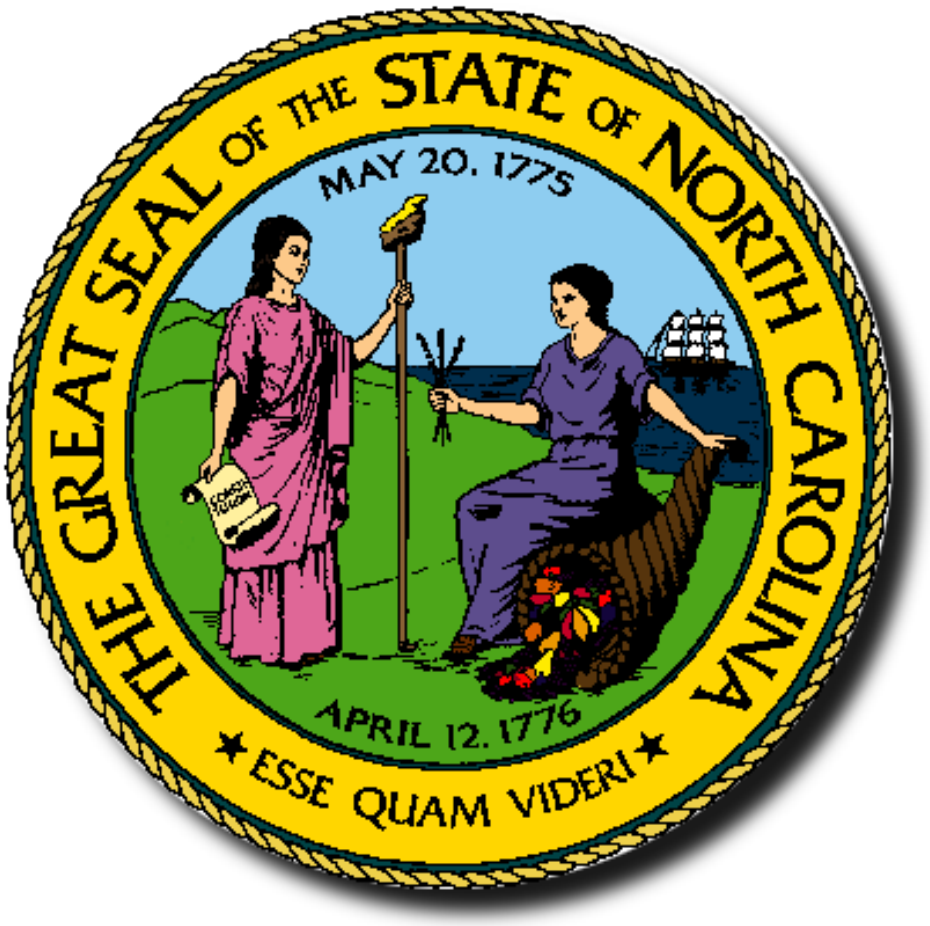
Enterprise Security and Risk Management Office
*Risk Management Services*




# Risk Assessment Questionnaire

March 22, 2011
Revision 1.5

# Risk Assessment Questionnaire

# Risk Assessment Questionnaire

| | | | |
|---|---|---|---|
| Initial Release Date: | March 31, 2004 | Version: | 1.0 |
| Date of Last Review: | March 22, 2011 | Version: | 1.5 |
| Date Retired: | | | |
| Architecture Interdependencies: | | | |
| Reviewer Notes: 01/09/2006 - Added question 20 in Phase I.<br>03/09/2007 – Updated Office name and added checklist.<br>12/11/2009 – Scheduled review, minor updates.<br>03/22/2011 – Scheduled review, minor updates. | | | |

**Risk Assessment Questionnaire**

# Introduction

The Risk Assessment Questionnaire compliments the Risk Management Guide. Questions consider risk categories pertinent to government and are presented in both individual and multi-component formats. It is expected that responses be provided in a team environment and where a facilitator will collect and report results. The questionnaire is considered confidential when complete per G.S. § 132-6.1(c).

The pre-risk assessment form must be completed prior to starting the risk assessment process. See Appendix B in the Risk Management Guide.

Completion of a Risk Assessment utilizing this questionnaire can be used in support of State law G.S. § 147-33.89 Business Continuity Planning and statewide security policy Information Technology Risk Management Policy with Guidelines.

