March 2, 2022:

1. Initial Assessment: How does IT get involved with the procurement of a vendor?

* How is the involvement documented?
* What are the Third Party Risk Levels?
  + How are they determined for each vendor?
* Is there an assessment done?
  + Independent assessments/audits for Report of Compliance, SOC1\_2\_3, NIST, Gramm Leach Bliley Act, SIG, SOX, HIPAA…
* If there are exceptions, how is it remediated for?
  + Security, IT, Privacy…
* When is IT’s role complete?

1. Ongoing Monitoring
   1. What is being done to ensure that the appropriate controls are not only in place but being adhered to?
   2. Based on Risk… how often are the re-assessments performed (High, Medium, Low, etc…)?
2. Security Exceptions
3. Review and Approvals – when is the CVS TPRG Tools used?
4. Renewal and Terminations. Does IT have a role?

Enterprise Third Party Risk Governance Program:

* Identifying areas of Risk with the Vendor?
  + Impacts of business or controls
    - Get a list of risk and “*What keeps the Governance team up at night*?”
    - Performance measurements, KPIs
* How does IT get involved with the procurement of a vendor?
  + Security, IT, Privacy…
* What are the roles of those involved with this program?
  + IT
  + Security
  + Compliance
  + Privacy/Legal – Non disclosure Agreements
  + Business specific
* Where are the roles and relationships of stakeholders noted?
  + What is the vendor/Third Party Role?
    - Type of support for CVS Health
    - What service to they provide?
    - Do these include SLA’s? (Business decision??)

Is there an inventory of Third Party Risk / Vendor policies?

* Specifically for IT and Security…
* Are these policies inspected/reviewed?
  + How often?

What does the vendor use for the monitoring and response of Cybersecurity and IT events?

* Incident Management and notification
  + CCERT, Incident Response Teams for process
* Most recent vulnerability and penetration tests

Does this vendor manage PHI, Financial Accounts, PCI, Business proprietary?

* Independent assessments/audits for Report of Compliance, SOC1\_2\_3, NIST, Gramm Leach Bliley Act, SIG, HIPAA…
* Is there a Non-Disclosure agreement?

HR Policies (ex. New Hire Onboarding & Termination)

Do they have formal Change Management processes?

Is there a Business Continuity and Disaster Recovery program?

* Regular testing for key systems and business processes
* Formal Plans approved by stakeholders