
Pratum
Vendor Requirements From a Cybersecurity Perspective and Third Party Risk Management

Pratum

Ben is a Certified Information Systems Auditor (CISA) with 12 years of Information Security and Information Technology experience. As an information security consultant for Pratum, he works with clients to support their risk management and compliance efforts. Prior to joining Pratum, he held positions as Risk Manager, Lead IT Security and GRC Analyst, IT Operations Supervisor, and Systems Administrator.

Ben has expertise in Third-Party Risk Management, Change Management, Access Control, Security Operations, Business Continuity, and Disaster Recovery (BC/DR), Security and Risk Management, and Security Awareness. Additionally, he has IT Compliance experience across a multitude of Regulatory Frameworks. Ben has also spent some time on the IT Operational side, which has provided him a holistic view of how security impacts IT operations.

Ben also serves on the Information Systems Security Association board (ISSA) as the VP since July of 2019 and is also active in the local ISACA and InfraGard chapters.

Agenda

- Regulatory Requirements
- Vendor and Third-Party Management
- Classifying Vendors
- Information Security and Cybersecurity Baselines
- Risk Evaluation and Mitigation
- Next Steps

Pratum

Organizations relying on outside vendors to provide and perform services opens up the organization to new risk potential. In this presentation, we will go over the steps necessary to properly evaluate the information security controls for a vendor and develop a plan to mitigate possible risks. We will also discuss how to continue to evaluate vendors on an ongoing basis.

Vendor management and third-party risk management are necessary as the increasing compliance obligations that are imposed on organizations through most regulators that mandate risk management policies extend to vendors as they have the potential to insert risk into the environment are typically outside of an organizations direct control. As such organizations have an obligation to understand the risks represented by vendors and need to actively take the appropriate steps to mitigate or limit how those risks impact their business.

GDPR – for those with a global presence, The GDPR clearly states that all businesses and their partners are responsible for protecting user data. Third parties are legally obligated to comply with all aspects of the regulation to ensure consistency and true protection for consumers.

NY DFS – Covered entities are required to not only implement written policies and procedures that are designed to ensure the security of Information Systems and Nonpublic Information that are accessible or managed by third party service providers but that they are also evaluating those third parties at a regular cadence dependent on the assessed risk level.

SOC 2 – The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities a
rising from business partners, customers, and others with access to the entity's information systems. Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties

ISO 27001 – Requires that in order to ensure protection of the organization’s assets that are accessible by suppliers, information security requirements for mitigating the risks associated with supplier’s access to the those assets should be evaluated regularly and documented.

OCC – States that organizations should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.

PCI – DSS – Has certain restrictions regarding the use of third parties for outsourced services and an annual assessment is required and the third party must provide evidence to their customers that demonstrate their compliance.

FFIEC – As part of a financial institution's third-party management program, management should ensure that third-party providers effectively provide support by negotiating clear and comprehensive contracts with appropriate terms that meet the institution's requirements; ensuring that the financial statements are audited at least annually; review results of independent audits of IT controls; and monitor the responsiveness of third-party provider's customer service.

Key Definitions

Vendor – Any third-party, service provider, supplier or contractor that supplies products, goods or services to an organization.

Vendor Management – Set of policies, processes and procedures used to strategically source and manage vendors so that investments are maximized and business risk is minimized.

Third-Party Risk Management – The process of identifying, assessing and controlling risks presented throughout the lifecycle of an organizations relationships with third-parties.

Pratum

Vendor management is a strategic process that's dedicated to the sourcing and management of vendor relationships so that value to the organization is maximized while risk is minimized. This process requires dedicated effort from the organization and the vendor. The approach and level of effort will differ and is dependent on the vendor relationship as well as the scope of services. Each vendor relationship may require a different process and documentation for review. Organizations should focus their vendor management efforts on third-party relationships that:

- Play a vital role in the organization's daily operations – are deemed critical or high to the organization and have a critical impact on the success of the organization's strategic projects
- Require long-term contracts
- Have potential for significant financial implications
- Are difficult to change overnight
- Require frequent interaction and collaboration for disputes or have complex problem-resolution mechanisms
- Access or manage substantial critical or sensitive data

Vendor and Third-Party Risk Management

- Planning
- Due Diligence and Selection
- Contract Negotiation
- Ongoing Monitoring
- Termination of Services

Pratum

Planning – Organization has defined that there is a need for the use of a vendors services as those needs cannot be met in-house.

