

# SIG Lite Security Assessment Questionnaire

Standardized Information Gathering v2017.1 · Free resource from Macktez

Governance /  
Risk

Assets / Devices

Human  
Resources

Physical

Operations

Access Control

Applications

Incidents /  
Threats

Compliance

Network /  
Privacy

ORGANIZATION NAME

PRIMARY CONTACT

TITLE / ROLE

EMAIL ADDRESS

PHONE NUMBER

ASSESSMENT DATE

SERVICE / RELATIONSHIP SCOPE

VENDOR / PROVIDER NAME

## How to Complete This Questionnaire

- For each question, select Yes, No, IDK (I Don't Know), or N/A.
- Use Additional Notes to explain, especially for No, IDK, or N/A answers.
- Honest responses are more useful and safer than inflated ones.
- Misrepresenting controls creates liability if a breach occurs.
- "Scoped Data" = systems and data relevant to this specific service relationship.
- A SOC 2 Type II report, if available, is generally preferred over a completed SIG Lite.
- For help completing or interpreting this form: [macktez.com](https://macktez.com)

## A. Risk Assessment and Treatment

| QUESTION / REQUIREMENT                                                                                                                                                                                       | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------------|
| 1 Is there a risk assessment program that has been approved by management, communicated to constituents and an owner to maintain and review the program? if yes, does it include:                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 2 Is there a program to manage the treatment of risks identified during assessments?                                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 3 A formal process for assigning appropriate management ownership for each risk?                                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 4 A formal process for appropriate management knowingly and objectively accepting risks and approving action plans?                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 5 A formal process for tracking the status of action plans and reporting them to management?                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 6 Controls identified for each material risk?                                                                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 7 Measures for defining, monitoring, and reporting risk metrics?                                                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 8 Do Subcontractors have access to Scoped Systems and Data? (backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors, etc.)? If yes, is there: | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 9 A documented vendor management process in place for the selection, oversight and risk assessment of third party vendors? If yes, does it include:                                                          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 10 Approval by management?                                                                                                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 11 Annual review?                                                                                                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 12 Required reassessment when service delivery or contract changes?                                                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 13 Review of the subcontractor's vendor management policy and procedures?                                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 14 Is there a process to identify and log subcontractor information security, privacy and/or data breach issues?                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |

|    |                                                                                                                                               |                          |                          |                          |                          |  |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--|
| 15 | Is there a vendor management program?                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 16 | Do external parties have access to Scoped Systems and Data or processing facilities?                                                          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 17 | Is the maturity of IT management processes formally evaluated at least annually using an established benchmark (e.g., COBIT maturity models)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 18 | Are there regular privacy risk assessments conducted? If yes, provide frequency and scope. If no, explain reason.                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 19 | Are identified privacy risks and associated mitigation plans formally documented and reviewed by management?                                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 20 | Are reasonable resources (in time and money) allocated to mitigating identified privacy risks?                                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 21 | Is there a compliance risk management system that addresses the quality and accuracy of reported consumer data?                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 22 | Is there a compliance risk management system that addresses the quality of assembling and maintaining the data?                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |

## B. Security Policy

| QUESTION / REQUIREMENT                                                                                                                                                    | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------------|
| 23 Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 24 Have the policies been reviewed in the last 12 months?                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |

## C. Organizational Security

| QUESTION / REQUIREMENT                                                                       | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES |
|----------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------------|
| 25 Is there a respondent information security function responsible for security initiatives? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |

