NATIONAL
CREDITORS BAR
ASSOCIATION

Third Party Assessment Introduction Packet

1/25/2023

Table of Contents

Contents

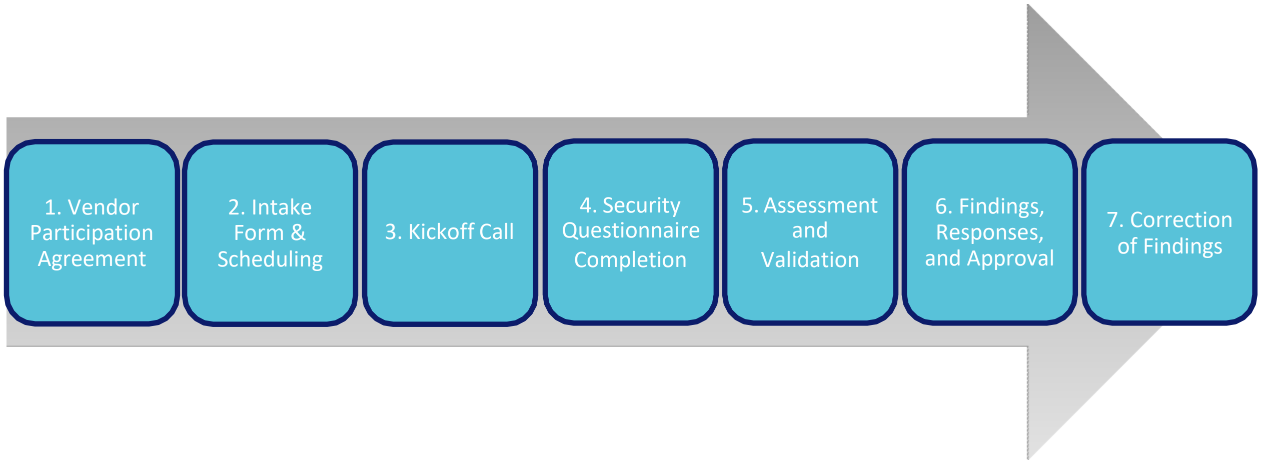
Purpose of Third Party Security Assessments

NCBA seeks to engage with the vendors that serve or intend to serve its members to provide a program that allows these vendors to demonstrate their internal control environment.

Third Party Assessments seek to protect customers, third parties, and NCBA members through enforcement of best practices and create an open dialogue between the third party and NCBA for improving in the following areas:

- Contracts
- Human Resources
- Information Security
- Customer Contact (Phone Calls)
- Physical/Environmental Security
- Incident Reporting
- Business Continuity & Disaster Recovery
- Insurance

Third Party Assessment Process Overview


1. Vendor Participation Agreement
2. Intake Form & Scheduling
3. Kickoff Call
4. Security Questionnaire Completion
5. Assessment and Validation
6. Findings, Responses, and Approval
7. Correction of Findings

1. Vendor Participation Agreement

NCBA will complete an internal process to determine which third parties are required to go through the assessment process. NCBA will work with the third parties to complete the Vendor Participation Agreement.

2. Intake Form & Scheduling

Crowe, a Third Party Assessments service provider to NCBA, will provide a link to the Intake Form to be completed in Crowe's instance of RSA Archer. This Intake Form must be completed within 1 week of receiving the link.

Following the completion of the Intake Form, the vendor will select a date using the Acuity Scheduling link provided in the Assessment Notification Email. This will align you with an assessor who will reach out to schedule a kickoff call. Please choose an assessment date that gives the assessor at least 2 weeks to review responses prior to the date.

3. Kickoff Call

Crowe may arrange an introductory meeting to answer any questions you have about the process, to confirm the high-level understanding of your service and to set expectations for completion of assessment. The start time of the assessment date will also be determined on this kickoff call.

Additionally, during the kickoff call you should have access to the full population of third parties, employees, and terminations for the assessor to select a random sample via the WebEx.

4. Assessment Questionnaire Completion

An Assessment questionnaire link will be issued via Crowe's instance of the RSA Archer application through email (see Appendix A). The Assessment questionnaire must be completed within 2 weeks of receiving the link.

Please access the link and provide detail in your questionnaire responses, including any relevant supporting attachments (e.g. security reports, certifications, policies and procedures). **NOTE: Please do NOT attach any PII within the Archer system.**

Be sure to include copies of your latest external network, web application and/or mobile application penetration assessment(s).

