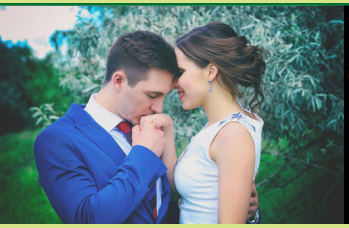
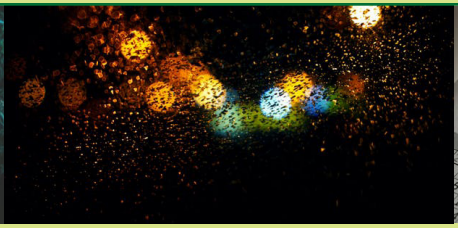
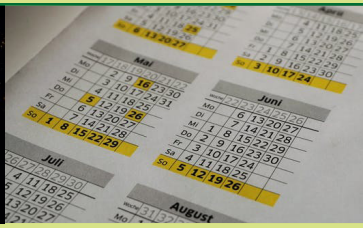
Information Security Management

COMPLETE SELF-ASSESSMENT GUIDE

PRACTICAL TOOLS FOR SELF-ASSESSMENT

Diagnose projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices

Implement evidence-based best practice strategies aligned with overall goals

Integrate recent advances and process design strategies into practice according to best practice guidelines

Use the Self-Assessment tool Scorecard and develop a clear picture of which areas need attention

The Art of Service

Information Security Management Complete Self-Assessment Guide

The guidance in this Self-Assessment is based on Information Security Management best practices and standards in business process architecture, design and quality management. The guidance is also based on the professional judgment of the individual collaborators listed in the Acknowledgments.

Table of Contents

About The Art of Service

The Art of Service, Business Process Architects since 2000, is dedicated to helping business achieve excellence.

Defining, designing, creating, and implementing a process to solve a business challenge or meet a business objective is the most valuable role… In EVERY company, organization and department.

Unless you're talking a one-time, single-use project within a business, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions.

Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?'

With The Art of Service's Business Process Architect Self-Assessments, Research, Toolkits, Education and Certifications we empower people who can do just that — whether their title is marketer, entrepreneur, manager, salesperson, consultant, Business Process Manager, executive assistant, IT Manager, CIO etc... —they are the people who rule the future. They are people who watch the process as it happens, and ask the right questions to make the process work better.

Contact us when you need any support with this Self-Assessment and any help with templates, blue-prints and examples of standard documents you might need:

http://theartofservice.com
service@theartofservice.com

Acknowledgments

This checklist was developed under the auspices of The Art of Service, chaired by Gerardus Blokdyk.

Representatives from several client companies participated in the preparation of this Self-Assessment.

Our deepest gratitude goes out to Matt Champagne, Ph.D. Surveys Expert, for his invaluable help and advise in structuring the Self Assessment.

Mr Champagne can be contacted at
http://matthewchampagne.com/

In addition, we are thankful for the design and printing services provided.

Included Resources - how to access

Included with your purchase of the book is the Information Security Management Self-Assessment downloadable resource, which contains all questions and Self-Assessment areas of this book.

Get it now- you will be glad you did - do it now, before you forget.

How? Simply send an email to **access@theartofservice.com** with this books' title in the subject to get all the Information Security Management Self-Assessment questions in a ready to use Excel spreadsheet, containing the self-assessment, graphs, and project RACI planning - all with examples to get you started right away.

Your feedback is invaluable to us

If you recently bought this book, we would love to hear from you! You can do this by writing a review on amazon (or the online store where you purchased this book) about your last purchase! As part of our continual service improvement process, we love to hear real client experiences and feedback.

How does it work?
To post a review on Amazon, just log in to your account and click on the Create Your Own Review button (under Customer Reviews) of the relevant product page. You can find examples of product reviews in Amazon. If you purchased from another online store, simply follow their procedures.

What happens when I submit my review?
Once you have submitted your review, send us an email at review@theartofservice.com with the link to your review so we can properly thank you for your feedback.

Purpose of this Self-Assessment

This Self-Assessment has been developed to improve understanding of the requirements and elements of Information Security Management, based on best practices and standards in business process architecture, design and quality management.

It is designed to allow for a rapid Self-Assessment of an organization or facility to determine how closely existing management practices and procedures correspond to the elements of the Self-Assessment.

The criteria of requirements and elements of Information Security Management have been rephrased in the format of a Self-Assessment questionnaire, with a seven-criterion scoring system, as explained in this document.

In this format, even with limited background knowledge of

Information Security Management, a facility or other business manager can quickly review existing operations to determine how they measure up to the standards. This in turn can serve as the starting point of a 'gap analysis' to identify management tools or system elements that might usefully be implemented in the organization to help improve overall performance.

How to use the Self-Assessment

On the following pages are a series of questions to identify to what extent your Information Security Management initiative is complete in comparison to the requirements set in standards.

To facilitate answering the questions, there is a space in front of each question to enter a score on a scale of '1' to '5'.

1 Strongly Disagree

2 Disagree

3 Neutral

4 Agree

5 Strongly Agree

Read the question and rate it with the following in front of mind:

'In my belief,
the answer to this question is clearly defined'.

There are two ways in which you can choose to interpret this statement;

1. how aware are you that the answer to the question is clearly defined

2. for more in-depth analysis you can choose to gather evidence and confirm the answer to the question. This obviously will take more time, most Self-Assessment users opt for the first way to interpret the question and dig deeper later on based on the outcome of the overall Self-Assessment.

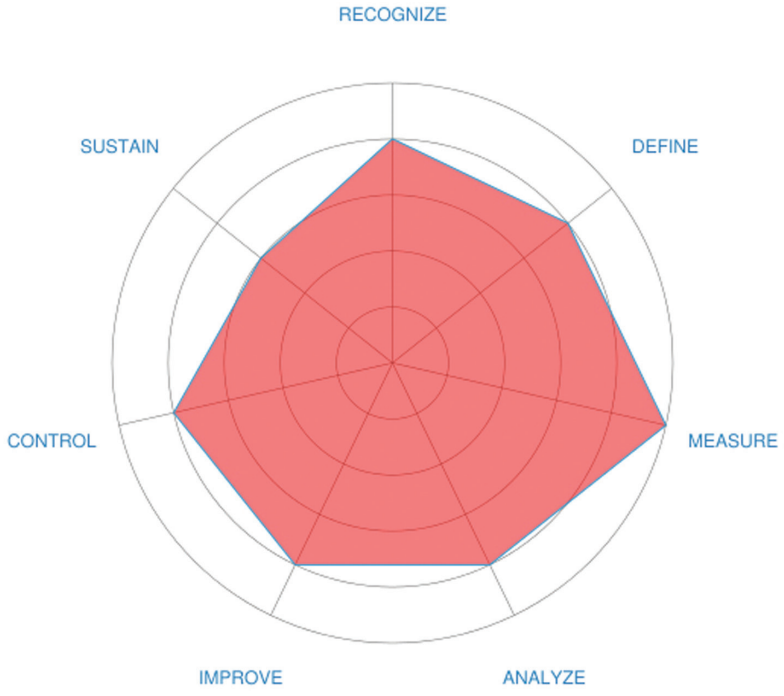
A score of '1' would mean that the answer is not clear at all, where a '5' would mean the answer is crystal clear and defined. Leave emtpy when the question is not applicable or you don't want to answer it, you can skip it without affecting your score. Write your score in the space provided.

After you have responded to all the appropriate statements in each section, compute your average score for that section, using the formula provided, and round to the nearest tenth. Then transfer to the corresponding spoke in the Information Security Management Scorecard on the second next page of the Self-Assessment.

Your completed Information Security Management Scorecard will give you a clear presentation of which Information Security Management areas need attention.