## D. Asset and Information Management

| QUESTION / REQUIREMENT                                                                                                                                                                                                                                | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------------|
| 26 Is there an asset management policy approved by management, communicated to constituents and an owner to maintain and review?                                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 27 Is information classified?                                                                                                                                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 28 Is there a removable media policy or program (CDs, DVDs, tapes, disk drives) that has been approved by management, communicated to appropriate constituents, and an owner to maintain and review the policy?                                       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 29 Is Scoped Data sent or received via physical media?                                                                                                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 30 Are encryption tools managed and maintained for Scoped Data? If yes:                                                                                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 31 Are clients provided with the ability to generate a unique encryption key?                                                                                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 32 Are clients provided with the ability to rotate their encryption key on a scheduled basis?                                                                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 33 Are staff able to access client Scoped Data in an unencrypted state?                                                                                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 34 Are staff able to access client's encryption keys?                                                                                                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 35 Is data segmentation and separation capability between clients provided?                                                                                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 36 Does the ability exist to legally demonstrate sufficient data segmentation, in the event of a client subpoena or a forensics incident, so as not to impact other clients data if using resource pooling?                                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 37 Is there a data classification retention program that identifies the data types that require additional management and governance?                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 38 Is there a self-service portal or API call available to clients which provides the ability to place a "Legal hold" on client data which may be subject to a legal action, without impacting other clients data retention or destruction schedules? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |

## E. Human Resource Security

| QUESTION / REQUIREMENT                                                                                                                                 | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------------|
| 39 Is there a Human Resource policy approved by management, communicated to constituents and an owner to maintain and review? If yes, does it include: | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 40 Security roles and responsibilities?                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 41 Background screening?                                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 42 Employment agreements?                                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 43 Security awareness training?                                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 44 Disciplinary process for non-compliance?                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 45 Termination or change of status process?                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 46 Are background checks performed for Service Provider Contractors and Subcontractors?                                                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 47 Do information security personnel have professional security certifications?                                                                        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |

## F. Physical and Environmental Security

| QUESTION / REQUIREMENT                                                                       | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES |
|----------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------------|
| 48 Is there a physical security program?                                                     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 49 Are physical security and environmental controls in the data center and office buildings? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 50 Are visitors permitted in the facility?                                                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |

## G. Operations Management

| QUESTION / REQUIREMENT                                    | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES |
|-----------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------------|
| 51 Are management approved operating procedures utilized? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |

|    |                                                                                                                                                                                                           |                          |                          |                          |                          |  |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--|
| 52 | Is there an operational change management/change control policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 53 | Are backups of Scoped Systems and Data performed?                                                                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 54 | Are Cloud Services provided? If yes, what service model is provided (select all that apply):                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 55 | Software as a Service (SaaS)?                                                                                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 56 | Infrastructure as a Service (IaaS)?                                                                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 57 | Private cloud?                                                                                                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 58 | Public cloud?                                                                                                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 59 | Community cloud?                                                                                                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 60 | Hybrid cloud?                                                                                                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 61 | Is there a client management portal which allows distributed business accounts (business units/departments) to be managed under a single central corporate account?                                       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 62 | Are application self service features or an Internet accessible self-service portal available to clients?                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 63 | Can clients run their own security services within their own cloud environment?                                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 64 | Is there a management approved process to ensure that image snapshots containing Scoped Data are authorized prior to being snapped?                                                                       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 65 | Is there a formal process to ensure clients are notified prior to changes being made which may impact their service? If yes, what is the communication method:                                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 66 | Is there a scheduled maintenance window? If yes, what is the frequency:                                                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |

**67** Is there a scheduled maintenance window which results in client downtime? If yes, what is the downtime: ☐ ☐ ☐ ☐

**68** Is there an online incident response status portal, which outlines planned and unplanned outages? If yes, how long after an unplanned outage is this updated: ☐ ☐ ☐ ☐

## H. Access Control

| QUESTION / REQUIREMENT                                                                                                                                                                                      | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|----------------------|
| <b>69</b> Are electronic systems used to transmit, process or store Scoped Systems and Data?                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>70</b> Are individual IDs required for user authentication to applications, operating systems, databases and network devices?                                                                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>71</b> Are passwords used?                                                                                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>72</b> Is there a password policy for systems that transmit, process or store Scoped Systems and Data that has been approved by management, communicated to constituents, and enforced on all platforms? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>73</b> Is remote access permitted?                                                                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>74</b> Is standards based federated ID capability available to clients (e.g., SAML, OpenID)?                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>75</b> Is two factor authentication required to access the production environment containing Scoped Data?                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>76</b> Are staff able to access client Scoped Data? If not, please identify the controls used to prevent this.                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>77</b> Is there a process which allows the client to specifically list who from the provider will have access to their Scoped Systems and Data?                                                          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |

