Compliance Checklist: Third-Party Risk for ISO 27001, GDPR, CCPA, & NIST
## Agenda

<table>
<thead>
<tr>
<th>01</th>
<th>Third-party Risk Management Drivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>02</td>
<td>Uptick in Regulations &amp; Standards</td>
</tr>
<tr>
<td>03</td>
<td>Major Regulatory Considerations for Today</td>
</tr>
</tbody>
</table>
What’s Driving the Need for Vendor Risk Management

- New Technology
- More Breaches
- Greater Consequences
Through 2022, growth in enterprise IT spending for cloud-based offerings will be faster than growth in traditional (non-cloud) IT offerings, making cloud computing one of the most disruptive forces in IT markets since the early days of the digital age.

- Gartner
Target to Pay $18.5M for 2013 Data Breach that Affected 41 Million Consumers

Last week, Target told reporters at The Wall Street Journal and Reuters that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor.

- KrebsOnSecurity
Consumers Now Expect Data Security & Privacy

67% of people support major online privacy & security legislation in the U.S.

- HarrisX
Uptick in Regulations & Standards
Background

2013
- ISO 27001
- OCC 2013-29

2017
- NYDFS

2018
- GDPR

2019
- CCPA
- ISO 27701

2020
- NIST rev5
- Brazil LGPD
These Regulations Are Only the Tip of the Iceberg

Third-Party Vendor Laws Span Hundreds of Countries and Jurisdictions
# Hundreds of Standards & Frameworks Used Across Stakeholders

<table>
<thead>
<tr>
<th>Standards, Frameworks, and Global Laws</th>
<th>Critical Business Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>FedRAMP, HIPAA, IS0 27001, CSA, SFG, SHARED ASSESSMENTS, AICPA SOC 2019, PCI DSS, NIST, CobiT 2019</td>
<td>TPRM, InfoSec, Privacy, Procurement, IT, Legal</td>
</tr>
</tbody>
</table>

**Critical Business Units:**
- TPRM
- InfoSec
- Privacy
- Procurement
- IT
- Legal
What We Will Focus On Today

- **2013**: ISO 27001, OCC 2013-29
- **2017**: NYDFS
- **2018**: GDPR
- **2019**: CCPA
- **2020**: ISO 27701, Brazil LGPD
ISO 27001

- ISO 27001
- OCC 2013-29
- 2013

- NYDFS
- GDPR
- 2017

- CCPA
- ISO 27701
- 2018

- NIST rev5
- Brazil LGPD
- 2019

- 2020

- 2018
- 2019
ISO 27001 Major Consideration: Mitigating Supplier Risks

Does your organization have information security requirements in place for mitigating the risks associated with the supplier’s access to the organization’s assets that are agreed upon with the supplier and documented?
Add Risk Treatment Consistency Across Teams & Individuals

CONTROL IDENTIFICATION
Assess controls (or the lack thereof) on all your vendors to generate risks

RISK RATINGS
Standardize to equally apply risks throughout your organization

TREATMENT PLANS
Collaborate with risk owners and track risk mitigation activities in a single view

RISK EXCEPTIONS
Manage exceptions and leverage compensation controls when necessary
Standardize on Risk

Same Risk Scoring Methodology

Define Probability and Impact for Your Organization

Use Standardized Risk to Prioritize Your Third Parties
Organize Processes Across Stakeholders

CREATE WORKFLOWS
Leverage automation technology or create a documented assessment workflow process

DYNAMIC ASSESSMENTS
Use inherent risk scoring to determine the depth of your vendor assessment

MANAGED SERVICES
Outsource vendor chasing if necessary with managed services
Risk Lifecycle

- Risk Identified
- Risk Assigned
- Remediation Proposed
- Exception Requested
- Risk Reduced
- Risk Retained
Benefit of Automation When Undergoing an Audit

During Audits, Manual Processes Are Scrutinized
Europe’s General Data Protection Regulation

- ISO 27001
- OCC 2013-29
- NYDFS
- GDPR
- CCPA
- ISO 27701
- Brazil LGPD
- NIST rev5
GDPR Major Consideration: Cross-Border Data Transfers

Does your organization maintain records on the recipients or categories of recipient to whom it has or will disclose personal data, in particular, the recipients in third countries or international organizations?