- These assessments must be performed by an independent third-party provider specializing in security penetration assessments.

5. Assessment & Validation

The Third Party Assessments team will review your responses and discuss any follow-ups and gaps during the assessment date chosen using the Acuity Scheduling link.

Third Party Assessments may request additional supporting documentation or evidence.

A demo of your product may be requested in order for us to gain a further understanding of the associated security risks with your services.

6. Findings, Response, and Approval

Following an assessment, the Third Party Security Assessments team will issue findings from the assessment.

Once a finding has been issued and reviewed, you will provide your response and management plan for remediation directly through Archer.

A report will be created once all responses are provided. The report will be delivered to NCBA and the vendor.

7. Correction of Findings

As a vendor of NCBA members, you will be required to address any issues not meeting NCBA’s requirements.

At the request of NCBA, Crowe may work with you for a period of one year to track remediation of all findings from the assessment.

Appendix A – FAQ

We have a SOC 2 report, is that enough to forego an assessment?
While a SOC report is a helpful artifact to aid our assessment team in validating controls, it does not cover all of the controls that we are required to validate. We will map the SOC 2 Type 2 report to our controls and use the information is it matches our testing procedure, but additional documentation and validation will need to occur for what is not covered.

We have a SOC 1 report, is that enough to forgo the assessment?
Unfortunately, the SOC 1 report is primarily used for controls around financial reporting; therefore, we cannot use a lot of the attestation for our security assessment. Additionally, a type 1 and type 2 differs in that a type 1 does not test the operating effectiveness of the control only that the control is implemented. We require our testing procedure to match that of the attestation report in order to use it to validate our controls.

We have many services and applications that our organization offers, what is in scope for this assessment?
Any service provided to NCBA members is eligible to undergo the security assessment process. Please list the services and accompanying applications that your organization would like to be in scope and NCBA will confirm the appropriate coverage.

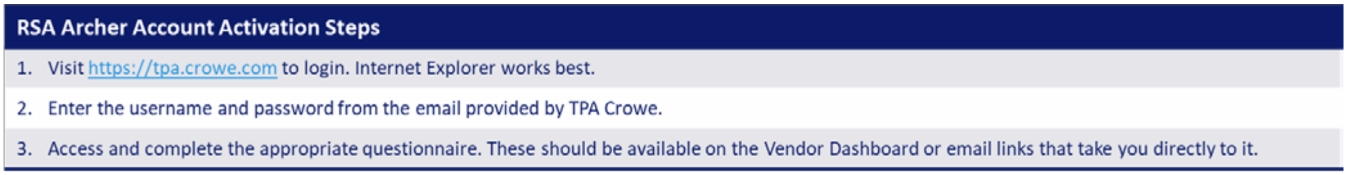
Appendix B – RSA Archer

RSA General Archer Information

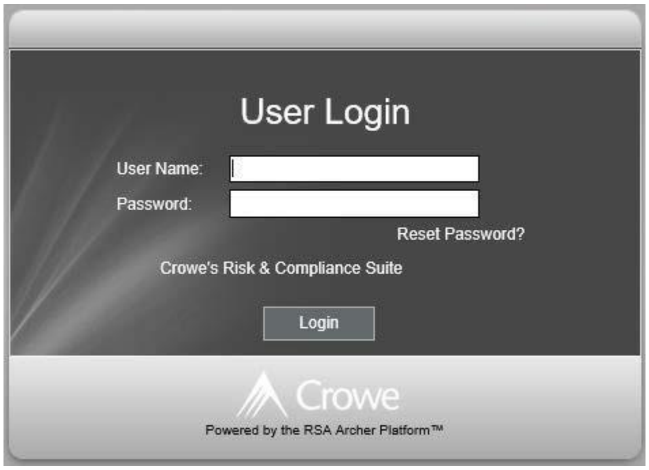
Each Third Party will be sent an email providing your username and temporary password for accessing RSA Archer. This password will be changed at first log-in.

Expect a system-generated email from the RSA Archer system requiring response with a link to the applicable questionnaires. If not received, please confirm your appropriate contact information by emailing TPA@Crowe.com.