# Risk Assessment Checklist

## Collect the following information

Completed pre-risk assessment form:_____

Requester:_____

Technical contact:_____

Agency:_____

Division:_____

Application/Business Process being assessed:_____

Level of exposure: _____
(Agency, Department, Division, ITS Internal, Multiple Agencies, Organizations or State)

Risk Assessment Facilitator:_____

Participants:_____

Comments:_____

_____

_____

**Risk Assessment Questionnaire**

## Phase I Questions

Q1. Would the failure to provide the automated business service result in significant health and safety concerns for the citizens of NC?
A1. Yes
A2. No

Q2. What number of citizens would this business failure impact?
A1. Significant impact on large number
A2. Small number of citizens affected
A3. No impact likely on any citizens

Q3. Would the consequences to the citizens be catastrophic?
A1. Yes
A2. No

Q4. Are there legal, regulatory, or policy requirements relative to delivery of your automated services?
A1. Yes
A2. No

Q4a. If yes, are they implemented?
A1. Yes
A2. No
A3. N/A

Q5. Can you demonstrate compliance with applicable standards, legal and regulatory requirements?
A1. Yes
A2. No
A3. N/A

Q6. If applicable, are there negative consequences for non-compliance to legal and regulatory requirements?
A1. Yes
A2. No
A3. N/A

Q7. If there were an IT failure when providing the business service, would this have an adverse impact to the reputation of the organization?
A1. Yes
A2. No

Q8. Which of the following is the most likely threat to occur in your agency resulting in an IT disruption?
A1) Technological < 4 hours
A2) Technological generally > 4 hours & < 24 hours downtime
A3) Technological > 24 hours downtime
A4) Man-made < 4 hours
A5) Man-made generally > 4 hours & < 24 hours downtime
A6) Man-made > 24 hours downtime
A7) Natural < 4 hours
A8) Natural > 4 hours & < 24 hours downtime
A9) Natural > 24 hours downtime

Q9. What is the frequency of technological, man-made or natural events causing a downtime > 24 hours?
A1) Occurrence between 1 and 30 days
A2) Occurrence between 31 and 365 days
A3) Occurrence greater than 365 days

Q10. Does your IT planning process adequately include operational resources to support the automated line of business?
A1) Yes
A2) No

Q11. Are operational resources adequate to deliver this essential service?
A1) Yes
A2) No

Q12. Who would be considered directly responsible and accountable if elements within the automated system failed?
A1) Elected or appointed official
A2) Agency Department Head
A3) Line of Business Owner
A4) State Employed IT Staff
A5) Vendor IT Staff

Q13. Have steps been taken to protect your agency's automated resources as it relates to physical security (building access, terrorism)?
A1) Yes
A2) No

Q14. Have steps been taken to protect your agency's automated resources as it relates to physical IT security (data center access, server access, need to know)?
A1) Yes
A2) No

Q15. Do you have a documented communication procedure where affected parties are notified of the requirements (objectives and strategies, new deployments, change management) to deliver the business service?
A1) Yes
A2) No

Q16. Have the elements of the IT infrastructure that supports the line of business including interdependencies been identified, documented and communicated?
A1. Yes
A2. No

Q17. Has a secure infrastructure (passwords, PCs, firewall, network, policies, procedures, hardware, software, etc.) to protect the information assets (data integrity, confidentiality, availability) been developed, implemented and communicated?
A1. Yes
A2. No

Q18. Have you developed backup strategies for continuity of automated services should you have an IT failure?
A1. Yes
A2. No

Q19. Is the automated system you are performing this risk assessment on considered critical or vital to your line of business?
A1. Yes
A2. No
A3. N/A

Q20. Has the application(s) currently being assessed been incorporated into the agency's Business Continuity Plan?
A1. Yes
A2. No
A3. N/A

## Phase II Questions

Q1. Would there be a delay in delivery of services in the event of an IT failure that resulted in missed deliverables, deadlines or reporting requirements?
A. Yes
B. No

Q2. If an IT failure resulted in a newsworthy event, how widespread would it be communicated?
A1. Local
A2. Regional
A3. Statewide
A4. National

Q3. As viewed by our citizens or customers, what would be the potential negative impact to the Agency's image as a result of an IT failure?
A1. No impact
A2. Minor
A3. Moderate
A4. Severe

Q4. For resources that support the automated systems:

1) Are resources provided documented roles and responsibilities?
2) Are they adequately trained?
3) Is staff turnover or unexpected loss considered and planned for?
4) Is system coverage adequately maintained?
5) Do you have adequate funding to fill the supporting roles?