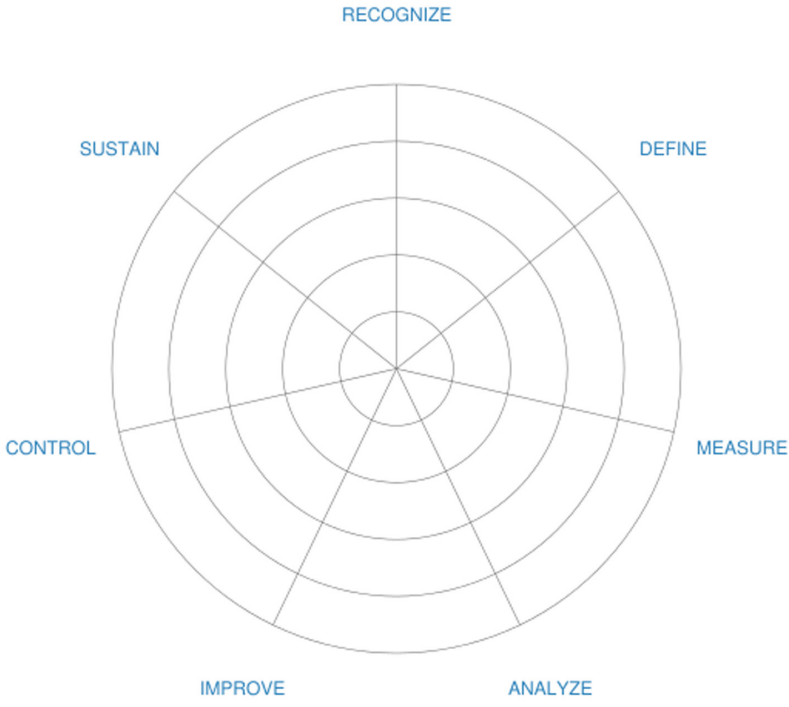
Information Security Management Scorecard Example

Example of how the finalized Scorecard can look like:



Information Security Management Scorecard

Your Scores:



BEGINNING OF THE SELF-ASSESSMENT:

SELF-ASSESSMENT SECTION START

CRITERION #1: RECOGNIZE

INTENT: Be aware of the need for change. Recognize that there is an unfavorable variation, problem or symptom.

In my belief, the answer to this question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. What was the problem?
<--- Score

2. What is the smallest subset of the problem we can usefully solve?
<--- Score

3. What information do users need?
<--- Score

4. How do you identify the information basis for later specification of performance or acceptance criteria?
<--- Score

5. What tools and technologies are needed for a custom Information Security Management project?
<--- Score

6. Has the organization identified authorizing officials for the information system and all common controls inherited by the system?
<--- Score

7. Will it solve real problems?
<--- Score

8. Has management issued a policy statement on information security?
<--- Score

9. Do we know what we need to know about this topic?
<--- Score

10. Would the average employee recognize a security issue?
<--- Score

11. How do you identify the kinds of information that you will need?
<--- Score

12. Are there any specific expectations or concerns

about the Information Security Management team, Information Security Management itself?
<--- Score

13. How do you assess your Information Security Management workforce capability and capacity needs, including skills, competencies, and staffing levels?
<--- Score

14. What else needs to be measured?
<--- Score

15. As a sponsor, customer or management, how important is it to meet goals, objectives?
<--- Score

16. Are there recognized Information Security Management problems?
<--- Score

17. Consider your own Information Security Management project. what types of organizational problems do you think might be causing or affecting your problem, based on the work done so far?
<--- Score

18. How does it fit into our organizational needs and tasks?
<--- Score

19. What does Information Security Management success mean to the stakeholders?
<--- Score

20. Does Information Security Management create potential expectations in other areas that need to be recognized and considered?
<--- Score

21. How are we going to measure success?
<--- Score

22. Has the organization established an Identity and Access Management program that is consistent with requirements, policy, and applicable guidelines and which identifies users and network devices?
<--- Score

23. Has the organization consulted information system owners when identifying common controls to ensure that the security capability provided by the inherited controls is sufficient to deliver adequate protection?
<--- Score

24. Who defines the rules in relation to any given issue?
<--- Score

25. What prevents me from making the changes I know will make me a more effective Information Security Management leader?
<--- Score

26. What are the expected benefits of Information Security Management to the business?
<--- Score

27. What vendors make products that address the

Information Security Management needs?
<--- Score

28. Who else hopes to benefit from it?
<--- Score

29. How much are sponsors, customers, partners, stakeholders involved in Information Security Management? In other words, what are the risks, if Information Security Management does not deliver successfully?
<--- Score

30. Would people recognise a security incident when they saw one?
<--- Score

31. What are the business objectives to be achieved with Information Security Management?
<--- Score

32. What situation(s) led to this Information Security Management Self Assessment?
<--- Score

33. Does our organization need more Information Security Management education?
<--- Score

34. Will Information Security Management deliverables need to be tested and, if so, by whom?
<--- Score

35. How are the Information Security Management's objectives aligned to the organization's overall business strategy?

<--- Score

36. Have you identified your Information Security Management key performance indicators?
<--- Score

37. What do we need to start doing?
<--- Score

38. What would happen if Information Security Management weren't done?
<--- Score

39. When a Information Security Management manager recognizes a problem, what options are available?
<--- Score

40. Are there Information Security Management problems defined?
<--- Score

41. What problems are you facing and how do you consider Information Security Management will circumvent those obstacles?
<--- Score

42. What training and capacity building actions are needed to implement proposed reforms?
<--- Score

43. How do we Identify specific Information Security Management investment and emerging trends?
<--- Score

44. Will new equipment/products be required to

facilitate Information Security Management delivery for example is new software needed?
<--- Score

45. Who needs to know about Information Security Management ?
<--- Score

46. Liability in the event sensitive information is compromised?
<--- Score

47. How is the board kept informed of information security issues?
<--- Score

48. How can auditing be a preventative security measure?
<--- Score

49. Is it clear when you think of the day ahead of you what activities and tasks you need to complete?
<--- Score

50. Think about the people you identified for your Information Security Management project and the project responsibilities you would assign to them. what kind of training do you think they would need to perform these responsibilities effectively?
<--- Score

51. What is the smallest subset of the problem we can usefully solve?
<--- Score

52. Are controls defined to recognize and contain problems?
<--- Score

53. For your Information Security Management project, identify and describe the business environment. is there more than one layer to the business environment?
<--- Score

54. Has the organization provided all of the essential supporting assessment-related materials needed by the assessor(s) to conduct an effective security control assessment?
<--- Score

55. Will a response program recognize when a crisis occurs and provide some level of response?
<--- Score

56. Can Management personnel recognize the monetary benefit of Information Security Management?
<--- Score

57. Why do we need to keep records?
<--- Score

58. What should be considered when identifying available resources, constraints, and deadlines?
<--- Score

59. What do I need to comply with?
<--- Score

Add up total points for this section:

_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Information Security Management Index at the beginning of the Self-Assessment.

SELF-ASSESSMENT SECTION START

CRITERION #2: DEFINE:

INTENT: Formulate the business problem. Define the problem, needs and objectives.