Activating Archer Account

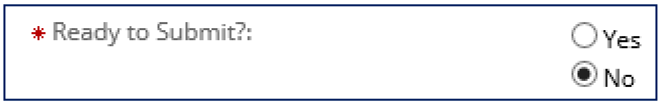


RSA Archer Account Activation Steps
1. Visit https://tpa.crowe.com to login. Internet Explorer works best.
2. Enter the username and password from the email provided by TPA Crowe.
3. Access and complete the appropriate questionnaire. These should be available on the Vendor Dashboard or email links that take you directly to it.


User Login
User Name:
Password:
Reset Password?
Crowe's Risk & Compliance Suite
Login
Crowe
Powered by the RSA Archer Platform™

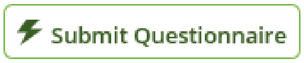
Completing the Assessment Questionnaire

A direct link to the Assessment Questionnaire will be provided via an email notification from RSA Archer. Please complete all included sections, answering questions fully and attaching documentation where requested. Once all sections are complete, mark the questionnaire as ready to be submitted at the top of the screen.



* Ready to Submit?: ○ Yes ● No

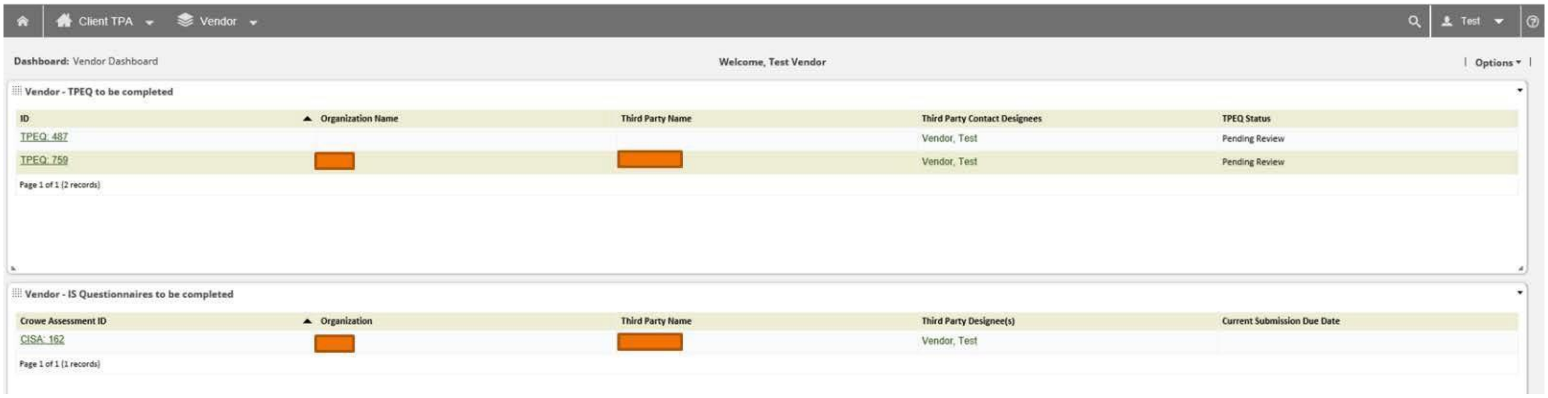
Once marked "Yes", click the button in the top right to submit the questionnaire



Vendor Dashboard

A dashboard is available to see everything that you are assigned. If you cannot find a link to the Intake Form (TPEQ) or Assessment Questionnaire, you can find it on the dashboard.

Click the "Vendor" button in the top right to get to your dashboard. Below is how it will look.



Dashboard: Vendor Dashboard

Welcome, Test Vendor

Vendor - TPEQ to be completed

ID	Organization Name	Third Party Name	Third Party Contact Designees	TPEQ Status
TPEQ: 487			Vendor, Test	Pending Review
TPEQ: 759	[redacted]	[redacted]	Vendor, Test	Pending Review

Page 1 of 1 (2 records)

Vendor - IS Questionnaires to be completed

Crowe Assessment ID	Organization	Third Party Name	Third Party Designee(s)	Current Submission Due Date
CISA: 162	[redacted]	[redacted]	Vendor, Test	

Page 1 of 1 (1 records)

