AWS Prescriptive Guidance

Value creation during M&A and divestitures: cybersecurity and compliance

AWS Prescriptive Guidance: Value creation during M&A and divestitures: cybersecurity and compliance

Table of Contents

Home 1
Overview 2
    Background 2
    Best practices 2
    Transforming due diligence to value 2
What customers want and what regulators require 3
How AWS can help 4
    Strategy and target identification phase 4
    Due diligence and deal fulfillment phase 5
    Integration phase 5
    Post-transaction value creation phase 5
FAQ 7
    How long is the engagement with AWS? 7
    Does AWS provide an audit service to the board of directors? 7
Next steps 8
Resources 9
Document history 10

Value creation during M&A and divestitures: cybersecurity and compliance

Sali Osman, Principal Security Advisor, AWS Professional Services

November 2020

Whenever there is a global event, the market witnesses a shift in the industry. This results in an increase in relevant industry acquisitions and other impacted divestitures. As the number of mergers and acquisitions (M&A) and divestitures increases in highly regulated industries such as technology, pharmaceutical, health, and life sciences, more attention is given to security, risk, and compliance. This strategy outlines how Amazon Web Services (AWS) products and advisory practices can provide value to AWS customers through these critical transitions.

Targeted business outcomes:

- For business executives, raise awareness of cybersecurity and compliance considerations during M&A and divestiture transitions
- Provide guidance to customers who may potentially struggle to assess security, risk, and compliance during these transitions
- Leverage AWS services and advisory offerings to mitigate risk throughout transactions

Overview

Background

In 2011, the U.S. Securities and Exchange Commission (SEC) published guidance regarding disclosure obligations relating to cybersecurity risks and cyber incidents, in addition to anti-fraud and fair deal requirements. For the past decade, regulators have been blocking acquisitions or divestitures that are a compliance liability. The global market has witnessed mergers that inherited unknown security risks and non-regulatory compliance from the acquired company. With the unforeseen global changes during 2020, experts expect a higher number of divestitures.

Corporate executives are aware of the personal accountability and the board of directors' fiduciary responsibility for cybersecurity and regulatory risks, and the monitoring and mitigating activities needed. The SEC and courts can sanction mergers and acquisitions (M&A) deals even if penalties to settle securities fraud charges weren't paid on time, and privacy class action or securities lawsuits brought by shareholders weren't settled. To validate the importance of cybersecurity in business valuation, Donnelly Financial Solutions performed a survey in 2017 and found the following:

- 40 percent of investors walked away from a deal because of cybersecurity issues.
- 80 percent of respondents say that they have uncovered data security breaches in 26-75 percent of M&A targets.
- 60 percent are concerned about the potential intellectual property theft of the company that is being acquired.

Best practices

Companies that manage their overall risks support compliance throughout their business operations and functions. It is easier to divest a business or acquire a new one when there is a high level of maturity in control implementations—policies are established, procedures are implemented, teams are trained, and tools that ensure automation, monitoring, and reporting are used. To manage your cybersecurity and regulatory risks, follow these best practices:

- Operate with a regulatory framework and risk model in mind throughout the acquisitions or divestiture lifecycle; design a playbook to use.
- Align with SEC and regulatory guidance and industry best practices. This is critical when the divested or acquired business has special requirements.
- Leverage the cross-functional teams in AWS that have industry specialty and transactional experience.

Transforming due diligence to value

The purpose of the AWS cross-functional M&A Value Realization Office is to help customers transform the M&A and divestiture process from a due diligence process to an efficient value realization by leveraging AWS subject matter expertise throughout the M&A lifecycle. The advantage that AWS has is in the visibility it provides to customers and the metadata it maintains of customers' technical inventory.

What customers want and what regulators require

As a control objective for the industry, the U.S. Securities and Exchange Commission (SEC) looks at the fairness of the deal, for the purchaser and for the target company, to ensure that there is no forced deal, fraud, or escaping regulatory liability.