In my belief, the answer to this question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. Are security/privacy roles and responsibilities formally defined?
<--- Score

2. Is there a critical path to deliver Information Security Management results?
<--- Score

3. Are improvement team members fully trained on Information Security Management?

<--- Score

4. Is it clearly defined in and to your organization what you do?
<--- Score

5. How will variation in the actual durations of each activity be dealt with to ensure that the expected Information Security Management results are met?
<--- Score

6. What key business process output measure(s) does Information Security Management leverage and how?
<--- Score

7. Is Information Security Management Required?
<--- Score

8. Has the organization addressed minimum assurance requirements for the security controls employed within and inherited by the information system?
<--- Score

9. Are Required Metrics Defined?
<--- Score

10. How is the team tracking and documenting its work?
<--- Score

11. What are the dynamics of the communication plan?
<--- Score

12. Do we all define Information Security

Management in the same way?
<--- Score

13. Have specific policy objectives been defined?
<--- Score

14. What is the minimum educational requirement for potential new hires?
<--- Score

15. Has a project plan, Gantt chart, or similar been developed/completed?
<--- Score

16. Are roles and responsibilities formally defined?
<--- Score

17. Is the team adequately staffed with the desired cross-functionality? If not, what additional resources are available to the team?
<--- Score

18. Is data collected and displayed to better understand customer(s) critical needs and requirements.
<--- Score

19. Are accountability and ownership for Information Security Management clearly defined?
<--- Score

20. Will team members regularly document their Information Security Management work?
<--- Score

21. How can the value of Information Security

Management be defined?
<--- Score

22. Has anyone else (internal or external to the organization) attempted to solve this problem or a similar one before? If so, what knowledge can be leveraged from these previous efforts?
<--- Score

23. Are different versions of process maps needed to account for the different types of inputs?
<--- Score

24. Are business processes mapped?
<--- Score

25. Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with requirements, policy, and applicable guidelines?
<--- Score

26. Is the team sponsored by a champion or business leader?
<--- Score

27. What are the rough order estimates on cost savings/opportunities that Information Security Management brings?
<--- Score

28. Is the current 'as is' process being followed? If not, what are the discrepancies?
<--- Score

29. Do the problem and goal statements meet the

SMART criteria (specific, measurable, attainable, relevant, and time-bound)?
<--- Score

30. What customer feedback methods were used to solicit their input?
<--- Score

31. Is there a completed SIPOC representation, describing the Suppliers, Inputs, Process, Outputs, and Customers?
<--- Score

32. Are task requirements clearly defined?
<--- Score

33. Is full participation by members in regularly held team meetings guaranteed?
<--- Score

34. Have all of the relationships been defined properly?
<--- Score

35. When are meeting minutes sent out? Who is on the distribution list?
<--- Score

36. Who defines (or who defined) the rules and roles?
<--- Score

37. What constraints exist that might impact the team?
<--- Score

38. How often are the team meetings?

<--- Score

39. How do you keep key subject matter experts in the loop?
<--- Score

40. How will the Information Security Management team and the organization measure complete success of Information Security Management?
<--- Score

41. How and when will be baselines be defined?
<--- Score

42. Do the requirements that we've gathered and the models that demonstrate them constitute a full and accurate representation of what we want?
<--- Score

43. What Organizational Structure is Required?
<--- Score

44. Have all basic functions of Information Security Management been defined?
<--- Score

45. Scope of application?
<--- Score

46. Are customer(s) identified and segmented according to their different needs and requirements?
<--- Score

47. Has the direction changed at all during the course of Information Security Management? If so, when did it change and why?

<--- Score

48. Are there different segments of customers?
<--- Score

49. Are security roles and responsibilities clearly defined and communicated?
<--- Score

50. What would be the goal or target for a Information Security Management's improvement team?
<--- Score

51. Is there a completed, verified, and validated high-level 'as is' (not 'should be' or 'could be') business process map?
<--- Score

52. What are the boundaries of the scope? What is in bounds and what is not? What is the start point? What is the stop point?
<--- Score

53. In what way can we redefine the criteria of choice in our category in our favor, as Method introduced style and design to cleaning and Virgin America returned glamor to flying?
<--- Score

54. Is Information Security Management currently on schedule according to the plan?
<--- Score

55. What critical content must be communicated – who, what, when, where, and how?
<--- Score

56. What are the Roles and Responsibilities for each team member and its leadership? Where is this documented?
<--- Score

57. What sources do you use to gather information for a Information Security Management study?
<--- Score

58. Is the team equipped with available and reliable resources?
<--- Score

59. Has/have the customer(s) been identified?
<--- Score

60. How was the 'as is' process map developed, reviewed, verified and validated?
<--- Score

61. What are the compelling business reasons for embarking on Information Security Management?
<--- Score

62. When was the Information Security Management start date?
<--- Score

63. How do you define security?
<--- Score

64. Has the organization established a remote access program that is consistent with FISMA requirements, policy, and applicable NIST guidelines?

<--- Score

65. Are there any constraints known that bear on the ability to perform Information Security Management work? How is the team addressing them?
<--- Score

66. Will team members perform Information Security Management work when assigned and in a timely fashion?
<--- Score

67. How would one define Information Security Management leadership?
<--- Score

68. Has a high-level 'as is' process map been completed, verified and validated?
<--- Score

69. How does the Information Security Management manager ensure against scope creep?
<--- Score

70. Does the team have regular meetings?
<--- Score

71. Is the team formed and are team leaders (Coaches and Management Leads) assigned?
<--- Score

72. What baselines are required to be defined and managed?
<--- Score

73. Is Information Security Management linked to key

business goals and objectives?
<--- Score

74. Is there regularly 100% attendance at the team meetings? If not, have appointed substitutes attended to preserve cross-functionality and full representation?
<--- Score

75. Has a team charter been developed and communicated?
<--- Score

76. Has the Information Security Management work been fairly and/or equitably divided and delegated among team members who are qualified and capable to perform the work? Has everyone contributed?
<--- Score

77. Is the Information Security Management scope manageable?
<--- Score

78. Does Information Security Management include applications and information with regulatory compliance significance (or other contractual conditions that must be formally complied with) in a new or unique manner for which no approved security requirements, templates or design models exist?
<--- Score

79. Is the scope of Information Security Management defined?
<--- Score

80. When is the estimated completion date?
<--- Score

81. Are customers identified and high impact areas defined?
<--- Score

82. What tools and roadmaps did you use for getting through the Define phase?
<--- Score

83. Define ISMS scope what businesses, business units, departments and/or systems are going to be covered by your Information Security Management System?
<--- Score

84. Is a fully trained team formed, supported, and committed to work on the Information Security Management improvements?
<--- Score

85. If substitutes have been appointed, have they been briefed on the Information Security Management goals and received regular communications as to the progress to date?
<--- Score

86. What defines Best in Class?
<--- Score

87. Has everyone on the team, including the team leaders, been properly trained?
<--- Score

88. How would you define the culture here?

<--- Score

89. Are team charters developed?
<--- Score

90. Has the improvement team collected the 'voice of the customer' (obtained feedback – qualitative and quantitative)?
<--- Score

91. What specifically is the problem? Where does it occur? When does it occur? What is its extent?
<--- Score

92. Is there a Information Security Management management charter, including business case, problem and goal statements, scope, milestones, roles and responsibilities, communication plan?
<--- Score

93. Who are the Information Security Management improvement team members, including Management Leads and Coaches?
<--- Score

94. Is the improvement team aware of the different versions of a process: what they think it is vs. what it actually is vs. what it should be vs. what it could be?
<--- Score

95. Has the organization taken into account the minimum assurance requirements when implementing security controls?
<--- Score

96. Have the customer needs been translated into

specific, measurable requirements? How?
<--- Score

97. In what way can we redefine the criteria of choice clients have in our category in our favor?
<--- Score

98. Are approval levels defined for contracts and supplements to contracts?
<--- Score

99. How did the Information Security Management manager receive input to the development of a Information Security Management improvement plan and the estimated completion dates/times of each activity?
<--- Score

100. Are audit criteria, scope, frequency and methods defined?
<--- Score

Add up total points for this section:
_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Information Security Management Index at the beginning of the Self-Assessment.

SELF-ASSESSMENT SECTION START

CRITERION #3: MEASURE:

INTENT: Gather the correct data.
Measure the current performance and
evolution of the situation.