*(Answer each question)*
A1. Yes
A2. Somewhat
A3. No

Q5. Does your line of business require SLAs or MOUs/MOAs with clients?
A1. Yes
A2. No

Q6. If yes, are you in full compliance with the stated deliverables in the SLAs & MOUs/MOAs?
A1. Yes
A2. No
A3. N/A

Q7. If no, what are the financial or legal repercussions for not meeting the SLAs, MOUs/MOAs?
A1. Not significant
A2. Somewhat significant
A3. Very significant
A4. N/A

Q8. What is the potential financial exposure to the agency should the automated system fail during service delivery?
A1. Not significant
A2. Somewhat significant
A3. Very significant

Q9. Where applicable, have the following controls been considered:

1) Homeland Security Advisory System?
2) Visitor and employee identification measures for building access and control?
3) Building evacuation procedures / signs been posted throughout the building?
4) Fire alarm system?
5) Appropriate fire suppression system?
6) Electrical power backup?
7) Temperature/Humidity?
8) Maintenance and testing of the above items 2 – 7?
9) Physical location, security measures, visibility profile?
10) Personnel safety?
11) Appropriate storage and retention of hardcopy material?

*(Answer each question)*

A1. Yes
A2. No
A3. N/A

Q10. Do you know what to do and whom you would contact for the following events: fire, accident, and inappropriate physical access?

A1. Yes
A2. No

Q11. Do agency inter-dependencies supporting the IT infrastructure operate seamlessly in the delivery of service to the citizens and/or customers? (Ex. change control, end-to-end processing, customer support, cross teaming, etc.)

A1. Yes
A2. Somewhat
A3. No

Q12. Do you have a process to communicate new policies and procedures to your staff and provide education, if necessary?

A1. Yes
A2. No

Q13. Has appropriate focus been placed on the functional end-to-end process for the entire system: how the application components are deployed, communicated, secured or otherwise interact with both the user and server components?

A1. Yes
A2. No
A3. N/A

# Risk Assessment Questionnaire

Q14. For your application:

1) Has the flow of transactions with procedures been documented (flow diagram)?
2) Has testing been performed on the application system controls?
3) Is input entering the system complete, accurate and authorized?
4) Is processing occurring within the application accurate?
5) Is the output produced complete and properly translated/interfaced with other applicable systems?
6) Is consideration given to end-user documentation and usability throughout the life cycle of the application?
7) Have the security requirements to support the application been determined?
8) Does it qualify for ongoing application and/or vendor support?
9) Are capacity planning & management, as well as redundancy incorporated?

*(Answer each question)*

A1. Yes
A2. Somewhat
A3. No

Q15. Do all applications and/or software have current licenses?
A1. Yes
A2. No

Q16. Where applicable, have the applications and/or software been approved by review designees such as Desktop Support, etc.?
A1. Yes
A2. No
A3. N/A

Q17. Are controls in place to disclose vulnerabilities in software (commercial or in-house developed)?
A1. Yes
A2. No
A3. N/A

Q18. How much down time can your line of business afford in the event of a disaster?
A1. Less than 1 hour
A2. > 1 hour but < 24 hours
A3. > 24 hours but < 48 hours
A4. > 48 hours but < 72 hours
A5. > 72 hours

Q19. Are any data associated with the application / process considered confidential per statute or other regulation?
A1. Yes
A2. No
A3. N/A

Q19a. If yes, are the data treated accordingly?
A1. Yes
A2. No
A3. N/A

Q20. Are all production servers, applications or supporting software physically located in the data center?
A1. Yes
A2. No

Q21.With regards to business continuity planning (BCP), have you:

1) Documented the critical automated systems that support the business functions?
2) Developed recovery strategies and integrated them into a business continuity plan?
3) Reviewed and tested the BCP plan within the last 12 months?
4) Updated the BCP plan as necessary?
5) Arranged for offsite disaster recovery?

*(Answer each question)*

A1. Yes
A2. No
A3. N/A

Q22. Have you been briefed on or aware of any security concerns with this automated system?