## I. Application Security

| QUESTION / REQUIREMENT                                                     | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES     |
|----------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|----------------------|
| <b>78</b> Are applications used to transmit, process or store Scoped Data? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |

|    |                                                                                                                                                                                                                                 |                          |                          |                          |                          |  |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--|
| 79 | Is a web site supported, hosted or maintained that has access to Scoped Systems and Data?                                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 80 | Are Web Servers used for transmitting, processing or storing Scoped Data? If yes, for all server platforms is/are:                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 81 | Is HTTPS enabled for all web pages used as part of the scoped service?                                                                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 82 | All available high-risk security patches applied and verified at least monthly?                                                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 83 | Are third party alert services used to keep up to date with the latest vulnerabilities?                                                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 84 | Events relevant to supporting incident investigation regularly reviewed using a specific methodology to uncover potential incidents?                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 85 | Operating system and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?                                                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 86 | Is application development performed?                                                                                                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 87 | Is there a secure software development lifecycle policy (including mobile software applications) that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 88 | Is development, test, and staging environment separate from the production environment? If so, how are they segmented:                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 89 | Is there a formal Software Development Life Cycle (SDLC) process?                                                                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 90 | Are change control procedures required for all changes to the production environment?                                                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 91 | Is Scoped Systems and Data ever used in the test, development, or QA environments? If yes, is:                                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 92 | Is there a documented change management / change control process? If yes, does it include:                                                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |

|           |                                                                                                       |                          |                          |                          |                          |                      |
|-----------|-------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|----------------------|
| <b>93</b> | Are compilers, editors or other development tools present in the production environment?              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>94</b> | Is a secure code review performed at least annually?                                                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>95</b> | Is each release subject to a full secure code review?                                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>96</b> | Are applications analyzed on a regular basis to determine their vulnerability against recent attacks? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>97</b> | Is there a formal development methodology in operation? If yes, which groups does it include?:        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>98</b> | Are mobile applications that access Scoped Systems and Data developed?                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |

## J. Incident Event and Communications Management

| QUESTION / REQUIREMENT                                                                                                                                                                                  | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|----------------------|
| <b>99</b> Is there an Incident Management Program that has been approved by management, communicated to constituents and an owner to maintain and review the program? If yes, does the program include: | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>100</b> Privacy Incidents?                                                                                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>101</b> Is there a formal Incident Response Plan?                                                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>102</b> Is there a 24x7x365 staffed phone number available to clients to report security incidents?                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |

## K. Business Resiliency

| QUESTION / REQUIREMENT                                                                                                                            | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES     |
|---------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|----------------------|
| <b>103</b> Is there an established Business Resiliency program that has been approved by management and communicated to appropriate constituents? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>104</b> Has a Business Impact Analysis been conducted?                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |
| <b>105</b> Is there a formal process focused on identifying and addressing risks of disruptive incidents to the organization?                     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="text"/> |

|     |                                                                                                                                        |                          |                          |                          |                          |  |
|-----|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--|
| 106 | Are specific response and recovery strategies defined for the prioritized activities?                                                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 107 | Are formal business continuity procedures developed and documented?                                                                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 108 | Has senior management assigned the responsibility for the overall management of the response and recovery efforts?                     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 109 | Is there a periodic (at least annual) review of your Business Resiliency Program?                                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 110 | Are there any dependencies on critical third party service providers?                                                                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 111 | Is there a formal, documented exercise and testing program in place?                                                                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 112 | Is there an Influenza Pandemic / Infectious Disease Outbreak Plan?                                                                     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 113 | Is there a specific Recovery Time Objective (RTO)? If yes, what is it?                                                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 114 | Are all suppliers of critical hardware, network services and facility services involved in annual continuity and recovery tests?       | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 115 | Are site failover tests performed at least annually?                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 116 | Do contracts with Critical Service Providers include a penalty or remediation clause for breach of availability and continuity SLAs?   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| 117 | Is there sufficient redundancy capacity to ensure services are not impacted in multi-tenancy environments during peak usage and above? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |

## L. Compliance

| QUESTION / REQUIREMENT                                                                                                                                                                                                   | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------------|
| 118 Is there an internal audit, risk management, or compliance department, or similar management oversight unit with responsibility for assessing, identifying and tracking resolution of outstanding regulatory issues? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |

**119** Are there policies and procedures to ensure compliance with applicable legislative, regulatory and contractual requirements including intellectual property rights on business processes or information technology software products?