In my belief, the answer to this
question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. Are priorities and opportunities deployed to your suppliers, partners, and collaborators to ensure organizational alignment?
<--- Score

2. Is there a Performance Baseline?
<--- Score

3. Is data collected on key measures that were identified?

<--- Score

4. Is data collection planned and executed?
<--- Score

5. How are measurements made?
<--- Score

6. How frequently do you track Information Security Management measures?
<--- Score

7. How large is the gap between current performance and the customer-specified (goal) performance?
<--- Score

8. What are the types and number of measures to use?
<--- Score

9. How is the value delivered by Information Security Management being measured?
<--- Score

10. What methods are feasible and acceptable to estimate the impact of reforms?
<--- Score

11. How are you going to measure success?
<--- Score

12. Are process variation components displayed/ communicated using suitable charts, graphs, plots?
<--- Score

13. How will effects be measured?
<--- Score

14. Will We Aggregate Measures across Priorities?
<--- Score

15. What are my customers expectations and measures?
<--- Score

16. How do you measure success?
<--- Score

17. What are measures?
<--- Score

18. How can we measure the performance?
<--- Score

19. How will you measure your Information Security Management effectiveness?
<--- Score

20. What will be measured?
<--- Score

21. Do we effectively measure and reward individual and team performance?
<--- Score

22. Among the Information Security Management product and service cost to be estimated, which is considered hardest to estimate?
<--- Score

23. What evidence is there and what is measured?
<--- Score

24. How do you measure success?
<--- Score

25. Are we taking our company in the direction of better and revenue or cheaper and cost?
<--- Score

26. Who should receive measurement reports ?
<--- Score

27. Customer Measures: How Do Customers See Us?
<--- Score

28. What to measure and why?
<--- Score

29. What measurements are possible, practicable and meaningful?
<--- Score

30. Does Information Security Management systematically track and analyze outcomes for accountability and quality improvement?
<--- Score

31. What measurements are being captured?
<--- Score

32. Is it possible to estimate the impact of unanticipated complexity such as wrong or failed assumptions, feedback, etc. on proposed reforms?
<--- Score

33. Are there any easy-to-implement alternatives to Information Security Management? Sometimes other solutions are available that do not require the cost

implications of a full-blown project?
<--- Score

34. Is this an issue for analysis or intuition?
<--- Score

35. Who participated in the data collection for measurements?
<--- Score

36. Does Information Security Management analysis show the relationships among important Information Security Management factors?
<--- Score

37. Are key measures identified and agreed upon?
<--- Score

38. What is the total cost related to deploying Information Security Management, including any consulting or professional services?
<--- Score

39. What are the agreed upon definitions of the high impact areas, defect(s), unit(s), and opportunities that will figure into the process capability metrics?
<--- Score

40. Which methods and measures do you use to determine workforce engagement and workforce satisfaction?
<--- Score

41. How Will We Measure Success?
<--- Score

42. What Relevant Entities could be measured?
<--- Score

43. Are high impact defects defined and identified in the business process?
<--- Score

44. How will success or failure be measured?
<--- Score

45. What has the team done to assure the stability and accuracy of the measurement process?
<--- Score

46. What are the uncertainties surrounding estimates of impact?
<--- Score

47. What is an unallowable cost?
<--- Score

48. Have the types of risks that may impact Information Security Management been identified and analyzed?
<--- Score

49. Which customers can't participate in our market because they lack skills, wealth, or convenient access to existing solutions?
<--- Score

50. Are you taking your company in the direction of better and revenue or cheaper and cost?
<--- Score

51. Have you found any 'ground fruit' or 'low-

hanging fruit' for immediate remedies to the gap in performance?
<--- Score

52. Why do measure/indicators matter?
<--- Score

53. What are the key input variables? What are the key process variables? What are the key output variables?
<--- Score

54. Will Information Security Management have an impact on current business continuity, disaster recovery processes and/or infrastructure?
<--- Score

55. Can we do Information Security Management without complex (expensive) analysis?
<--- Score

56. What charts has the team used to display the components of variation in the process?
<--- Score

57. What particular quality tools did the team find helpful in establishing measurements?
<--- Score

58. Do you regularly scan your systems and networks, using a vulnerability analysis tool, for security exposures?
<--- Score

59. What are the costs of reform?
<--- Score

60. What data was collected (past, present, future/ ongoing)?
<--- Score

61. Is key measure data collection planned and executed, process variation displayed and communicated and performance baselined?
<--- Score

62. Are the units of measure consistent?
<--- Score

63. Why identify and analyze stakeholders and their interests?
<--- Score

64. How will measures be used to manage and adapt?
<--- Score

65. Is a solid data collection plan established that includes measurement systems analysis?
<--- Score

66. How will your organization measure success?
<--- Score

67. How to measure variability?
<--- Score

68. Is Process Variation Displayed/Communicated?
<--- Score

69. Does the practice systematically track and analyze outcomes related for accountability and quality improvement?
<--- Score

70. How frequently do we track measures?
<--- Score

71. Is the organization effectively analyzing the security impacts of identified changes to the information system and its environment of operation?
<--- Score

72. Have changes been properly/adequately analyzed for effect?
<--- Score

73. Does your enterprise follow a patch/update management and evaluation process to prioritize and mediate new security vulnerabilities?
<--- Score

74. Are there measurements based on task performance?
<--- Score

75. How can you measure Information Security Management in a systematic way?
<--- Score

76. When is Knowledge Management Measured?
<--- Score

77. How to measure lifecycle phases?
<--- Score

78. Why do the measurements/indicators matter?
<--- Score

79. Are the measurements objective?
<--- Score

80. Which customers cant participate in our Information Security Management domain because they lack skills, wealth, or convenient access to existing solutions?
<--- Score

81. Why Measure?
<--- Score

82. Does Information Security Management analysis isolate the fundamental causes of problems?
<--- Score

83. How is Knowledge Management Measured?
<--- Score

84. Do staff have the necessary skills to collect, analyze, and report data?
<--- Score

85. What potential environmental factors impact the Information Security Management effort?
<--- Score

86. Resulting risks, and selected countermeasures are the same for all companies. If a large number of companies have documented their experiences in this area, alongside the countermeasures they have selected for the possible risks, why do a comprehensive risk analysis to probably arrive at the same result?
<--- Score

87. Which Stakeholder Characteristics Are Analyzed?
<--- Score

88. What is the right balance of time and resources between investigation, analysis, and discussion and dissemination?
<--- Score

89. What does the charts tell us in terms of variation?
<--- Score

90. Was a data collection plan established?
<--- Score

91. What key measures identified indicate the performance of the business process?
<--- Score

92. Financial data, research results, etc.) that would violate policy, legal or regulatory requirements or cause embarrassment or competitive disadvantage if it were leaked?
<--- Score

93. What should be measured?
<--- Score

94. How do we focus on what is right -not who is right?
<--- Score

95. Where is it measured?
<--- Score

96. What are your key Information Security

Management organizational performance measures, including key short and longer-term financial measures?
<--- Score

97. How do you identify and analyze stakeholders and their interests?
<--- Score

98. Why should we expend time and effort to implement measurement?
<--- Score

99. Is the solution cost-effective?
<--- Score

100. Have all non-recommended alternatives been analyzed in sufficient detail?
<--- Score

101. Is performance measured?
<--- Score

102. Are losses documented, analyzed, and remedial processes developed to prevent future losses?
<--- Score

103. Does the Information Security Management task fit the client's priorities?
<--- Score

104. Has a business impact assessment been performed?
<--- Score

105. How do we do risk analysis of rare, cascading,

catastrophic events?
<--- Score

106. Is long term and short term variability accounted for?
<--- Score

107. Meeting the challenge: are missed Information Security Management opportunities costing us money?
<--- Score

108. How is progress measured?
<--- Score

109. What is measured?
<--- Score

110. What are our key indicators that you will measure, analyze and track?
<--- Score

111. What about Information Security Management Analysis of results?
<--- Score

112. Do we aggressively reward and promote the people who have the biggest impact on creating excellent Information Security Management services/products?
<--- Score

113. Have the concerns of stakeholders to help identify and define potential barriers been obtained and analyzed?
<--- Score

114. Can We Measure the Return on Analysis?
<--- Score

Add up total points for this section:
_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Information Security Management Index at the beginning of the Self-Assessment.

SELF-ASSESSMENT SECTION START

CRITERION #4: ANALYZE:

INTENT: Analyze causes, assumptions and hypotheses.

