Advisory Board | Health Care IT Advisor

Third-Party Security Risk Management Checklist

A planning guide to improve your third-party risk management program

Third-party risk management is not a one-time process; rather, it is a cycle of conversations, risk assessments, adjustments, and internal discussions. But a thorough program does not have to be difficult. Use this checklist to kick-start your program or assess your current approach to third-party risk management.

	Recommendations	Your organization's action items
Create an inventory of all third parties	An accurate inventory of all third parties is a time-consuming, yet essential, first step. If you don't already have such a list, use our Excel-based sample inventory to get started. Edit it to fit your specific needs and preferences.	
Set minimum standards for third parties based on level of intimacy	Know your minimum security standard and stick to it. Offer some secure interim solutions like VDI[1] or remote access until your minimum standards are met. Critical partners require stricter terms.	
Establish standard contract requirements based on own internal policies and standards	Outline expectations for certain situations, such as penalties for noncompliance, timelines for adherence, etc. Consult your internal policies as well as external standards such as NIST, [2] HITRUST, [3] ISO[4] 31000, etc.	
Schedule regular reviews and check-ins with third parties to reassess risk	Establish a cadence for check-ins, risk assessments, and remediation. Track results in a central location to ensure continuity and continued progress. Use major system changes and updates as triggers for risk reassessments. The regularity of risk assessments should depend on the ultimate categorization of risk (as determined in another action in this checklist).	

1) Virtual desktop infrastructure.
2) National Institute of Standards and Technology.
3) Health Information Trust Alliance.
4) International Organization for Standards.

Third-party security risk checklist cont.

Planning guide to improve your third-party risk management program

	Recommendations	Your organization's action items
 **Establish the assessment method to be used for check-ins**	The method for assessment needs to be clarified ahead of time. Methods can include questionnaires and checklists, on-site surveys, penetration tests, audits, and/or flowcharts of activity that lead up to all touchpoints. The method used depends on the depth of the relationship.	
 **Establish security liaison or contact with each third party**	Determine who on your internal team is responsible for scheduling and conducting check-ins and assessments. Have a backup identified and trained. Document the third party's main business representative and their security liaison, as they likely are not the same individual.	
 **Determine a business relationship owner for each third party**	Each third party should have an internal business relationship owner at your organization. Document their name and contact information. Establish clear understanding of the role third-party risk management plays for the organization and when and how the IT/security/risk contact should be engaged.	
 **Work with the business relationship owner to establish contingency plans to replace the third party, if necessary**	The contingency plan should include alternatives in case of an emergency, as well as a plan for full replacement should it become necessary. A full replacement may be necessary for several reasons including the cessation of business, refusal to conform to standards, perceived risk that is too high for your organization to carry.	

Third-party security risk checklist cont.

Planning guide to improve your third-party risk management program

	Recommendations	Your organization's action items
Set a schedule to review the risks with relationship owner	Internal communication and collaboration is critical. Document conversations in a central location and update the business relationship owner of any "red flags" and their implications. Work with business relationship owner to address any issues together before the situation escalates.	
Document data flows with third parties	This is another time-consuming, yet critical component to third-party risk management. Changes in data flow must be updated and documented. Incorporate data flow mapping updates into your regular check-ins with the third party.	
Document all touchpoints with third parties	As previous activities mention, document every conversation with third parties in a central location. Note who will reach out for the next check-in and when your organization plans to reach out next. Create a reliable trigger so touchpoints aren't missed (e.g., an email reminder or task). Prioritize these conversations. Don't let them fall victim to competing priorities.	
Assess and categorize the risk associated with each third party	Key considerations include how much access the vendor has to your data and systems, the sensitivity of the data and criticality of the systems the vendor has access to, how critical the vendor's work is to your daily operations, business risk factors (e.g., financial, audit reports), and known shortfalls compared to your set standards. Set how often each category will be subject to risk reassessment.	

Third-party security risk checklist cont.

Planning guide to improve your third-party risk management program

	Recommendations	Your organization's action items
Plan for and perform technical reviews	Discuss and document technology measures taken by the third party to secure their digital environment.	
Scan any externally provided hardware, devices, or software for vulnerabilities	You may catch vulnerabilities that the vendor has not. Share the results with the vendor so they can make corrections for other clients.	
Regularly audit network access for third-party users	Reach out to ensure that specific users and their level of network access is still necessary for each vendor. Provide a deadline for a response and be prepared to prohibit system access as appropriate. .	
Evaluate formal outbound data transfers	A data governance council or privacy officer is a good way to ensure instances of sharing data are truly necessary. Make sure the team/individual has the authority to deny sharing data.	

Third-party security risk checklist cont.

Other considerations

The following are additional considerations that should be settled with a third party prior to doing business. These considerations do not necessarily need to be included within a contractual agreement, but they should be fully documented on both sides with at least a memorandum of understanding (MOU).

Operational considerations

- Who will agree to indemnify whom?
- Expectations of risk assessments, audits, and sharing of results
- Clarification of certain policies:
  - Minimum required protections
  - Identity and access management
  - Password policies
- When data is exchanged, what are the lifecycle terms?
  - Limitations on use
  - Disposal requirements
- Notification responsibility when a legitimate user's role changes and access should be revoked
- SLAs[1] around provisioning and de-provisioning

In the event of a **breach**

- Who has the right of notification (to compromised parties, regulatory authorities, and the media)?
- Who has the responsibility for notification (to compromised parties, regulatory authorities, etc.)?
- Who has approval authority over notifications?
- Who covers the cost of notification and remediation?
- Who will notify the media?
- Whose insurance covers what?
- Who pays for remediation efforts for impacted individuals (e.g., identity theft monitoring)?
- Who conducts forensics?
- Who has the right to review results of forensics?

Additional Advisory Board resources

Slide deck and webconference

Security and the C-Suite: Leadership's role in building cyber-resilient organizations

Cheat sheets

Cybersecurity Cheat Sheets for the C-Suite and Board: What executive leaders need to know about cybersecurity

1) Service-level agreements.