☐ ☐ ☐ ☐

**120** Is there a records retention policy covering paper and electronic records, including email in support of applicable regulations, standards and contractual requirements?

☐ ☐ ☐ ☐

**121** Is licensing maintained in all jurisdictions where required?

☐ ☐ ☐ ☐

**122** Is there an documented internal compliance and ethics program to ensure professional ethics and business practices are implemented and maintained?

☐ ☐ ☐ ☐

**123** Are marketing or selling activities conducted directly to Client's customers?

☐ ☐ ☐ ☐

**124** Are there direct interactions with your client's customers?

☐ ☐ ☐ ☐

**125** Are documented policies and procedures maintained for enabling compliance with applicable legal, regulatory, or contractual obligations related to information security requirements?

☐ ☐ ☐ ☐

**126** Is there a documented governance process to identify and assess changes that could significantly affect the system of internal controls for security, confidentiality and availability?

☐ ☐ ☐ ☐

**127** Are accounts opened, transactions initiated or other account initiation activity applying payments, taking payments, transferring funds, etc. through either electronic, telephonic, written or in-person requests made on behalf of your client's?

☐ ☐ ☐ ☐

**128** Are these sites, applications and systems used to also transmit, process or store non-scoped data?

☐ ☐ ☐ ☐

**129** Are all transaction details (such as payment card info and information about the parties conducting transactions) prohibited from being stored in the DMZ?

☐ ☐ ☐ ☐

**130** Does the service provider permit client audits and assessments?

☐ ☐ ☐ ☐

## M. End User Device Security

| QUESTION / REQUIREMENT                                                                                                                                                                                                | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------------|
| 131 Are End User Devices (Desktops, Laptops, Tablets, Smartphones) used for transmitting, processing or storing Scoped Data? If yes, for all platforms, are:                                                          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 132 Security configuration standards documented? If yes, are:                                                                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 133 All available high-risk security patches applied and verified at least monthly on all server platforms?                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 134 Sufficient detail contained in Operating System and application logs to support incident investigation, including successful and failed login attempts and changes to sensitive configuration settings and files? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 135 Operating system and application logs relevant to supporting incident investigation protected against modification, deletion, and/or inappropriate access?                                                        | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 136 Are constituents allowed to utilize mobile devices within your environment? If yes, which of the following functions are allowed:                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 137 View Scoped Data?                                                                                                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 138 Process Scoped Data?                                                                                                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 139 Delete Scoped Data?                                                                                                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 140 Store Scoped Data?                                                                                                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 141 Is there a mobile device management program in place that has been approved by management and communicated to appropriate constituents?                                                                           | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 142 Is there a Mobile Device Management solution in place?                                                                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| 143 Is there an approved process for IT to off-board mobile devices when a constituent terminates, or requests to on-board a new mobile device? If yes, does it:                                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |

**144** Are staff technically prevented from accessing the administrative environment via non-managed private devices? If yes, is it from:

☐ YES ☐ NO ☐ IDK ☐ N/A

## N. Network Security

### QUESTION / REQUIREMENT

YES NO IDK N/A ADDITIONAL NOTES

**145** Are there external network connections (Internet, extranet, etc.)?

☐ YES ☐ NO ☐ IDK ☐ N/A

**146** Security and hardening standards for network devices, including Firewalls, Switches, Routers and Wireless Access Points (baseline configuration, patching, passwords, access control)?

☐ YES ☐ NO ☐ IDK ☐ N/A

**147** Are firewalls used to isolate critical and sensitive systems into network segments separate from network segments with less sensitive systems?

