Building a Successful Vendor Risk Assessment (VRA) Program by Leveraging The HITRUST CSF & Associated Assurance Program

Ashish Vashishtha
Director – Enterprise Information Security
UnitedHealth Group

Agenda

- Welcome & Introductions
- Vendor Risk and its Impact on an Organization
- Obtaining Leadership Support
- Identifying and Partnering with Key Stakeholders
- Developing a Closed Loop Vendor Risk Assessment (VRA) Program
- Developing an Organization's Vendor Risk Assessment Toolkit by Aligning with and Leveraging the HITRUST CSF
- Assessment Considerations
- Risk Identification, Monitoring and Reporting
- Model and Align Proprietary Methodologies with the HITRUST CSF
- Q&A and Wrap-up

Vendor Risk and Its Impact on an Organization

- Healthcare industry relies upon a tremendous number of 3rd party vendors to support various services
- Vendors represent potential risk to the customer if they host customer's data, have access to customer's data, or connect to customer's network
- Vendors may not be able to protect customer's data due to ineffective / insufficient security and privacy controls which may lead to loss of data resulting in name appearing on DHS OCR "Wall of Shame" portal
- This makes it extremely important for an organization to assess it's vendors to understand if security and privacy controls are in place and operating effectively

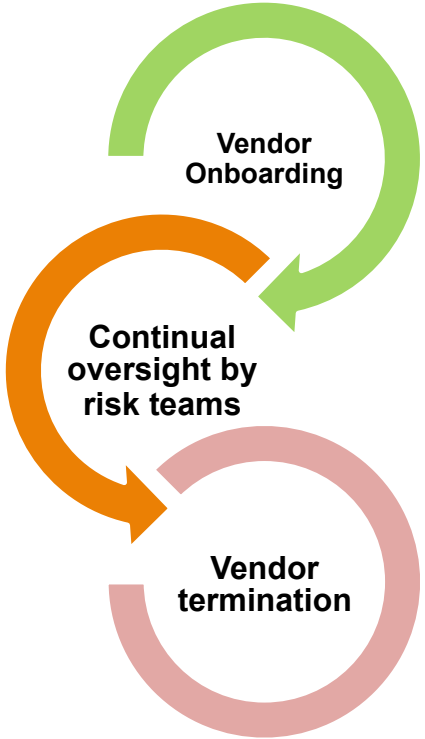
Obtaining Leadership Support

- Buy-in from board/executive team to align security initiatives with the organization's strategic goals
  - Top down approach to help drive requirements throughout organization
  - Communicate leadership support and requirements to internal stakeholders
- Vendor Risk Assessment policy defining core program requirements
  - Requirements for contractual agreements
  - When do we need to perform an assessment?
  - What should be the Methodology?
  - What level of due-diligence is required?
  - What are the roles and responsibilities of stakeholders?
- Contractual requirements
  - Contracts should consistently state what security requirements vendor must agree to
  - Embed requirement for Independent 3rd party accredited certification / report in the contract with vendor
  - Security and Privacy breach notification to customer requirements

Identifying and Partnering with Key Stakeholders

- Information Security
  - Responsibility & accountability for developing, documenting, maintaining, and communicating a comprehensive Risk Management Program
- Legal
  - Developing and maintaining contractual language
  - Consultation on applicable laws and regulations
- Privacy
  - Consultation and agreement to ensure privacy requirements are embedded into VRA Program
- Sourcing & Procurement
  - Facilitation in contract negotiation and Business Associate Agreement (BAA)
- Business
  - Who in the business can accept risk
  - What is the business escalation process
- Compliance
  - Developing and maintaining compliance requirements for vendors

Developing a Closed Loop Vendor Risk Assessment (VRA) Program



- ✓ Due-Diligence by various risk teams
- ✓ Sign required contracts/BAA with vendor
- ✓ Process to identify minimum necessary data that can be shared based on business risk

- ✓ Periodic risk assessment by various risk teams based on business risk

- ✓ Develop and follow consistent termination process
- ✓ Ensure all logical & physical access is de-provisioned
- ✓ Formal data destruction certification is obtained

HITRUST 2017
Learn. Collaborate. Deliver.

Developing an Organization's Vendor Risk Assessment Toolkit by Aligning with and Leveraging the HITRUST CSF

- Leverage HITRUST CSF Assurance Program to develop assessment questionnaire
- Develop criteria to assess vendors
  - Frequency
  - Type of review (Remote, Onsite, etc.)
  - Appropriate level of due-diligence
- Develop guidance for internal and external stakeholders to help drive assessment efforts
  - Regulatory requirements
  - Contractual requirements
  - Expectation associated with healthcare industry standards and best practices (HITRUST CSF)

Assessment Considerations

- Vendors Posing High Risk to Organization's Data
  - In lieu of proprietary assessment, accept HITRUST or alternate certification (SSAE 16, SOC 2® or ISO) mapped with HITRUST CSF
  - Perform specialized assessments based on processing environment on case to case basis to measure effectiveness of security controls
  - Perform onsite assessments to measure effectiveness of security controls until certification is obtained
- Vendors Posing Medium Risk to Organization's Data
  - In lieu of proprietary assessment accept HITRUST or alternate certification (SSAE 16 SOC 2 or ISO) mapped with HITRUST CSF
  - Perform remote, paper-based assessments leveraging HITRUST CSF
- Vendors Posing Low Risk to Organization's Data
  - In lieu of proprietary assessment accept HITRUST or alternate certification (SSAE 16 SOC 2 or ISO) mapped with HITRUST CSF
  - Perform remote paper based assessments leveraging HITRUST CSF
- Vendors That Do Not Pose Any Risk to Organization's Data
  - No assessment required

Risk Identification, Monitoring and Reporting

- Risk Identification
  - Analyze and rank risk, identified risks and associated impact to organization
  - Document risks in a centralized GRC repository or equivalent
- Risk Monitoring
  - Negotiate remediation requirements and associated plan with internal stakeholders and vendor
  - Communicate risk and associated impact to internal stakeholders
  - Periodic status check for remediation milestones
- Risk Reporting
  - Share risk metrics and associated progress periodically
  - Record accountability of accepted residual risks through formal, consistent process

Model and Align Proprietary Methodologies with the HITRUST CSF

- Adopt HITRUST CSF in developing any proprietary assessment methodology
  - Helps ensure consistency throughout the healthcare industry to assess vendors
  - Aligns to other regulatory requirements and industry best practices
- Accept HITRUST Certification for independent review of vendor's environment
  - HITRUST CSF is a single, comprehensive framework that harmonizes multiple standards and best practices to help ensure a consistent and efficient approach is followed
  - Assess once, use many: Helps business associates to leverage certification for other organizations across healthcare industry
  - Helps organizations to reduce time and efforts in order to focus more on specialized reviews of vendors
  - Can be tailored for unique requirements (i.e. SOC 2 Mapped with HITRUST CSF, EHNAC with HITRUST CSF, etc.)
- Consider and leverage HITRUST CSF BASICs for small and lower-risk healthcare vendors

Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight

HITRUST 2017
Learn. Collaborate. Deliver.