Appendix C – Assessment Questionnaire

Control #	Topic	Sub Topic	Control	Question	Test
Contracts.1.0	Contracts	Vendor Contracts	Subcontractor must have up-to-date contracts with all material vendors.	Do you use vendors or subcontractors to support the services in scope for this assessment? If yes, Please list all third parties that support that have access to systems or data for in scope services.	Sample 3 contracts and validate that the following are included: Audit Rights Master Service Agreement/Service Legal Agreement Adherence Background Check requirements Existence of Business Continuity/DR Plan Physical and Data Security Requirements Minimum Insurance Requirements (document amount) Termination Rights
HR.1.0	Human Resource Security	Background Checks	Employees with direct access to NPI have underdone a 10 year National Background check (criminal)	Does your organization require employees with direct access to NPI to undergo background checks, including criminal, reference, SSN trace, etc.?	Sample 5 employees to verify that they have undergone background checks.
HR.2.0	Human Resource Security	Employment Forms	Organization appropriately stores and requires employees to complete I-9/W-2 forms.	Are all employees required to complete an I-9 or equivalent?	Using the same 5 employees, request the completed I-9/W-2 forms and validate they are completed and being stored appropriately.
HR.3.0	Human Resource Security	Acceptable Use/Employee Handbook	Employees are required to acknowledge an employee handbook or equivalent upon onboarding	Are all employees required to provide written adherence to understanding company policies and acceptable use of devices?	Using the same 5 employees, request signed versions of the employee handbook or equivalent.

IS.1.0	Information Security	Information Security Program	Organization has a documented and implemented Information Security Program.	Do you have an Information Security Policy that is reviewed and approved annually and communicated to the entire organization?	Inspect the Information Security Program/Policy and validate that it has been reviewed in the past year and approved by management.
IS.2.0	Information Security	Information Security Organization	The Organization has a dedicated Information Security Organization responsible for implementing the program.	Do you have a dedicated Information Security?	Inspect an org chart for information security
IS.3.0	Information Security	Network Architecture/Data Flow	Vendor maintains an up-to-date network diagram and appropriate segmentation is in place (layers, DMZ, etc.).	Do you have an up-to-date network diagram? Describe how data flows in and out of the environment and systems supporting NCBA members.	Inspect a network diagram and determine if the architecture is appropriate (2-tier/3-tier, DMZs, etc.).
IS.4.0	Information Security	Data in transit	NCBA member data is transmitted to and from the vendor in a secure manner. Transport and/or data layer encryption is appropriately employed given data sensitivity.	Is all data encrypted in transit?	Inspect network diagram and data flow diagram and confirm that appropriate encryption is in place in transit.
IS.5.0	Information Security	Intrusion Detection and Prevention	Organization has implemented an IDS/IPS and logs are being sent to a SIEM and configured to alert.	Has your organization implemented and IDS/IPS solution?	Validate that and IDS/IPS has been implemented and logs are sent to a SIEM solution.
IS.6.0	Information Security	Logging and Monitoring		Has your organization implemented a Security Information and Event Management (SIEM) solution?	Validate that all critical systems are sending logs to a SIEM.
IS.7.0	Information Security	Data at Rest	Data flows specific to the vendor's solution appropriately secure data at rest.	Is all data encrypted at rest?	Validate that appropriate encryption is in place for data at rest. Document what is being used.

IS.8.0	Information Security	Access Review Policies	User access policies are in place that define how users are added, removed, and changed	Do you have a documented process in place for user access, changes, and terminations.	Inspect Policy and validate that there is a process in place to provide access to in scope systems. Does this include administrative rights?
IS.9.0	Information Security	Role-Based Access	Systems require role-based access based on users job functions.	Do the in scope systems employ role-based access?	Review Policy or Role Matrix and Validate that the systems use role-based access.
IS.10.0	Information Security	Access Reviews	User access is reviewed at least quarterly	Are access reviews performed at least quarterly?	Inspect policy and validate it requires quarterly access reviews. Inspect the last access review performed.
IS.11.0	Information Security	Termination Review Policies	User access policies include Terminations and require accounts to be disabled within 1 business day from all systems	Do you have documented termination procedures in place?	Ensure the policies and procedures for terminating employees include removal of physical and systems access within 1 business day. Select a sample of recent terms and verify their access is removed.
IS.12.0	Information Security	Remote Access	The Vendor properly secures remote access to its networks.	Is remote access to the production environment appropriately secured?	Validate that remote access is appropriately restricted and logged.
IS.13.0	Information Security	Password Parameters	Passwords for the solution(s) provided to NCBA Member firms have been appropriately implemented to protect application data, including password length, strength, history, expiration. -8 character minimum - At least two character sets required for password complexity - Password reuse restricted -maximum password age/change interval of 90 days -account lockout enforced after no more than 3	Do Passwords for the solution(s) provided to NCBA Member firms meet the below requirements: -8 character minimum - At least two character sets required for password complexity - Password reuse restricted -maximum password age/change interval of 90 days -account lockout enforced after no more than 3 incorrect attempts, and locks out until reset by an administrator	Inspect a screenshot of the password Policies for the solutions provided to NCBA member firms