☐ YES ☐ NO ☐ IDK ☐ N/A

**148** Is there a process that requires security approval to allow external networks to connect to the company network, and enforces the least privilege necessary?

☐ YES ☐ NO ☐ IDK ☐ N/A

**149** Are all available high-risk security patches applied and verified at least monthly?

☐ YES ☐ NO ☐ IDK ☐ N/A

**150** Are Intrusion Detection/Prevention Systems employed in all sensitive network zones and wherever firewalls are enabled?

☐ YES ☐ NO ☐ IDK ☐ N/A

**151** Are wireless networking devices connected to networks containing scoped systems and data?

☐ YES ☐ NO ☐ IDK ☐ N/A

**152** Are there controls to prevent one client attempting to compromise another client in a resource pooled environment?

☐ YES ☐ NO ☐ IDK ☐ N/A

## P. Privacy

### QUESTION / REQUIREMENT

YES NO IDK N/A ADDITIONAL NOTES

**153** Is Scoped Data transmitted, processed, or stored that can be classified as non-public information (NPI), personally identifiable information (PII), or sensitive customer financial information? If yes, describe and list types of data.

☐ YES ☐ NO ☐ IDK ☐ N/A

**154** Do agreements with third parties who have access or potential access to Scoped Data, address confidentiality, audit, security, and privacy, including but not limited to incident response, ongoing monitoring, data sharing and secure disposal of Scoped Data?

☐ ☐ ☐ ☐


**155** Is a business associate contract in place to address obligations for the privacy and security requirements for the services provided?

☐ ☐ ☐ ☐


**156** For Scoped Data, is personal information about individuals transmitted to or received from countries outside the United States? If yes, list the countries.

☐ ☐ ☐ ☐


**157** Is personal information transmitted, processed, stored, or disclosed to or retained by third parties? If yes, describe.

☐ ☐ ☐ ☐


**158** Are there contractual controls to ensure that personal information transmitted, processed, stored or disclosed to or retained by third parties is limited to defined parameters for access, use and disclosure? If yes, describe. If no, explain reason.

☐ ☐ ☐ ☐


**159** Is personal information accessed, disclosed, processed, transmitted or retained with third parties outside the US? If yes, describe and list the countries.

☐ ☐ ☐ ☐


**160** Is there a documented privacy policy or procedures for the protection of information transmitted, processed, or maintained on behalf of the client?

☐ ☐ ☐ ☐


**161** Are transactions for covered accounts accessed, modified, or processed, including address changes and discrepancies? If yes, describe.

☐ ☐ ☐ ☐


## T. Threat Management

QUESTION / REQUIREMENT

YES NO IDK N/A ADDITIONAL NOTES

**162** Is there an anti-malware policy or program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?

☐ ☐ ☐ ☐


**163** Prohibition of disabling anti-malware with exceptions requiring Security approval and reenabling as soon as possible.

☐ ☐ ☐ ☐

|            |                                                                                                                                                                                               |                          |                          |                          |                          |  |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--|
| <b>164</b> | Is there a vulnerability management policy or program that has been approved by management, communicated to appropriate constituents and an owner assigned to maintain and review the policy? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>165</b> | Are vulnerability scans performed on all internet-facing applications at least monthly and after significant changes?                                                                         | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>166</b> | Are vulnerability scans performed against internal networks and systems?                                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>167</b> | Are penetration tests performed?                                                                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |
| <b>168</b> | Are there processes to manage threat and vulnerability assessment tools and the data they collect?                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |  |

## U. Server Security

| QUESTION / REQUIREMENT                                                                            | YES                      | NO                       | IDK                      | N/A                      | ADDITIONAL NOTES |
|---------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------------|
| <b>169</b> Are Servers used for transmitting, processing or storing Scoped Data?                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| <b>170</b> Are systems and applications patched?                                                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| <b>171</b> Are default hardened base virtual images applied to virtualized operating systems?     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |
| <b>172</b> Are Hypervisors used to manage systems used to transmit, process or store Scoped Data? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                  |