In my belief, the answer to this question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. Do you perform background checks on all employees with access to sensitive data, areas, or access points?
<--- Score

2. What conclusions were drawn from the team's data collection and analysis? How did the team reach these conclusions?
<--- Score

3. Record-keeping requirements flow from the

records needed as inputs, outputs, controls and for transformation of a Information Security Management process. ask yourself: are the records needed as inputs to the Information Security Management process available?
<--- Score

4. What successful thing are we doing today that may be blinding us to new growth opportunities?
<--- Score

5. Is the suppliers process defined and controlled?
<--- Score

6. Were Pareto charts (or similar) used to portray the 'heavy hitters' (or key sources of variation)?
<--- Score

7. Has the organization used its risk assessment (either formal or informal) to inform and guide the security control selection process?
<--- Score

8. What project management qualifications does the Project Manager have?
<--- Score

9. Are gaps between current performance and the goal performance identified?
<--- Score

10. Has the organization completed a security categorization of the information system including the information to be processed, stored, and transmitted by the system?
<--- Score

11. Do our leaders quickly bounce back from setbacks?
<--- Score

12. Is the performance gap determined?
<--- Score

13. A compounding model resolution with available relevant data can often provide insight towards a solution methodology; which Information Security Management models, tools and techniques are necessary?
<--- Score

14. Does the organization have an effective process in place to report the security status of the information system and its environment of operation to the authorizing officials and other designated senior leaders within the organization on an ongoing basis?
<--- Score

15. What other jobs or tasks affect the performance of the steps in the Information Security Management process?
<--- Score

16. Was a cause-and-effect diagram used to explore the different types of causes (or sources of variation)?
<--- Score

17. What is the cost of poor quality as supported by the team's analysis?
<--- Score

18. What are your current levels and trends in key measures or indicators of Information Security Management product and process performance that are important to and directly serve your customers? how do these results compare with the performance of your competitors and other organizations with similar offerings?
<--- Score

19. What tools were used to narrow the list of possible causes?
<--- Score

20. What are the revised rough estimates of the financial savings/opportunity for Information Security Management improvements?
<--- Score

21. Do you, as a leader, bounce back quickly from setbacks?
<--- Score

22. Identify an operational issue in your organization. for example, could a particular task be done more quickly or more efficiently?
<--- Score

23. What were the crucial 'moments of truth' on the process map?
<--- Score

24. Was a detailed process map created to amplify critical steps of the 'as is' business process?
<--- Score

25. Is sensitive data on laptops and remote

systems encrypted?
<--- Score

26. Have the problem and goal statements been updated to reflect the additional knowledge gained from the analyze phase?
<--- Score

27. What are our Information Security Management Processes?
<--- Score

28. Is there an effective and tested process to deal with information security incidents/emergencies?
<--- Score

29. Do your employees have the opportunity to do what they do best everyday?
<--- Score

30. Is the gap/opportunity displayed and communicated in financial terms?
<--- Score

31. How do you use Information Security Management data and information to support organizational decision making and innovation?
<--- Score

32. What other organizational variables, such as reward systems or communication systems, affect the performance of this Information Security Management process?
<--- Score

33. Think about some of the processes you

undertake within your organization. which do you own?
<--- Score

34. What were the financial benefits resulting from any 'ground fruit or low-hanging fruit' (quick fixes)?
<--- Score

35. What tools were used to generate the list of possible causes?
<--- Score

36. How was the detailed process map generated, verified, and validated?
<--- Score

37. What are the disruptive Information Security Management technologies that enable our organization to radically change our business processes?
<--- Score

38. I need to dispose of a computer that may have held personal or confidential data. do I need to do anything to ensure I do not contravene the data protection act?
<--- Score

39. Were there any improvement opportunities identified from the process analysis?
<--- Score

40. How does the organization define, manage, and improve its Information Security Management processes?
<--- Score

41. What kind of crime could a potential new hire have committed that would not only not disqualify him/her from being hired by our organization, but would actually indicate that he/she might be a particularly good fit?
<--- Score

42. What process should we select for improvement?
<--- Score

43. Did any additional data need to be collected?
<--- Score

44. Is there an effective and tested process to deal with information security incidents and emergencies?
<--- Score

45. Has the organization examined opportunities for reusing assessment results from previous assessments or from other sources?
<--- Score

46. How do mission and objectives affect the Information Security Management processes of our organization?
<--- Score

47. How do you measure the Operational performance of your key work systems and processes, including productivity, cycle time, and other appropriate measures of process effectiveness, efficiency, and innovation?
<--- Score

48. Have any additional benefits been identified that will result from closing all or most of the gaps?
<--- Score

49. What quality tools were used to get through the analyze phase?
<--- Score

50. An organizationally feasible system request is one that considers the mission, goals and objectives of the organization. key questions are: is the solution request practical and will it solve a problem or take advantage of an opportunity to achieve company goals?
<--- Score

51. What controls do we have in place to protect data?
<--- Score

52. Can we add value to the current Information Security Management decision-making process (largely qualitative) by incorporating uncertainty modeling (more quantitative)?
<--- Score

53. Were any designed experiments used to generate additional insight into the data analysis?
<--- Score

54. What are the best opportunities for value improvement?
<--- Score

55. Does the organization have an enterprise deviation handling process and is it integrated with an automated scanning capability?

<--- Score

56. Are the results of the security categorization process for the information system consistent with the organizations enterprise architecture and commitment to protecting organizational mission/ business processes?
<--- Score

57. How is the way you as the leader think and process information affecting your organizational culture?
<--- Score

58. Is there an ongoing process to ensure alignment of information security with business objectives?
<--- Score

59. What does the data say about the performance of the business process?
<--- Score

60. Is there an information asset classification process in place to ensure that critical assets are adequately protected?
<--- Score

61. What did the team gain from developing a sub-process map?
<--- Score

62. Security and privacy for data warehouses: opportunity or threat?
<--- Score

63. How will we keep the business going during

the recovery process?
<--- Score

64. How often will data be collected for measures?
<--- Score

65. Where is the data coming from to measure compliance?
<--- Score

66. Is Data and process analysis, root cause analysis and quantifying the gap/opportunity in place?
<--- Score

67. What data safeguards are available?
<--- Score

68. Do we have production data in non-production systems?
<--- Score

69. How do we promote understanding that opportunity for improvement is not criticism of the status quo, or the people who created the status quo?
<--- Score

70. What are your current levels and trends in key Information Security Management measures or indicators of product and process performance that are important to and directly serve your customers?
<--- Score

71. Is the Information Security Management process severely broken such that a re-design is necessary?

<--- Score

72. Think about the functions involved in your Information Security Management project. what processes flow from these functions?
<--- Score

73. Did any value-added analysis or 'lean thinking' take place to identify some of the gaps shown on the 'as is' process map?
<--- Score

74. When conducting a business process reengineering study, what should we look for when trying to identify business processes to change?
<--- Score

Add up total points for this section:
_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Information Security Management Index at the beginning of the Self-Assessment.

SELF-ASSESSMENT SECTION START

CRITERION #5: IMPROVE:

INTENT: Develop a practical solution. Innovate, establish and test the solution and to measure the results.

In my belief, the answer to this question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. Who controls key decisions that will be made?
<--- Score

2. How significant is the improvement in the eyes of the end user?
<--- Score

3. Is there a small-scale pilot for proposed improvement(s)? What conclusions were drawn from the outcomes of a pilot?

<--- Score

4. How do we improve productivity?
<--- Score

5. Is a solution implementation plan established, including schedule/work breakdown structure, resources, risk management plan, cost/budget, and control plan?
<--- Score

6. Are there any constraints (technical, political, cultural, or otherwise) that would inhibit certain solutions?
<--- Score

7. How does the solution remove the key sources of issues discovered in the analyze phase?
<--- Score

8. What is at Risk?
<--- Score

9. Are improved process ('should be') maps modified based on pilot data and analysis?
<--- Score

10. Risk factors: what are the characteristics of Information Security Management that make it risky?
<--- Score

11. How do you use other indicators, such as workforce retention, absenteeism, grievances, safety, and productivity, to assess and improve workforce engagement?