			incorrect attempts, and locks out until reset by an administrator		
IS.13.1	Information Security	Password Storage	For the solution(s) provided to NCBA Member firms, passwords are encrypted at rest, or hashed using a secure one-way cipher and salted	Are passwords encrypted at rest for the in scope solutions?	Validate that passwords are encrypted or hashed and salted.
IS.14.0	Information Security	Multifactor	Multifactor authentication is used to strengthen communication controls for the solution(s) provided to NCBA Member firms, where appropriate.	Is MFA required for access to all in scope solutions for general users?	determine if MFA is in place and document what is used.
IS.15.0	Information Security	Shared Accounts	The vendor does not allow shared accounts.	Are all user accounts unique?	Validate that all accounts are unique and no shared accounts are used for in scope systems.
IS.16.0	Information Security	Email Requirements	Users access to email is restricted based on job function.	Is access to email restricted based on business need?	Review group policy or equivalent to determine that email is restricted by job function.
IS.16.1	Information Security	Email Data Loss Protection	Appropriate DLP controls are in place to restrict exfiltration of sensitive data.	Do you employ network based or host based DLP in the production environment?	Validate that DLP controls are in place for outgoing email, including encrypted and unencrypted attachments.
IS.17.0	Information Security	Removable Media Restrictions	Removable media is restricted	Is removable media restricted from all users?	Validate via Group Policy or Equivalent that Removable media is restricted.

IS.18.0	Information Security	Web Proxy	Access to high risk sites like public file sharing sites is restricted	Is access to high risk sites, including public cloud sharing sites (dropbox, box) restricted?	Validate that a web content filter or web proxy is in places restricting access to sites like dropbox and box, personal email, etc.
IS.19.0	Information Security	Internet Restrictions	Internet is restricted to appropriate users.	Do you restrict access to the internet based on business need?	Validate that all users with internet access have a business need for it.
IS.20.0	Information Security	Administrative Access	Users administrative rights have been restricted unless required for business purposes	Have local administrator rights been removed from all users accept for business need?	Validate that admin privileges have been restricted and that any users with admin access have been reviewed and approved. Confirm that users are restricted from changing configuration settings on their workstations, including AV and account lockout time.
IS.21.0	Information Security	Full Disk Encryption	Full disk encryption is required for laptops and workstations	Does you employ full disk encryption on all workstations and Laptops	Inspect a screenshot showing full disk encryption.
IS.22.0	Information Security	Vulnerability Management	The vendor has a documented vulnerability management program in place.	Do you have a documented vulnerability management program in place?	Validate that there is a documented vulnerability management program and Inspect the most recent vulnerability scans and determine if there are any open high risk issues.
IS.23.0	Information Security	Web Application Penetration Testing	Web Application Penetration Testing has been performed on any web solution provided by the vendor. This includes unauthenticated and authenticated testing, performed both by internal resources and independent provider.	Have you contracted with an independent third party to perform Web Application Penetration testing on the in scope applications?	Inspect the most recent web application penetration test executive summary.

IS.24.0	Information Security	External/Internal Network Penetration testing	The vendor contracts with a reputable third-party to perform independent network penetration testing (internal and external) at least annually on all networks that contain or access NCBA Member data.	Have you contracted with an independent third party to perform internal and external network Penetration testing on the production environment?	Inspect the most recent internal, external penetration test executive summary.
IS.25.0	Information Security	Mobile Application Penetration Testing	Mobile application penetration testing has been performed on any mobile application provided by the vendor. This includes unauthenticated and authenticated testing, performed by independent provider.	Have you contracted with an independent third party to perform Mobile Application Penetration testing on the in scope applications?	Inspect the most recent mobile app penetration test executive summary.
IS.26.0	Information Security	Patch Management	Servers are patched for operating system and major component updates upon patch release and evaluation. These practices are governed by a formal policy and/or procedure. Patches are applied in a timely fashion based on the significance of the vulnerability. Patches are applied in accordance with system change management standards.	Do you have a Patch Management Policy in Place?	Review the patch management policy and document the requirement on critical and security patches. Validate patches are current by looking at the patch console.
IS.27.0	Information Security	Anti Virus	Anti-virus software is used to protect all servers and workstations, per Supplier policy. No exceptions apply to any systems housing NCBA member data. Email and attachments are scanned by the mail server and blocked as appropriate	Is anti-virus installed on all workstations and servers with updated signatures?	Sample a workstation to verify that AV signatures are up to date.