A1. Yes
A2. No

Q23.Where applicable, have the following protection measures been put in place to protect personal and/or confidential information on computers in your area:

1) Install and maintain a firewall to protect data?
2) Require all systems connected to your network to be configured in accordance with applicable Security Standards?
3) Monitor OS levels and security patches and keep them up to date?
4) Protect stored and transmitted data using encryption?
5) Use and regularly update anti virus software at gateways and on personal computers?
6) Restrict access by need to know?
7) Assign unique ID to each person with computer access and track all access to data by unique ID?
8) Is authentication, based on industry best practices, performed?
9) Are separation of duties documented for your area of responsibility?
10) Have you documented an aggregate separation of duties for all people with access to your applications?
11) Do all key roles have a designated backup?
12) All system administrators have adequate security skills?
13) Restrict physical access to data to those with a need to know?
14) Implement and enforce an information security policy?

*(Answer each question)*

A1.Yes
A2. No
A3. N/A

Q24. Have you installed and do you maintain an Intrusion Detection System/Intrusion Prevention System (IDS/IPS) for your network and/or systems?

A1. Yes
A2. No
A3. N/A

Q25. Have you employed vulnerability testing/scanning on an ongoing basis for your IT Infrastructure, and client side security testing that would identify the potential failure points that could compromise the system and data integrity?

A1. Yes
A2. No
A3. N/A

**Risk Assessment Questionnaire**

## Phase III

**Note:** Phase I & II must be completed prior to starting Phase III. All fields are required in this section.

**Purpose**: Appropriate levels of managers and staff perform a gap analysis that focuses on risk mitigation. They will further analyze and identify the differences, effects, and methods required for reducing risk between required capabilities and those that actually exist.

### Risk Analysis Results & Mitigation Plans

**Risk assessment number:**
**Risk status:**
**Risk level:**
**Application / Business process being assessed:**

**Owner Detail**
Owner/Manager:
Department:
Organization:
Location:

**Detailed description of gap analysis:**

**Based on your experience, what is the probability of this risk or risks occurring? (Low, Moderate, High)**

**Detail the impact to the Line of Business:**

**Detail the permanent solution to eliminate or effectively reduce the risk to an acceptable level:**
(Action to be taken within next 12 months)

**Length of time needed to correct or reduce the risk to an acceptable level:**
(Cannot exceed 12 months**)**

## Risk Assessment Questionnaire

**What will it cost to eliminate or effectively reduce the risk to an acceptable level?**
(In US Dollars) $

**Detail interim controls to reduce or mitigate the risk:**
(Include dates, tasks)

**Are the interim controls currently in place?**
(Yes or No and optional comments)

**Supporting documentation:**
(Attach .doc files here)

**Comments:**

**Responsible parties for execution of actions to eliminate/reduce the risk and to perform the interim controls:**

1st Reviewer:
2nd Reviewer:
3rd Reviewer:
4th Reviewer:
5th Reviewer:
6th Reviewer:
7th Reviewer:
8th Reviewer:

**This assessment has been received and reviewed by:**
(Reviewer signatures and optional comments)

**Assessment completion date:**

Reminder: Update your Business Continuity Plan to reflect your risk analysis & mitigation plan.

**Risk Assessment Questionnaire**

# Scoring Key

## Phase I Questions

Q1. Would the failure to provide the automated business service result in significant health and safety concerns for the citizens of NC?
A1. Yes *(High)*
A2. No *(Low)*

Q2. What number of citizens would this business failure impact?
A1. Significant impact on large number *(High)*
A2. Small number of citizens affected *(Moderate)*
A3. No impact likely on any citizens *(Low)*

Q3. Would the consequences to the citizens be catastrophic?
A1. Yes *(High)*
A2. No *(Low)*

Q4. Are there legal, regulatory, or policy requirements relative to delivery of your automated services?
A1. Yes *(Low)*
A2. No *(Low)*

Q4a.If yes, are they implemented?
A1. Yes *(Low)*
A2. No *(High)*
A3. N/A *(Low)*

Q5. Can you demonstrate compliance with applicable standards, legal and regulatory requirements?
A1. Yes *(Low)*
A2. No *(High)*
A3. N/A *(Low)*

Q6. If applicable, are there negative consequences for non-compliance to legal and regulatory requirements?
A1. Yes *(High)*
A2. No *(Low)*
A3. N/A *(Low)*

Q7. If there were an IT failure when providing the business service, would this have an adverse impact to the reputation of the organization?
A1. Yes *(High)*
A2. No *(Low)*