<--- Score

12. Do we cover the five essential competencies-Communication, Collaboration,Innovation, Adaptability, and Leadership that improve an organization's ability to leverage the new Information Security Management in a volatile global economy?
<--- Score

13. Is there a cost/benefit analysis of optimal solution(s)?
<--- Score

14. What should a proof of concept or pilot accomplish?
<--- Score

15. How will the team or the process owner(s) monitor the implementation plan to see that it is working as intended?
<--- Score

16. How will you know when its improved?
<--- Score

17. What actually has to improve and by how much?
<--- Score

18. Does the audit committee clearly understand its role in information security and how it will set direction with management and auditors?
<--- Score

19. Has the organization documented how system-specific and hybrid security controls have been

implemented within the information system taking into account specific technologies and platform dependencies?
<--- Score

20. How do you manage and improve your Information Security Management work systems to deliver customer value and achieve organizational success and sustainability?
<--- Score

21. Can the solution be designed and implemented within an acceptable time period?
<--- Score

22. Is the optimal solution selected based on testing and analysis?
<--- Score

23. How do we keep improving Information Security Management?
<--- Score

24. What is the team's contingency plan for potential problems occurring in implementation?
<--- Score

25. How do you improve your likelihood of success ?
<--- Score

26. How will we know that a change is improvement?
<--- Score

27. What is the implementation plan?
<--- Score

28. Are new and improved process ('should be') maps developed?
<--- Score

29. Was the authorization decision conveyed to appropriate organizational personnel including information system owners and common control providers?
<--- Score

30. What tools were most useful during the improve phase?
<--- Score

31. What is Information Security Management's impact on utilizing the best solution(s)?
<--- Score

32. Is information security risk assessment a regular agenda item at it and business management meetings and does management follow through and support improvement initiatives?
<--- Score

33. What can we do to improve?
<--- Score

34. Is the measure understandable to a variety of people?
<--- Score

35. What evaluation strategy is needed and what needs to be done to assure its implementation and use?
<--- Score

36. In the past few months, what is the smallest change we have made that has had the biggest positive result? What was it about that small change that produced the large return?
<--- Score

37. Has the organization tailored and supplemented the baseline security controls to ensure that the controls, if implemented, adequately mitigate risks to organizational operations and assets, individuals, other organizations, and the nation?
<--- Score

38. Do you understand what can accelerate change?
<--- Score

39. How will you measure the results?
<--- Score

40. What lessons, if any, from a pilot were incorporated into the design of the full-scale solution?
<--- Score

41. How important is the completion of a recognized college or graduate-level degree program in the hiring decision?
<--- Score

42. Was a pilot designed for the proposed solution(s)?
<--- Score

43. How can we improve performance?
<--- Score

44. What attendant changes will need to be made to ensure that the solution is successful?
<--- Score

45. Why improve in the first place?
<--- Score

46. How does the team improve its work?
<--- Score

47. Is the solution technically practical?
<--- Score

48. How do we measure improved Information Security Management service perception, and satisfaction?
<--- Score

49. Outline the types of risk responses that are acceptable to the organization (e.g., is risk transfer/sharing feasible and acceptable at this facility?
<--- Score

50. Is the implementation plan designed?
<--- Score

51. Were any criteria developed to assist the team in testing and evaluating potential solutions?
<--- Score

52. What improvements have been achieved?
<--- Score

53. Does the risk assessment consider what

information assets are subject to laws and regulations?
<--- Score

54. Who will be responsible for making the decisions to include or exclude requested changes once Information Security Management is underway?
<--- Score

55. Who are the people involved in developing and implementing Information Security Management?
<--- Score

56. Does the board understand the organizations dependence on information?
<--- Score

57. How did the team generate the list of possible solutions?
<--- Score

58. Who will be responsible for documenting the Information Security Management requirements in detail?
<--- Score

59. How Do We Link Measurement and Risk?
<--- Score

60. What does the 'should be' process map/design look like?
<--- Score

61. Has someone been appointed to be responsible for developing, implementing and managing the information security programme,

and is he/she held accountable?
<--- Score

62. Does the goal represent a desired result that can be measured?
<--- Score

63. Has the organization documented the common controls inherited from external providers?
<--- Score

64. Risk events: what are the things that could go wrong?
<--- Score

65. How do you measure progress and evaluate training effectiveness?
<--- Score

66. How do we Improve Information Security Management service perception, and satisfaction?
<--- Score

67. Who controls the risk?
<--- Score

68. Is a contingency plan established?
<--- Score

69. Are we Assessing Information Security Management and Risk?
<--- Score

70. What do we want to improve?
<--- Score

71. Is Supporting Information Security Management documentation required?
<--- Score

72. To what extent does management recognize Information Security Management as a tool to increase the results?
<--- Score

73. What tools do you use once you have decided on a Information Security Management strategy and more importantly how do you choose?
<--- Score

74. What needs improvement?
<--- Score

75. Are possible solutions generated and tested?
<--- Score

76. Applicable to development?
<--- Score

77. What are the implications of this decision 10 minutes, 10 months, and 10 years from now?
<--- Score

78. How do we decide how much to remunerate an employee?
<--- Score

79. When was the last time top management got involved in security-related decisions?
<--- Score

80. What is the risk?

<--- Score

81. What went well, what should change, what can improve?
<--- Score

82. How can skill-level changes improve Information Security Management?
<--- Score

83. What error proofing will be done to address some of the discrepancies observed in the 'as is' process?
<--- Score

84. Has the organization documented how common controls inherited by organizational information systems have been implemented?
<--- Score

85. Are the best solutions selected?
<--- Score

86. How do we go about Comparing Information Security Management approaches/solutions?
<--- Score

87. What is the magnitude of the improvements?
<--- Score

88. What tools were used to evaluate the potential solutions?
<--- Score

89. Describe the design of the pilot and what tests were conducted, if any?
<--- Score

90. What to do with the results or outcomes of measurements?
<--- Score

91. How will the organization know that the solution worked?
<--- Score

92. For decision problems, how do you develop a decision statement?
<--- Score

93. What resources are required for the improvement effort?
<--- Score

94. How do we measure risk?
<--- Score

95. Who will be using the results of the measurement activities?
<--- Score

96. Does the ceo request an information security evaluation, and are the results reviewed with staff and reported to the board of directors?
<--- Score

97. How will you know that you have improved?
<--- Score

98. How can we improve Information Security Management?
<--- Score

99. For estimation problems, how do you develop an estimation statement?
<--- Score

100. What tools were used to tap into the creativity and encourage 'outside the box' thinking?
<--- Score

101. How do the Information Security Management results compare with the performance of your competitors and other organizations with similar offerings?
<--- Score

102. How to Improve?
<--- Score

103. What communications are necessary to support the implementation of the solution?
<--- Score

104. Is there a high likelihood that any recommendations will achieve their intended results?
<--- Score

105. Where do you want to be a first mover, a fast follower or wait for industry solutions?
<--- Score

106. What were the underlying assumptions on the cost-benefit analysis?
<--- Score

107. How do you improve workforce health, safety, and security? What are your performance

measures and improvement goals for each of these workforce needs and what are any significant differences in these factors and performance measures or targets for different workplace environments?
<--- Score

108. Does the board understand the organisations dependence on information?
<--- Score

109. Is the enterprise clear on its position relative to IT and security risks?
<--- Score

110. If you could go back in time five years, what decision would you make differently? What is your best guess as to what decision you're making today you might regret five years from now?
<--- Score

111. At what point will vulnerability assessments be performed once Information Security Management is put into production (e.g., ongoing Risk Management after implementation)?
<--- Score

112. Is pilot data collected and analyzed?
<--- Score

Add up total points for this section:
_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Information Security Management Index at the beginning of the Self-Assessment.

SELF-ASSESSMENT SECTION START

CRITERION #6: CONTROL:

INTENT: Implement the practical solution. Maintain the performance and correct possible complications.