IS.28.0	Information Security	Device Hardening	The Supplier's Information security program includes defined standards for operating system, application and network device security and hardening	Do you have documented hardening guides for all devices?	Inspect a sample of hardening guides.
IS.29.0	Information Security	Software Development Program	A defined systems development methodology has been formally implemented with policies, procedures and standards communicated and followed. This methodology includes programming standards to confirm that design and structure standards are followed (confirm the correct implementation of logic and algorithms, removal of unneeded content, as well as standards to prevent security weaknesses, like OWASP top ten vulnerabilities)	Do you have a formally documented SDLC Program in place?	Inspect the SDLC Policy and comment the methodology and approach.
IS.30.0	Information Security	Static and Dynamic Code Scans	Static and dynamic code vulnerability analysis is performed on all code prior to implementation in production leveraging an industry standard code scanner.	Do you perform static and dynamic code scanning on the entire code base?	Validate static and dynamic scanning is occurring and document the tool names
IS.31.0	Information Security	Formal Approvals	Formal approvals are captured at each stage of the development lifecycle (Requirements, Design, Testing, User Acceptance, Production rollout, etc.). When approvals are captured, it is clear who is	Do you require formal approvals at all stages of the development lifecycle?	Inspect a ticket to determine that approvals happen before pushing code to production.

			approving, the date they are approving, and what they are approving.		
CC.1.0	Customer Contact - Phone Calls (ONLY if phone calls are made)	Recordings	All calls are recorded and stored securely for 3 years	Are all calls recorded and stored for 3 years?	Validate that all calls, both inbound and outbound, are recorded and stored securely. Document the retention and make sure its 3 years by sampling 5 calls.
CC.1.1	Customer Contact - Phone Calls (ONLY if phone calls are made)	Recording Retrieval	All call recordings can be obtained within 24 hours of request	Can all call recordings be obtained within 24 hours of a request?	Validate that all call recordings can be obtained within 24 hours of request
CC.2.0	Customer Contact - Phone Calls (ONLY if phone calls are made)	Call auditing	Organization has appropriate auditing procedures in place to ensure calls are audible	Do you have auditing procedures in place to ensure recordings are audible?	Inspect the most recent audit of phone calls and determine if any issues were identified.
CC.3.0	Customer Contact - Phone Calls (ONLY if phone calls are made)	Recording Policies	A process is in place to handle customers that do not wish to be recorded	Do you have a process in place to handle customers that do not wish to be recorded?	Inspect the policy and validate that it covers customers that do not want to be recorded.
CC.4.0	Customer Contact - Phone Calls (ONLY if phone calls are made)	Call Recording failure	A process is in place to handle recording failures.	Do you have a process in place to handle recording failures?	Validate that there is alerting in place to identify if a recording fails
CC.5.0	Customer Contact - Phone Calls (ONLY if phone calls are made)	Independent assessment of call recording Requirements	A process is in place to audit compliance with call recording requirements.	Do you have a process in place to audit compliance with call recording requirements?	Inspect last audit of call recording compliance.
IR.1.0	Incident Reporting	Fraudulent Activity Monitoring	Appropriate controls are in place to monitor user activity	Do you have controls in place to monitor user	Validate that technical controls are in place to log and alert on malicious activity and access.