Q8. Which of the following is the most likely threat to occur in your agency resulting in an IT disruption?
A1) Technological < 4 hours *(Low)*
A2) Technological generally > 4 hours & < 24 hours downtime *(Moderate)*
A3) Technological > 24 hours downtime *(High)*
A4) Man-made < 4 hours *(Low)*
A5) Man-made generally > 4 hours & < 24 hours downtime *(Moderate)*
A6) Man-made > 24 hours downtime *(High)*
A7) Natural < 4 hours *(Low)*
A8) Natural > 4 hours & < 24 hours downtime *(Moderate)*

**Risk Assessment Questionnaire**

A9) Natural > 24 hours downtime *(High)*

Q9. What is the frequency of technological, man-made or natural events causing a downtime > 24 hours?
A1) Occurrence between 1 and 30 days *(High)*
A2) Occurrence between 31 and 365 days *(Moderate)*
A3) Occurrence greater than 365 days *(Low)*

Q10. Does your IT planning process adequately include operational resources to support the automated line of business?
A1) Yes *(Low)*
A2) No *(Moderate)*

Q11. Are operational resources adequate to deliver this essential service?
A1) Yes *(Low)*
A2) No *(Moderate)*

Q12. Who would be considered directly responsible and accountable if elements within the automated system failed?
A1) Elected or appointed official *(High)*
A2) Agency Department Head *(High)*
A3) Business Owner *(High)*
A4) State Employed IT Staff *(Low)*
A5) Vendor IT Staff *(Low)*

Q13. Have steps been taken to protect your agency's automated resources as it relates to physical security (building access, terrorism)?
A1) Yes *(Low)*
A2) No *(High)*

Q14. Have steps been taken to protect your agency's automated resources as it relates to physical IT security (data center access, server access, need to know)?
A1) Yes *(Low)*
A2) No *(High)*

Q15. Do you have a documented communication procedure where affected parties are notified of the requirements (objectives and strategies, new deployments, change management) to deliver the business service?
A1) Yes *(Low)*
A2) No *(Moderate)*

Q16. Have the elements of the IT infrastructure that supports the line of business including interdependencies been identified, documented and communicated?
A1. Yes *(Low)*
A2. No *(Moderate)*

Q17. Has a secure infrastructure (passwords, PCs, firewall, network, policies, procedures, hardware, software, etc.) to protect the information assets (data integrity, confidentiality, availability) been developed, implemented and communicated?
A1. Yes *(Low)*
A2. No *(Moderate)*

Q18. Have you developed backup strategies for continuity of automated services should you have an IT failure?

| | |
|---|---|
| A1. Yes | *(Low)* |
| A2. No | *(Moderate)* |

Q19. Is the automated system you are performing this risk assessment on considered critical or vital to your line of business?

| | |
|---|---|
| A1. Yes | *(Low)* |
| A2. No | *(Low)* |
| A3. N/A | *(Low)* |

Q20. Has the application(s) currently being assessed been incorporated into the agency's Business Continuity Plan?

| | |
|---|---|
| A1. Yes | *(Low)* |
| A2. No | *(Moderate)* |
| A3. N/A | *(Low)* |

## Phase I Scoring Weight:

If any question is answered as 'moderate' or 'high' this requires the assessment to proceed with Phase II.
If one or more questions is answered as 'high', phase I = 'high'.
If five or more questions are answered as 'moderate', phase I = 'high'.
If one to four questions are answered as 'moderate', phase I = 'moderate'.
If all questions are answered as 'low', phase I = 'low'.

If Risk Level = **Low**
You have completed the questionnaire for Phase I and your risk level is '**low**'. You do not need to proceed further unless you desire to complete Phase II. Thank you.

If Risk Level = **Moderate**
You have completed the questionnaire for Phase I and your risk level is '**moderate**'. Please proceed to Phase II. Thank you.

If Risk Level = **High**
You have completed the questionnaire for Phase I and your risk level is '**high**'. Please proceed to Phase II. Thank you.

## Phase II Questions

Q1. Would there be a delay in delivery of services in the event of an IT failure that resulted in missed deliverables, deadlines or reporting requirements?

| | |
|---|---|
| A. Yes | *(Moderate* |
| B. No | *(Low)* |

Q2. If an IT failure resulted in a newsworthy event, how widespread would it be communicated?

| | |
|---|---|
| A1. Local | *(Low)* |
| A2. Regional | *(Moderate)* |
| A3. Statewide | *(High)* |
| A4. National | *(High)* |

Q3. As viewed by our citizens or customers, what would be the potential negative impact to the Agency's image as a result of an IT failure?

| | |
|---|---|
| A1. No impact | *(Low)* |
| A2. Minor | *(Low)* |
| A3. Moderate | *(Moderate)* |
| A4. Severe | *(High)* |

(If this is the only question answered as 'moderate' or 'high', do not proceed to phase III.)