In my belief, the answer to this question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. What other systems, operations, processes, and infrastructures (hiring practices, staffing, training, incentives/rewards, metrics/dashboards/scorecards, etc.) need updates, additions, changes, or deletions in order to facilitate knowledge transfer and improvements?
<--- Score

2. Is there a transfer of ownership and knowledge to process owner and process team tasked with the

responsibilities.
<--- Score

3. How will report readings be checked to effectively monitor performance?
<--- Score

4. Is the organization effectively monitoring changes to the information system and its environment of operation including the effectiveness of deployed security controls in accordance with the continuous monitoring strategy?
<--- Score

5. Is there a documented and implemented monitoring plan?
<--- Score

6. Have new or revised work instructions resulted?
<--- Score

7. Will any special training be provided for results interpretation?
<--- Score

8. Did the organization update appropriate security plans based on the findings and recommendations in the security assessment report and any subsequent changes to the information system and its environment of operation?
<--- Score

9. What other areas of the organization might benefit from the Information Security Management team's

improvements, knowledge, and learning?
<--- Score

10. How will input, process, and output variables be checked to detect for sub-optimal conditions?
<--- Score

11. What are the critical parameters to watch?
<--- Score

12. How do our controls stack up?
<--- Score

13. Who will be in control?
<--- Score

14. Who has control over resources?
<--- Score

15. How can we best use all of our knowledge repositories to enhance learning and sharing?
<--- Score

16. What are the known security controls?
<--- Score

17. Did the organization develop an appropriate authorization package with all key documents including the security plan, security assessment report, and plan of action and milestones (if applicable)?
<--- Score

18. How will the day-to-day responsibilities for monitoring and continual improvement be transferred from the improvement team to the

process owner?
<--- Score

19. In the case of a Information Security Management project, the criteria for the audit derive from implementation objectives. an audit of a Information Security Management project involves assessing whether the recommendations outlined for implementation have been met. in other words, can we track that any Information Security Management project is implemented as planned, and is it working?
<--- Score

20. If there currently is no plan, will a plan be developed?
<--- Score

21. How likely is the current Information Security Management plan to come in on schedule or on budget?
<--- Score

22. Who controls critical resources?
<--- Score

23. Is the organization conducting ongoing assessments of security controls in accordance with the monitoring strategy?
<--- Score

24. Have you utilized or do you plan to utilize any consulting services to implement your information security management system?
<--- Score

25. Who is the Information Security Management process owner?
<--- Score

26. Do the results of the security categorization process reflect the organizations risk management strategy?
<--- Score

27. Is new knowledge gained imbedded in the response plan?
<--- Score

28. How do you encourage people to take control and responsibility?
<--- Score

29. What quality tools were useful in the control phase?
<--- Score

30. Has the organization allocated security controls as system-specific, hybrid, or common controls consistent with the enterprise architecture and information security architecture?
<--- Score

31. Have appropriate organizational officials approved security plans containing system-specific, hybrid, and common controls?
<--- Score

32. What should we measure to verify effectiveness gains?
<--- Score

33. Does Information Security Management appropriately measure and monitor risk?
<--- Score

34. Is a response plan established and deployed?
<--- Score

35. Has the organization demonstrated the use of sound information system and security engineering methodologies in integrating information technology products into the information system and in implementing the security controls contained in the security plan?
<--- Score

36. Has the improved process and its steps been standardized?
<--- Score

37. Did the assessor(s) complete the security control assessment in accordance with the stated assessment plan?
<--- Score

38. What are your results for key measures or indicators of the accomplishment of your Information Security Management strategy and action plans, including building and strengthening core competencies?
<--- Score

39. Is knowledge gained on process shared and institutionalized?
<--- Score

40. Did the organization develop a plan of action and milestones reflecting organizational priorities for addressing the remaining weaknesses and deficiencies in the information system and its environment of operation?
<--- Score

41. What set of countermeasures will provide the best protection against these risks?
<--- Score

42. Implementation Planning- is a pilot needed to test the changes before a full roll out occurs?
<--- Score

43. How do our controls stack up?
<--- Score

44. Do you monitor the effectiveness of your Information Security Management activities?
<--- Score

45. Is there a business continuity/disaster recovery plan in place?
<--- Score

46. Against what alternative is success being measured?
<--- Score

47. What should we measure to verify efficiency gains?
<--- Score

48. Has the organization considered the appropriate level of assessor independence for the

security control assessment?
<--- Score

49. Does the Information Security Management performance meet the customer's requirements?
<--- Score

50. Is there a standardized process?
<--- Score

51. How do controls support value?
<--- Score

52. Are damage assessment and disaster recovery plans in place?
<--- Score

53. Can we learn from other industries?
<--- Score

54. Does a troubleshooting guide exist or is it needed?
<--- Score

55. How will the process owner verify improvement in present and future sigma levels, process capabilities?
<--- Score

56. How do we enable market innovation while controlling security and privacy?
<--- Score

57. How will new or emerging customer needs/ requirements be checked/communicated to orient the process toward meeting the new specifications and continually reducing variation?
<--- Score

58. Against which risks must the information resources be protected?
<--- Score

59. How will the process owner and team be able to hold the gains?
<--- Score

60. What is the control/monitoring plan?
<--- Score

61. What should the next improvement project be that is related to Information Security Management?
<--- Score

62. Are there documented procedures?
<--- Score

63. Is a response plan in place for when the input, process, or output measures indicate an 'out-of-control' condition?
<--- Score

64. What is our theory of human motivation, and how does our compensation plan fit with that view?
<--- Score

65. Will existing staff require re-training, for example, to learn new business processes?
<--- Score

66. Has the organization developed a comprehensive plan to assess the security controls employed within or inherited by the information

system?
<--- Score

67. Are operating procedures consistent?
<--- Score

68. Was the assessment plan reviewed and approved by appropriate organizational officials?
<--- Score

69. Where do ideas that reach policy makers and planners as proposals for Information Security Management strengthening and reform actually originate?
<--- Score

70. Does job training on the documented procedures need to be part of the process team's education and training?
<--- Score

71. Perhaps leaving parent organization responsibilities to be covered by the parent organizations own information security-related governance plan?
<--- Score

72. What are the key elements of your Information Security Management performance improvement system, including your evaluation, organizational learning, and innovation processes?
<--- Score

73. Has the organization supplemented the common controls with system-specific or hybrid controls when the security control baselines of

the common controls are less than those of the information system inheriting the controls?
<--- Score

74. Is there a control plan in place for sustaining improvements (short and long-term)?
<--- Score

75. Has the organization allocated all security controls to the information system as system-specific, hybrid, or common controls?
<--- Score

76. Whats the best design framework for Information Security Management organization now that, in a post industrial-age if the top-down, command and control model is no longer relevant?
<--- Score

77. Does the response plan contain a definite closed loop continual improvement scheme (e.g., plan-do-check-act)?
<--- Score

78. Are suggested corrective/restorative actions indicated on the response plan for known causes to problems that might surface?
<--- Score

79. Are pertinent alerts monitored, analyzed and distributed to appropriate personnel?
<--- Score

80. Are documented procedures clear and easy to follow for the operators?
<--- Score

81. Is there a business continuity, disaster recovery plan in place?
<--- Score

82. How do you select, collect, align, and integrate Information Security Management data and information for tracking daily operations and overall organizational performance, including progress relative to strategic objectives and action plans?
<--- Score

83. Are controls in place and consistently applied?
<--- Score

84. Is the organization updating critical risk management documents based on ongoing monitoring activities?
<--- Score

85. Were the planned controls working?
<--- Score

86. Are authorizing officials conducting ongoing security authorizations by employing effective continuous monitoring activities and communicating updated risk determination and acceptance decisions to information system owners and common control providers?
<--- Score

87. Did the final risk determination and risk acceptance by the authorizing official reflect the risk management strategy developed by the organization and conveyed by the risk executive

(function)?
<--- Score

88. Has the organization established a poa&m program that is consistent with fisma requirements, policy, and applicable nist guidelines and tracks and monitors known information security weaknesses?
<--- Score

89. Were the planned controls in place?
<--- Score

90. What are we attempting to measure/monitor?
<--- Score

91. How does your workforce performance management system support high-performance work and workforce engagement; consider workforce compensation, reward, recognition, and incentive practices; and reinforce a customer and business focus and achievement of your action plans?
<--- Score

92. Do the decisions we make today help people and the planet tomorrow?
<--- Score

93. What do we stand for--and what are we against?
<--- Score

94. How might the organization capture best practices and lessons learned so as to leverage improvements across the business?

