**Approach – Understand Environment**

• **Infrastructure, initial questions:**

– What does your team look like, do you use any third-parties, and who are the key resources? (network, servers, storage, etc.)

–  How is the datacenter setup and what are the key physical security controls?

–  How many offices/locations are supported?

–  What does the network diagram look like and what is the overall architecture of the network?

How is the network perimeter protected? (firewalls, IPS, WAF, URL filtering, AV)

What remote access technologies are in place? (MFA)

Is there a wireless network and how do users get access?

Do you have a separate cardholder data environment?

–  What is your physical and virtual server architecture?

How are virtual and physical servers patched?

* What is the overall process and technologies for server hardening and endpoint protections?
* How is administrative access restricted to servers? (MFA)
* What security events are being captured and reviewed?

–  What are your identity and access management solutions and how do they integrate across the environment?

–  Do you use any cloud environments (e.g., Office 365)?

* Do you have SANS? How do you manage it?
* Do you allow permanent access to third parties into your environment?

Why?

How?

–  What policies, standards or procedures do you have in place?

–  What are the major IT and security projects?

–  Any concerns related to security?

**Operations, initial questions:**

* What’s the overall onboarding and offboarding process for IT assets?
* How many computers/laptops and how are they protected against attacks (e.g., patching, hardening, endpoint protection, encryption, etc.)?
* What the policy for BYOD and how are mobile devices managed? • Do you have a mobile device management solution?
* How is user access managed?
  + What’s the onboarding / offboarding process?
* How is accessed to file shares and share points sites managed?
* How are passwords reset?
* What type of administrative access does operations have and how is it controlled?
* What policies, standards or procedures do you have in place?
* What is the major IT and security projects?
* Any concerns related to security?

**Applications, initial questions:**

–  What are the key applications, which ones are member facing and how critical/sensitive is the information in the applications?

–  How are the various applications secured and protected against attacks?

–  Are any applications hosted in cloud environments and how are they protected?

–  What’s your overall software development methodology and how do you protect vulnerabilities from being introduced during development?

–  How is access to applications managed? (onboarding/offboarding, SSO, password resets)

–  What types of databases do you have and how is access to databases restricted?

* Do you share/exchange information considered confidential (PII, Bank Account Information etc.) over Emails/DropBox etc.?
* Do you store considered confidential (PII, Bank Account Information etc.) on network drives?
  + How is the information protected? (Encryption)
  + How is access controlled?

–  What policies, standards or procedures do you have in place?

–  What are the major IT and security projects?

–  Any concerns related to security?

• **Risk/Security, initial questions:**

–  What types of security activities is your team involved in?

–  What security compliance requirements are in place? (e.g., PCI-DSS)

–  What is the security training and awareness program?

–  How are security incidents/events identified and managed?

–  What types of security assessments and testing is performed?

–  What does your vulnerability management process look like?

Who is performing vulnerability scanning and how are identified vulnerabilities remediated?

–  How is sensitive information identified and classified?

–  What policies, standards or procedures do you have in place?

–  What are the major IT and security projects?

–  Any concerns related to security?