Q4. For resources that support the automated systems:

6) Are resources provided documented roles and responsibilities?
7) Are they adequately trained?
8) Is staff turnover or unexpected loss considered and planned for?
9) Is system coverage adequately maintained?
10) Do you have adequate funding to fill the supporting roles?

*(Answer each question)*

| | |
|---|---|
| A1. Yes | *(Low)* |
| A2. Somewhat | *(Moderate)* |
| A3. No | *(High)* |

Q5. Does your line of business require SLAs or MOUs/MOAs with clients?

| | |
|---|---|
| A1. Yes | *(Low)* |
| A2. No | *(Low)* |

Q6. If yes, are you in full compliance with the stated deliverables in the SLAs & MOUs/MOAs?

| | |
|---|---|
| A1. Yes | *(Low)* |
| A2. No | *(Moderate)* |
| A3. N/A | *(Low)* |

Q7. If no, what are the financial or legal repercussions for not meeting the SLAs, MOUs/MOAs?

| | |
|---|---|
| A1. Not significant | *(Low)* |
| A2. Somewhat significant | *(Moderate)* |
| A3. Very significant | *(High)* |
| A4. N/A | *(Low)* |

Q8. What is the potential financial exposure to the agency should the automated system fail during service delivery?

| | |
|---|---|
| A1. Not significant | *(Low)* |
| A2. Somewhat significant | *(Moderate)* |

| | |
|---|---|
| A3. Very significant | *(High)* |

## Risk Assessment Questionnaire

Q9. Where applicable, have the following controls been considered:

12) Homeland Security Advisory System?
13) Visitor and employee identification measures for building access and control?
14) Building evacuation procedures / signs been posted throughout the building?
15) Fire alarm system?
16) Appropriate fire suppression system?
17) Electrical power backup?
18) Temperature/Humidity?
19) Maintenance and testing of the above items 2 – 7?
20) Physical location, security measures, visibility profile?
21) Personnel safety?
22) Appropriate storage and retention of hardcopy material?

*(Answer each question)*

A1. Yes *(Low)*
A2. No *(Moderate)*
A3. N/A *(Low)*

Q10. Do you know what to do and whom you would contact for the following events: fire, accident, and inappropriate physical access?

A1. Yes *(Low)*
A2. No *(Moderate)*

Q11. Do agency inter-dependencies supporting the IT infrastructure operate seamlessly in the delivery of service to the citizens and/or customers? (Ex. change control, end-to-end processing, customer support, cross teaming, etc.)

A1. Yes *(Low)*
A2. Somewhat *(Moderate)*
A3. No *(High)*

Q12. Do you have a process to communicate new policies and procedures to your staff and provide education, if necessary?

A1. Yes *(Low)*
A2. No *(Moderate)*

Q13. Has appropriate focus been placed on the functional end-to-end process for the entire system: how the application components are deployed, communicated, secured or otherwise interact with both the user and server components?

A1. Yes *(Low)*
A2. No *(High)*
A3. N/A *(Low)*

## Risk Assessment Questionnaire

Q14. For your application:

10) Has the flow of transactions with procedures been documented (flow diagram)?
11) Has testing been performed on the application system controls?
12) Is input entering the system complete, accurate and authorized?
13) Is processing occurring within the application accurate?
14) Is the output produced complete and properly translated/interfaced with other applicable systems?
15) Is consideration given to end-user documentation and usability throughout the life cycle of the application?
16) Have the security requirements to support the application been determined?
17) Does it qualify for ongoing vendor support?
18) Are capacity planning & management, as well as redundancy incorporated?

