and enforcement through constructive collaboration. But achieving deep third-party transparency is challenging; these companies are simply not part of your own organization so not subject to your direct oversight. The common practice of using risk questionnaires is helpful in periodically assessing the investments your third parties may have made in managing their cybersecurity risk. Unfortunately questionnaires don't tell you how well they implement and operate their programs.

But getting a handle on your third party risk is more important than ever. In the wake of the Facebook –Cambridge Analytica scandal and the reality of continual high profile cyber-attacks, the U.S. regulatory appetite may be trending toward stronger data management regulations; the European Union General Data Protection Regulation is a game-changer that will likely have ripple effects worldwide. The bottom line: it's time to up your third-party risk management game.

RiskRecon can help you continuously and objectively monitor how each of your vendors implements and operates their cybersecurity risk management program. This deep visibility will help you to better achieve your own risk management objectives and meet regulatory requirements to which you as the ultimate data owner are subject. To help you better understand the regulatory environment, this document provides you a list and references to the most pointed third-party risk management requirements prescribed by regulations since 2000.

riskrecon™
Control your third party risk reality.

Third Party Risk Management Regulations

FINANCIAL SERVICE SECTOR

Federal Financial Institutions Examination Council –

Risk Management of Outsourced Technology Services / FIL-81-2000 *(Issued 2000)*
"The board of directors and senior management are responsible for understanding the risks associated with outsourcing arrangements for technology services and ensuring that effective risk management practices are in place."

FFIEC Cybersecurity Assessment General Observations *(Issued 2014)*
"External dependency management includes the connectivity to third-party service providers, business partners, customers, or others and the financial institutions' expectations and practices to oversee these relationships.

"Many financial institutions have processes to manage third-party relationships and document their connections. Before executing a contract, it is important for management to consider the risks of each connection and evaluate the third party's cybersecurity controls. In addition, financial institutions should understand the third parties' responsibility for managing cybersecurity risk and incident response plans."

FFIEC IT Examination Handbook: Vendor and Third-Party Management
"Financial institutions should establish and maintain effective vendor and third-party management programs because of the increasing reliance on nonbank providers. Financial institutions must understand the complex nature of arrangements with outside parties and ensure adequate due diligence for the engagement of the relationships and ongoing monitoring."

Office of the Comptroller of the Currency –

OCC Bulletin 2001-47 *(Issued 2001)*
"A bank's use of third parties to achieve its strategic goals does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws. Many third-party relationships should be subject to the same risk management, security, privacy, and other consumer protection policies that would be expected if a national bank were conducting the activities directly."

OCC Bulletin 2013-29 *(Issued 2013)*
"The Office of the Comptroller of the Currency (OCC) expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party. A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws."

OCC Bulletin 2017-21 *(Issued 2017)*
"Bank management should conduct in-depth due diligence and ongoing monitoring of each of the bank's third-party service providers that support critical activities. The OCC realizes that although banks may want in-depth information, they may not receive all the information they seek on each critical third-party service provider, particularly from new companies. When a bank does not receive all the information it

seeks about third-party service providers that support the bank's critical activities, the OCC expects the bank's board of directors and management to

- develop appropriate alternative ways to analyze these critical third-party service providers.
- establish risk-mitigating controls."

Federal Deposit Insurance Corporation –

Guidance for Managing Third-Party Risk / FIL-22-2008 *(Issued 2008)*
"Financial institutions often rely upon third parties to perform a wide variety of services and other activities. An institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution."

New York Department of Financial Services –

23 NYCRR 500 *(Issued 2018)*
"Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:

(1) the identification and risk assessment of Third Party Service Providers;
(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;
(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and
(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices."

INSURANCE SECTOR

National Association of Insurance Commissioners –

Insurance Data Security Model *(Issued 2017)*
"(1) A Licensee shall exercise due diligence in selecting its Third-Party Service Provider; and
(2) A Licensee shall require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider. "

HEALTHCARE SECTOR

United States Department of Health and Human Services –

HIPAA Security Rule - 45 C.F.R. 164.308 *(Issued 2002)*
(b)(1) Standard: Business associate contracts and other arrangements. "A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory

assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information."

NOTE: Healthcare entities are managing fourth party risk by requiring business associates to comply with the HIPAA Privacy and Security rules.

HIPAA Omnibus rule *(Issued 2013)*
Make business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements.

These provisions include extending the applicability of certain of the Privacy and Security Rules' requirements to the business associates of covered entities; requiring that Health Information Exchange Organizations and similar organizations, as well as personal health record vendors that provide services to covered entities, shall be treated as business associates; requiring HIPAA covered entities and business associates to provide for notification of breaches of ''unsecured protected health information'';

"…it is the business associate that must obtain the required satisfactory assurances from the subcontractor to protect the security of electronic protected health information…"

HITECH Act Section 13401(d) *(Issued 2009)*
The HITECH Act extended the HIPAA Privacy and Security rules and related liability beyond covered entities to also include business associates – the vendors to covered entities.

"These provisions include extending the applicability of certain of the Privacy and Security Rules' requirements to the business associates of covered entities…"

CROSS- SECTOR

The European Union –

General Data Protection Regulation *(Issued 2016)*
Section 81 "To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing."

Section 83 "In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected."

Add: Risk Recon contact information, © notice, other branding marks