Accordingly, the SEC guidance stated that corporations should consider disclosing material information about cyber risks, not only in general terms, but also on an incident-by-incident basis. The SEC suggested that a corporation, in determining the contours of its disclosure, should weigh the following factors:

- Frequency and severity of prior cyber incidents
- Probability of cyber incidents occurring; potential costs and consequences (for example, assets or sensitive information misappropriation, corruption of data, or disruption of operations)
- Adequacy of preventative actions taken
- Risk level of threatened attacks

The SEC further suggested that companies, within their corporate filings, might want to disclose the following, based on their circumstances and materiality:

- Aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences
- Descriptions of any outsourced functions that might have material cybersecurity risks and how the registrant addresses those risks
- Descriptions of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a cost of incident and response, including investigation, penalties, and settlements
- Risks related to cyber incidents that might remain undetected for an extended period
- Description of cyber risk insurance policy coverage or any relevant risk transfer agreements

The SEC enforces rules for SEC-registered broker dealers and investment advisers, who are held accountable for protecting customer data and ensuring accuracy of cybersecurity disclosures. Although there is no explicit SEC rule for companies that aren't following guidelines, the M&A and divestiture process will become very expensive and lengthy in these cases, especially if the seller company encountered a cyber incident and didn't disclose the risks, or experienced changes in their stock price. The National Association of Corporate Directors (NACD) recommends that management retain external subject matter and legal expertise for their incident response plans, and receive updates regularly. For more information, see Cyber-Risk Oversight: Director's Handbook Series (NACD, 2017).

How AWS can help

In May 2020, a leading financial services company in the US reached out to AWS Professional Services for help with a series of long-term acquisitions across the globe. They asked AWS to help assess the security posture of all its targeted acquisitions, develop a remediation plan for security leadership to discuss with the business to be acquired, and help with remediation activities of all findings that posed a risk to the merger. The customer wanted a long-term plan to support their multi-year M&A roadmap. The Chief Information Security Officer (CISO) was looking for specific remediation activities with costs and resource requirements spread across the timeline of the acquisition deal. These types of inquiries surfaced after courts ordered seller companies that were slow to disclose data breaches during 2013-2016 to pay hundreds of millions of dollars in settlement to victims, which resulted in reduced offers from buyer companies.

AWS has been successfully advising corporate directors in governing digital transformation and emerging technologies. The Marsh & McLennan practical guide prepared in January 2020 for the National Association of Corporate Directors (NACD) noted that Amazon has been recognized for meeting customers' needs on business intelligence and technical capabilities. The guide recommends, "Boards should assess whether their enterprises are able to build these types of digital platforms, or if they are ready to become a lead contributor to the new business ecosystems that these digital platforms are creating." AWS has expertise in empowering customers from various industries on digital platforms. AWS Professional Services can help customers strengthen their regulatory and risk posture operating at the three lines of defense (3LoD)—that is, control implementation, control management and oversight, and control assessment.

AWS can aggregate insights on technology risks, which are fundamental data points to advising a company's audit committee and risk committee. The following sections describe the challenges companies face throughout four M&A and divestitures phases, and where AWS can help:

- Strategy and target identification phase (p. 4)
- Due diligence and deal fulfillment phase (p. 5)
- Integration phase (p. 5)
- Post-transaction value creation phase (p. 5)

Strategy and target identification phase

During the formulation of the thesis (the argument of the buyer's opportunity—including gross profit, top line revenue, asset value, and strong customer basis—should they choose to complete the deal) and target identification, potential buyers have less visibility into the security and compliance posture of the target company. This reduced visibility is attributed to various reasons, such as concerns about intellectual property and inadvertent disclosures of regulatory privileged and confidential information.

Asset management has been a known challenge for companies that are geographically dispersed and that have many third-party connections. This makes the technology asset identification process harder, especially when determining interrelationships among systems that might be affected by the divestiture. AWS Systems Manager Inventory provides visibility into a customer's Amazon Elastic Compute Cloud (Amazon EC2) and on-premises computing environment on the seller's side. AWS account structure and AWS Organizational Units (OUs) are fundamental during this process, because OUs can be created to park accounts and resources for businesses that are scoped to be sold. In addition, AWS provides assistance in the following ways:

- The decoupling nature of AWS technology makes it easier for executives to select the businesses targeted for the divestiture.