Art. 30 Data Mapping Obligations
How Is Data Actually Used?

1. Purpose
2. Individuals Involved
3. Data Transfers

EXAMPLES

- Marketing Emails
- Sales Cold Calls & Emails
- Employee Onboarding
Operations Must Change

How Do You Track Business Processes?

- Assessments
- Interviews
- Self-Service
- Ask Privacy Team for Art. 30 Records
Business Context of Third Party Vendor

- **Vendor**
- **Asset or App, Service or Product**
- **Engagement**
- **Business Process**

Database
Analyze Biometric Data
California’s Consumer Privacy Act

- ISO 27001
- OCC 2013-29
- NYDFS
- GDPR
- CCPA
- ISO 27701
- Brazil LGPD
- NIST rev5

Timeline:
- 2013: ISO 27001, OCC 2013-29
- 2017: NYDFS
- 2018: GDPR
- 2019: CCPA
- 2020: ISO 27701, Brazil LGPD
CCPA Major Consideration: Selling Personal Data

Do you know which third parties you sell personal data to?

Sale = Monetary or Other Valuable Consideration
After a consumer has opted out of the sale of their data, are you able to work with your third parties to ensure they stop using the consumer’s data?

If requested, are you able to cease *all* selling of consumers’ personal data to third parties?

Do you have processes in place to direct service providers to delete the consumer’s personal information from their records?
CCPA: Service Provider vs. Third Party

All Service Providers are Third Parties, But Not All Third Parties are Service Providers

Service providers must not further collect, sell or use the personal information except as necessary to perform the business purpose

Service providers are not obligated to stop processing data when the opt out of sale is executed

Why Does This Matter?

Service Providers Are Exempt from Opt-Out of Sale Cooperation
Identifying and Organizing Vendors at Scale

**SELF-SERVICE PORTAL**
Enable business owners to add vendors themselves & leverage threshold assessments

**SYSTEM INTEGRATIONS**
Integrate with procurement, ITSM & other systems to add vendors to your inventory

**BULK IMPORT**
Use existing information and bulk import it into a centralized vendor risk platform
System Integrations
NIST 800-53 rev5 Major Consideration: All-Source Intelligence

Does your organization use all-source intelligence to assist in the analysis of supply chain risk?

Supplier Risk Management
Spend Less Time Researching Vendors

AGGREGATED RESEARCH
Avoid starting from scratch and leverage databases of third-party research

SECURITY & PRIVACY CERTS.
Use a tool or manually check for cert. by going directly to the cert. website

VENDOR QUALIFICATION
Leverage third-party research information to sift through non-viable vendors
Aggregated Research

PRE-COMPLETED ASSESSMENTS

Industry Standards (NIST, SIG, CSA, and more)

Tiered Assessment Levels

PRE-POPULATED PRIVACY & SECURITY PROFILES

Privacy & Security Certifications

Privacy & Trust Details
Security & Privacy Certification Granularity

Vendor: Salesforce

- ISO 27017
- ISO 27018
- ISO 27019

Mulesoft Lacks the Following Certs:

- ISO 27017
- ISO 27018
- ISO 27019
Trusted by 4,500 Organizations, Both Big and Small

OneTrust Vendorpedia™
THIRD-PARTY RISK SOFTWARE

GLOBAL REGULATORY INTELLIGENCE
DataGuidance Alerts You to Breaches, Enforcements, and Changes to Vendor Risks

REAL-TIME EXCHANGE RESEARCH
Pre-Populated Cyber Risk & Performance Data with Product-Level Granularity

FREE VENDOR CHASING SERVICES
Offload Your Vendor Risk Assessment Chasing, at No Additional Cost

INDUSTRY’S SIMPLEST INTEGRATIONS
Built-in Plugins for Tools Like Coupa, Archer, ServiceNow, BitSight, & More
OneTrust Vendorpedia™
THIRD-PARTY RISK SOFTWARE

Visit booth #20 and learn more at vendorpedia.com

Start a free trial or request a demo today!