Due Diligence and third-party selection – Determine the security controls that are required of the vendor. Typically, these should be at least equal to the security controls and processes that exist at your organization and required from your regulators or certifying authorities. The review ensures that the organizations understands and is in control of the risks introduced through the use of the vendor.

Contract negotiation – Ensure that legal and compliance are consulted within the process to ensure the appropriate language exists within the contracts. Contracts should clearly define the expectations and responsibilities of the vendor.

Ongoing Monitoring – Performing ongoing monitoring of the vendor relationship once the contract is in place is important to the organization's ability to manage the risk of the vendor relationship.

Termination or Renewal of services – Developing a contingency plan to ensure that the organization can transition the activities to another third party, bring the activities

in-house, or discontinue the activities when a contract expires, the terms of the contract have been satisfied, in response to contract default, or in response to changes to the organizations or third party's business strategy. Once the contract has ended or is not being renewed, ensure that the vendor is destroying any data that they aren’t legally required to hold. Terminate any accesses, or other permissions that were established throughout the relationship.

Vendor and Third-Party Risk Management

- Identification and Categorization
- Assessment and Analysis
- Risk Identification
- Risk Mitigation and Monitoring
- Vendor Performance Monitoring

Pratum

Identification and Categorization – Identify, categorize the vendor based on criticality to the organization. Each vendor should be assigned a business owner of vendor/application.

Assessment and Analysis – Gather information from the vendor to be reviewed and assessed such as audit reports, policies and other information supplied by vendor, as part of the due diligence process, and identify any gaps, risks and shortcomings which have an adverse effect on your organization.

Risk Identification – Identified risks, gaps and shortcoming are fed back to the business for discussion with the owner of the vendor/application, and any areas which need to be addressed as part of the due diligence are fed back to the vendor for a potential corrective action plan to be created.

Risk Mitigation and Monitoring – The business owner, in conjunction with the risk management and compliance team, should monitor the vendor to ensure any corrective action plan(s) are acted upon, and chase closure with the vendor/application owner.

Vendor Performance Monitoring – The organization should have regular follow up reviews and assessments of the vendor based on criticality and continued suitability to the organization. These will range from annual audits to desk top reviews over a 1,2 or 3-year period (dependent on the criticality). Continuous assessment of the vendor through questionnaires, report gathering, etc. is crucial to the organizations ability to manage risks introduced through the use of the vendor.

Classifying Vendors

- Criticality
- Dependence
- Financial Commitment
- Performance
- Regulatory Impact
- Business Impact

Pratum

Factors to consider when classifying vendors include:
Criticality: Impact to operations if the vendor's service or product was suddenly not available and/or service or product subjected the organization to excessive liability.

Dependence: Degree of difficulty involved in finding and implementing a service or product replacement.

Financial Commitment: Higher financial commitment may equate to a greater loss of investment.

Performance: Vendors with substandard or unproven performance require a higher degree of monitoring by the service owner and IT Compliance.

Regulatory Impact: Vendor's ability to impact the company level of regulatory compliance.

Business Impact: Vendor's ability to impact business reputation or strategy.