- In an effort to make diligence easier for the buyer, AWS can incorporate clear value of the technology advancement and quantify the technology risk in the value realization.
- AWS Professional Services can perform AWS security assessments to enable strategic envisioning, regulatory risk predictions, business value and threat analysis, risk reduction, acceleration of results, and avoidance of obstacles with security and compliance.
- For customers who are aspiring for regulatory attestations, such as Payment Credit Card Industry (PCI) or Health Information Trust Alliance Common Security Framework (HITRUST CSF), AWS Security Assurance Services, LLC (AWS SAS) is a fully owned subsidiary of Amazon Web Services that helps AWS customers with regulatory readiness.

Due diligence and deal fulfillment phase

Industry best practices advise the buyer to complete the following steps:

- Perform an overall evaluation of the security governance and operating model.
- Evaluate investments on the security program and automation (or lack of automation).
- Evaluate the effectiveness of the risk management programs and board-level oversight on risks that affect business goals and regulatory posture.
- Review previous security incidents and non-compliance citations on regulatory frameworks pertaining to privacy.

The security, risk, and compliance advisory services offered by AWS Professional Services can help customers scope regulatory frameworks that are applicable to the industry, geographic region, and product or service. They can also perform an overall evaluation of the risk and operational readiness. This evaluation includes an in-depth architecture review and risk assessments, as well as help with remediation plans. Customers can choose to deploy AWS services such as Amazon Inspector as an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

Integration phase

Merging companies incur assimilation challenges, which affect the technology governance and operating models.

Technology governance is the foundation of security management. Consistent procedural controls by employees complement the technical controls that are embedded within corporate systems. AWS Professional Services offers governance at scale to help customers establish a governance structure and create an operating model that mitigates identified risks with the customer's office of change management.

For customers who don't have an office of change management, AWS can help set one up. As part of remediation plans, customers benefit from AWS expertise to implement controls based on their regulatory landscape, address security weaknesses, and enable technical teams to scale with security automation and tools to maintain continuous monitoring.

Post-transaction value creation phase

In this phase, companies need to be able to scale and grow their business while continuously managing their risks and new regulatory posture. AWS helps customers automate and scale their technical capabilities to meet their strategic goals, and helps ensure that the company's technology posture aligns

with their business strategy. AWS Security Hub aggregates, organizes, and prioritizes security alerts or findings from multiple AWS services and AWS Partner solutions. In addition, AWS Config enables customers to assess, audit, and evaluate their configurations of AWS resources in a continuous manner.

FAQ

How long is the engagement with AWS?

It varies from customer to customer, depending on where you are in your cloud journey and the M&A phase you're in when the engagement begins.

Does AWS provide an audit service to the board of directors?

This is not an audit service. It is an advisory engagement in which AWS customers can benefit from the AWS offerings that align with the risk and audit governance model through the three lines of defense: technology implementations, control assessors, and audit functions.

Next steps

Given increasing expectations from shareholders and regulators on the board of directors to govern digital transformation strategies and risks during divestitures and M&A, customers can benefit greatly from AWS technical capabilities and operating models. AWS can help customers materialize the technology assets and technology risks throughout the lifecycle of the M&A deal. AWS advises customers to start early and plan accordingly. Whether you're on the buyer side or the seller side, due diligence is required. AWS can help with M&A and divestiture transactions.

Review the guides and articles in the Resources (p. 9) section for AWS best practices pertaining to specific regulatory frameworks and industries.

Resources

References

- AWS Professional Services
- How CFOs can help accelerate divestitures (Tze-Liang Chiam, EY website, June 2020)
- M&A at a glance (Paul, Weiss website, June 2020)
- CF Disclosure Guidance: Topic No. 2 (U.S. Securities and Exchange Commission website, October 13, 2011)
- Cyber-Risk Oversight (NACD, 2017)
- Guide to Broker-Dealer Registration (U.S. Securities and Exchange Commission website, April 2008)
- FCPA Resource Guide (U.S. Department of Justice, July 2020)

AWS guides and Quick Starts

- European Union General Data Protection Regulation Control Mapping Worksheet
- Reference Architecture for HIPAA on AWS
- Standardized Architecture for PCI DSS Compliance on AWS
- Standardized Architecture for NIST on AWS

Document history

The following table describes significant changes to this document. If you want to be notified about future updates, you can subscribe to an RSS feed.

update-history-change	update-history-description	update-history-date
Initial publication (p. 10)	—	November 4, 2020