*(Answer each question)*

| | |
|---|---|
| A1. Yes | *(Low)* |
| A2. Somewhat | *(Moderate)* |
| A3. No | *(High)* |

Q15. Do all applications and/or software have current licenses?

| | |
|---|---|
| A1. Yes | *(Low)* |
| A2. No | *(Moderate)* |

Q16. Where applicable, have the applications and/or software been approved by review designees such as Desktop Support, etc.?

| | |
|---|---|
| A1. Yes | *(Low)* |
| A2. No | *(Moderate)* |
| A3. N/A | *(Low)* |

Q17. Are controls in place to disclose vulnerabilities in software (commercial or in-house developed)?

| | |
|---|---|
| A1. Yes | *(Low)* |
| A2. No | *(High)* |
| A3. N/A | *(Low)* |

Q18. How much down time can your line of business afford in the event of a disaster?

| | |
|---|---|
| A1. Less than 1 hour | *(High)* |
| A2. > 1 hour but < 24 hours | *(High)* |
| A3. > 24 hours but < 48 hours | *(Moderate)* |
| A4. > 48 hours but < 72 hours | *(Moderate)* |
| A5. > 72 hours | *(Low)* |

Q19. Are any data associated with the application / process considered confidential per statute or other regulation?

| | |
|---|---|
| A1. Yes | *(Low)* |
| A2. No | *(Low)* |
| A3. N/A | *(Low)* |

Q19a. If yes, are the data treated accordingly?

| | |
|---|---|
| A1. Yes | *(Low)* |
| A2. No | *(High)* |
| A3. N/A | *(Low)* |

Q20. Are all production servers, applications or supporting software physically located in the data center?

| | |
|---|---|
| A1. Yes | *(Low)* |
| A2. No | *(High)* |

Q21.With regards to business continuity planning (BCP), have you:

6) Documented the critical automated systems that support the business functions?
7) Developed recovery strategies and integrated them into a business continuity plan?
8) Reviewed and tested the BCP plan within the last 12 months?
9) Updated the BCP plan as necessary?
10) Arranged for offsite disaster recovery?

*(Answer each question)*

A1. Yes *(Low)*
A2. No *(Moderate)*

Q22. Have you been briefed on or aware of any security concerns with this automated system?

A1. Yes *(Moderate)*
A2. No *(Low)*

Q23.Where applicable, have the following protection measures been put in place to protect personal and/or confidential information on computers in your area:

15) Install and maintain a firewall to protect data?
16) Require all systems connected to your network to be configured in accordance with applicable Security Standards?
17) Monitor OS levels and security patches and keep them up to date?
18) Protect stored and transmitted data using encryption?
19) Use and regularly update ant virus software at gateways and on personal computers?
20) Restrict access by need to know?
21) Assign unique ID to each person with computer access and track all access to data by unique ID?
22) Is authentication, based on industry best practices, performed?
23) Are separation of duties documented for your area of responsibility?
24) Have you documented an aggregate separation of duties for all people with access to your applications?
25) Do all key roles have a designated backup?
26) All system administrators have adequate security skills?
27) Restrict physical access to data to those with a need to know?
28) Implement and enforce an information security policy?

*(Answer each question)*

A1.Yes *(Low)*
A2. No *(Moderate= 4,8, 9,14 / High = 1, 2, 3, 5,6, 7, 10, 11, 12,13)*
A3. N/A *(Low)*

Q24. Have you installed and do you maintain an Intrusion Detection System/Intrusion Prevention System (IDS/IPS) for your network and/or systems?

A1. Yes *(Low)*
A2. No *(Moderate)*
A3. N/A *(Low)*

Q25. Have you employed vulnerability testing/scanning on an ongoing basis for your IT Infrastructure, and client side security testing that would identify the potential failure points that could compromise the system and data integrity?

A1. Yes *(Low)*
A2. No *(High)*
A3. N/A *(Low)*

## Phase II  Scoring Weight:

If any question is answered as 'moderate' or 'high' this requires the assessment to proceed with Phase III, with the exception of question 3.
If one or more questions is answered as 'high', phase II = 'high'.
If twenty or more questions are answered as 'moderate', phase II = 'high'.
If one to nineteen questions are answered as 'moderate', phase II = 'moderate'.
If all questions are answered as 'low', phase II = 'low', and assessment can end.

If Risk Level = **Low**
You have completed the questionnaire for Phase II and your risk level is '**low**'.  You do not need to proceed further unless you desire to complete Phase III.  Thank you.

If Risk Level = **Moderate**
You have completed the questionnaire for Phase II and your risk level is '**moderate**'.  Please proceed to Phase III.  Thank you.

If Risk Level = **High**
You have completed the questionnaire for Phase II and your risk level is '**high**'.  Please proceed to Phase III.  Thank you.

~End of document~