High Rating

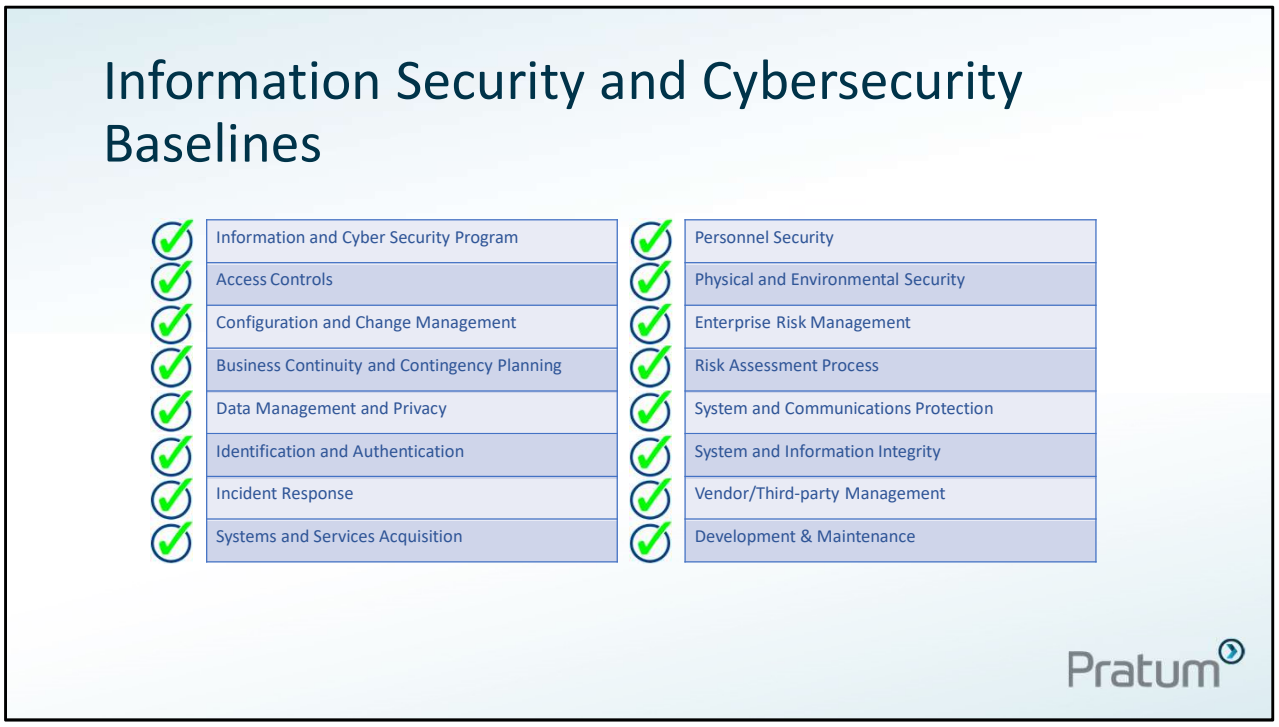
- Processes, stores, hosts, or transmits restricted/confidential Data on behalf of the organization.
- Has direct network access into organizational infrastructure.
- Deemed mission critical and loss of third party will result in severe adverse impact.

Moderate Rating

- Has access to restricted/confidential data but does not process, store, hosts or transmit that data
- Loss of third party will be tolerable, with moderate difficulty of replacement.

Low Rating

- Used of third party will have low impact, replacement readily available.



Now that we have the vendor(s) identified and classified, the next few steps in the process are related to what to assess and evaluate and who are the stakeholders? Legal, Risk Management, Compliance, IT, HR, business heads, etc. should all play a role within the assessment process. Develop a criteria checklist that needs to be in place and the level of expectations you are relying on the vendor to have in place. Anything less than that should be flagged as a risk or a gap that needs to be monitored and controlled.

Key areas to highlight – data access and data flow. What access will the vendor have and what controls are in place?

Risk Evaluation and Mitigation

- Risk Management Process
- Risk Evaluation
- Mitigation Techniques
  - Mitigate with compensating control(s)
  - Transfer the risk
  - Avoidance
  - Accept

Follow your existing Risk Management Process for identified risks and gaps uncovered through your vendor assessment.

Treat the risks in the same manner that they would be treated if discovered within your own organization. Ex. If the vendor provides a web application that is open to the internet, that proposes a potential risk to your organization based on the data entered within the web application, therefore in addition to username and password, you may want to employ your SSO option or MFA if possible as an additional access control. You may also choose to monitor the endpoints within your SIEM solution.