			with systems containing sensitive data.	activity within systems containing sensitive data?	
IR.2.0	Incident Reporting	Incident Response Policy	A policy is in place that covers incident logging, roles, client communication.	Do you have a documented incident management policy?	Inspect the Incident Management Policy and validate it includes Roles, Logging of Incidents, and client communication.
IR.3.0	Incident Reporting	Incident Logging	Organization has an up to date log of all incidents	Do you have a formal log of all incidents?	Review the incident log and verify that the organization is centrally tracking incidents
BCDR.1.0	Business Continuity (BCP) and Disaster Recovery (DR)	Business Continuity and DR Plan/Policy	A BCP and DR plan is in place that includes, but is not limited to: - Weather - Events / Natural Disaster - Technical Failure (IT), - Power Outages, - Cyber Events, - Unavailability of Workforce, Physical Site or Telecom functionality	Do you have a documented BCP and DR plan?	Inspect the BCP/DR plan and verify the below is covered: - Weather - Events / Natural Disaster - Technical Failure (IT), - Power Outages, - Cyber Events, - Unavailability of Workforce, Physical Site or Telecom functionality
BCDR.2.0	Business Continuity (BCP) and Disaster Recovery (DR)	BCP/DR Plan	Organization has a dedicated team in place to respond to BCP/DR events.	Do you have a dedicated team in place to handle BCP/DR events?	Confirm that there is a call tree and pick 3 names from to confirm the persons are still employed by the company and contact information is correct.
BCDR.3.0	Business Continuity (BCP) and Disaster Recovery (DR)	RTO/RPO	The RTO/RPO is documented for each critical system	What is the RTO/RPO for all in scope applications?	Request the latest DR test and validate that Rto and RPO has been documented and meets the documented requirements.
BCDR.4.0	Business Continuity (BCP) and Disaster Recovery (DR)	Critical Failure	The BCP/DR plan includes a process for critical failure of a subcontractor	Does your BCP Plan include a process to deal with critical failure of a subcontractor or vendor?	Inspect the Policy an validate that it includes a process for critical failure of a subcontractor or vendor.

BCDR.5.0	Business Continuity (BCP) and Disaster Recovery (DR)	BCP/DR Testing	BCP/DR testing occurs annually, has appropriate coverage and is communicated to management	Is your DR plan tested annually?	Inspect the latest BCP/DR test and validate that there were no issues. Validate that it includes: power backup or call recording back up (if required) Validate that the results were documented and remediated and tracked. Validate that the results were shared with leadership.
PS.1.0	Physical Security	Front Desk	Organization has a receptionist present that issues name tags/IDs to all visitors.	Does your organization have a receptionist or lobby attendant responsible for issuing name tags/visitor IDs at all locations?	Walkthrough the facility and verify that there is a front desk with appropriate coverage and IDs provided to visitors.
PS.2.0	Physical Security	Visitor Log	The organization keeps appropriate records of visitors.	Does your organization require visitors to sign a log?	Validate that all visitors are requires to sign into a visitor log upon entry and that the information is archived per best practices.
PS.3.0	Physical Security	Badge Access	The organization employs appropriate access controls on doors to secure areas.	Does your organization have appropriate access controls in place on doors (badge readers)?	Ensure that all sensitive areas (IR Room/Data Center) within the facility are secured and require restricted badge access.
PS.4.0	Physical Security	Door Alarms	The organization employs alarms at all doors; exterior, interior, secured rooms and fire doors activate alarms after no less than 90 seconds	Are alarms installed on all entry and exit points to sensitive areas?	Review console to verify alarms are in place on access points.
PS.5.0	Physical Security	CCTV	Facilities and datacenters have appropriate CCTVs throughout and monitoring sensitive areas.	Do you have CCTVs monitoring sensitive areas?	Through a walk through verify that CCTVs are in appropriate areas and document the retention period of the tapes.
PS.6.0	Physical Security	Printing	Organization has appropriate security controls around printers	Do you have controls around leaving sensitive information in printers?	Observe printers within the facility and validate that there is no sensitive data being left in

					the printer or that access cards are required for printing.
PS.7.0	Physical Security	Shred Bins	Organization requires clean desk, clear screen and has shred bins within the facility	DO you have a clean desk ,clear screen policy in place?	Validate that locked Shred Bins are on premise and inspect a certificate of destruction from the provider.
Insurance.1.0	Insurance	Insurance Requirements	Vendor has appropriate insurance in place where required. General Liability, A&O, Cyber, Umbrella	Please select all insurance policies that your organizations has: General Liability, A&O, Cyber, Umbrella	If they say yes, lets ask a follow up question asking them to attach the certificate, and defining the limits per occurrence and aggregate for each coverage type. For cyber liability, we should ask if their policy covers 1)Credit Monitoring for impacted parties 2)First Party Liability – Damages sustained by them directly 3) Third Party Liability – Damages sustained by their clients. We should provide a notes field for them to further describe their cyber coverage since this varies.