Mitigation Techniques – Be sure to document the risk and the potential remediation. Any risk exceptions should be reviewed annually to determine if the risk still exists or if additional controls need to be added to ensure the risk is within the risk appetite of your organization.

Next Steps

- Create a Vendor Management Policy
- Determine and Classify Vendors
- Build a checklist of the criteria for review
- Reach out to vendors and collect information
- Assess the Risk
- Continuous Monitoring

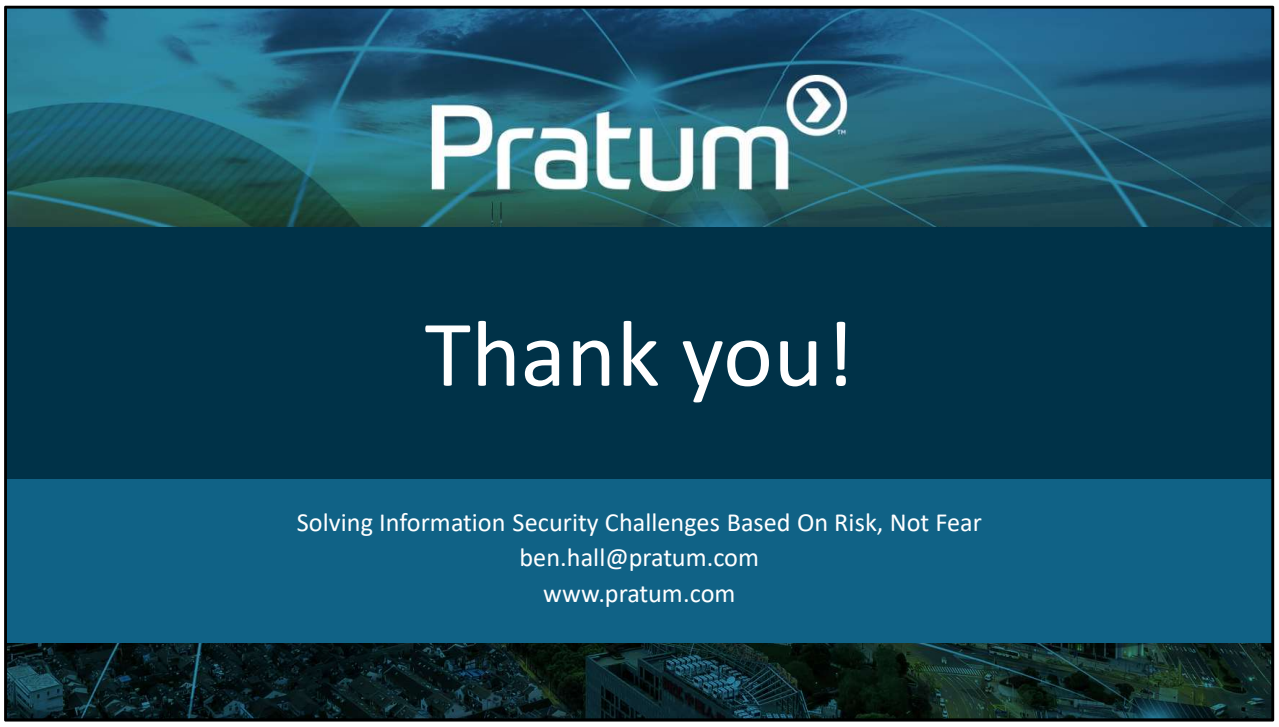
Pratum

Set a Security Policy
Communicate policies with staff
Create written out guidelines that are aimed at educating and helping your staff
Utilize established guidelines from trusted security frameworks and organizations (NIST, CIS, SANS, etc.)

Additional Sources & Resources

- https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
- https://pratum.com/blog/345-where-to-begin-with-it-vendor-management
- https://pratum.com/blog/419-analyzing-and-assessing-the-security-of-third-party-vendors

Pratum


Pratum
Thank you!
Solving Information Security Challenges Based On Risk, Not Fear
ben.hall@pratum.com
www.pratum.com