<--- Score

95. What key inputs and outputs are being measured on an ongoing basis?
<--- Score

96. Why is change control necessary?
<--- Score

97. What is your theory of human motivation, and how does your compensation plan fit with that view?
<--- Score

98. Is there a Information Security Management Communication plan covering who needs to get what information when?
<--- Score

99. Are new process steps, standards, and documentation ingrained into normal operations?
<--- Score

100. Do we monitor the Information Security Management decisions made and fine tune them as they evolve?
<--- Score

101. Is there a recommended audit plan for routine surveillance inspections of Information Security Management's gains?
<--- Score

102. Do the Information Security Management decisions we make today help people and the planet tomorrow?
<--- Score

103. Is reporting being used or needed?
<--- Score

104. Is there documentation that will support the successful operation of the improvement?
<--- Score

105. What is your quality control system?
<--- Score

106. What can you control?
<--- Score

107. What is the recommended frequency of auditing?
<--- Score

Add up total points for this section:
_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Information Security Management Index at the beginning of the Self-Assessment.

SELF-ASSESSMENT SECTION START

CRITERION #7: SUSTAIN:

INTENT: Retain the benefits.

In my belief, the answer to this question is clearly defined:

5 Strongly Agree

4 Agree

3 Neutral

2 Disagree

1 Strongly Disagree

1. Do you have a vision statement?
<--- Score

2. In a project to restructure Information Security Management outcomes, which stakeholders would you involve?
<--- Score

3. Are we spending a dollar to protect a dime?
<--- Score

4. How will you know that the Information Security Management project has been successful?

<--- Score

5. Are the criteria for selecting recommendations stated?
<--- Score

6. What information is critical to our organization that our executives are ignoring?
<--- Score

7. What business benefits will Information Security Management goals deliver if achieved?
<--- Score

8. Which Information Security Management goals are the most important?
<--- Score

9. Can we operate if critical information is unavailable, compromised or lost?
<--- Score

10. Political -is anyone trying to undermine this project?
<--- Score

11. If you were responsible for initiating and implementing major changes in your organization, what steps might you take to ensure acceptance of those changes?
<--- Score

12. Does anyone know how many computers the company owns?
<--- Score

13. Is maximizing Information Security Management protection the same as minimizing Information Security Management loss?
<--- Score

14. Why does this matter?
<--- Score

15. How will you motivate the dishwashers?
<--- Score

16. The purpose for ISO/IEC 17799?
<--- Score

17. How do we foster the skills, knowledge, talents, attributes, and characteristics we want to have?
<--- Score

18. How Does My Organisation Compare on Information Security Governance?
<--- Score

19. Do we think we know, or do we know we know ?
<--- Score

20. What are the rules and assumptions my industry operates under? What if the opposite were true?
<--- Score

21. Is every possible route to the Internet protected by a properly configured firewall?
<--- Score

22. What significant products are manufactured

and/or what services provided?
<--- Score

23. What are the Essentials of Internal Information Security Management Management?
<--- Score

24. Who is responsible for it?
<--- Score

25. What would have to be true for the option on the table to be the best possible choice?
<--- Score

26. What happens when a new employee joins the organization?
<--- Score

27. Are malicious software scanning tools deployed on all workstations and servers?
<--- Score

28. How does Information Security Management integrate with other business initiatives?
<--- Score

29. Who else should we help?
<--- Score

30. Were lessons learned captured and communicated?
<--- Score

31. Has the investment re-baselined during the past fiscal year?
<--- Score

32. What one word do we want to own in the minds of our customers, employees, and partners?
<--- Score

33. Does the head of security/ciso routinely meet or brief business management?
<--- Score

34. What technical safeguards are available?
<--- Score

35. Are you in a similar threat environment as the one assumed by the best practice?
<--- Score

36. How will we ensure we get what we expected?
<--- Score

37. In retrospect, of the projects that we pulled the plug on, what percent do we wish had been allowed to keep going, and what percent do we wish had ended earlier?
<--- Score

38. Has, is the policy statement subject to review, update and approval?
<--- Score

39. What potential megatrends could make our business model obsolete?
<--- Score

40. We have defined Information Security Management's Challenges, Critical Success Factors and Risks

<--- Score

41. Do we say no to customers for no reason?
<--- Score

42. What are all of our Information Security Management domains and what do they do?
<--- Score

43. Will it be accepted by users?
<--- Score

44. Are there appropriate training and awareness programmes to ensure that personnel are aware of their security responsibilities?
<--- Score

45. What threat is Information Security Management addressing?
<--- Score

46. What Should Information Security Governance Deliver?
<--- Score

47. What does the market believe?
<--- Score

48. Are we relevant? Will we be relevant five years from now? Ten?
<--- Score

49. Think of your Information Security Management project. what are the main functions?
<--- Score

50. How much contingency will be available in the budget?
<--- Score

51. Could someone walk into any of our locations and take something that doesnt belong to them?
<--- Score

52. What are nists fisma responsibilities?
<--- Score

53. Has the organization adequately described the characteristics of the information system?
<--- Score

54. How is business? Why?
<--- Score

55. Marketing budgets are tighter, consumers are more skeptical, and social media has changed forever the way we talk about Information Security Management. How do we gain traction?
<--- Score

56. We have defined Information Security Management's Scope
<--- Score

57. What is the purpose of Information Security Management in relation to the mission?
<--- Score

58. Are the resources you can expend similar to those called for by the best practice?
<--- Score

59. How Is Information Security Governance Evolving?
<--- Score

60. Is Information Security Management dependent on the successful delivery of a current project?
<--- Score

61. How do we make it meaningful in connecting Information Security Management with what users do day-to-day?
<--- Score

62. Who is responsible for errors?
<--- Score

63. We have defined Information Security Management's Purpose, Goal and Objective
<--- Score

64. How do we achieve information security?
<--- Score

65. Who Uses What?
<--- Score

66. What are the success criteria that will indicate that Information Security Management objectives have been met and the benefits delivered?
<--- Score

67. Schedule -can it be done in the given time?
<--- Score

68. When should you do training?
<--- Score

69. What is an unauthorized commitment?
<--- Score

70. Are we / should we be Revolutionary or evolutionary?
<--- Score

71. How do we Lead with Information Security Management in Mind?
<--- Score

72. What are strategies for increasing support and reducing opposition?
<--- Score

73. Who do we want out customers to become?
<--- Score

74. What are your most important goals for the strategic Information Security Management objectives?
<--- Score

75. What makes an Effective Information Security Policy?
<--- Score

76. Why Are Information Security and Information Security Governance Important?
<--- Score

77. We have defined Information Security Management's Value to the business

<--- Score

78. What are the gaps in my knowledge and experience?
<--- Score

79. How does my organization compare on information security governance?
<--- Score

80. Whos going to do all this?
<--- Score

81. What is your BATNA (best alternative to a negotiated agreement)?
<--- Score

82. How do you determine the key elements that affect Information Security Management workforce satisfaction? how are these elements determined for different workforce groups and segments?
<--- Score

83. Are there Information Security Management Models?
<--- Score

84. Can we maintain our growth without detracting from the factors that have contributed to our success?
<--- Score

85. Are the information assets subject to laws and regulations?
<--- Score

86. How are conflicts dealt with?
<--- Score

87. Are the user accounts of former employees immediately removed on termination?
<--- Score

88. Did the company suffer from the latest virus or malware attack?
<--- Score

89. What makes a good leader?
<--- Score

90. When information truly is ubiquitous, when reach and connectivity are completely global, when computing resources are infinite, and when a whole new set of impossibilities are not only possible, but happening, what will that do to our business?
<--- Score

91. What current systems have to be understood and/or changed?
<--- Score

92. Do you see more potential in people than they do in themselves?
<--- Score

93. What is a security blueprint?
<--- Score

94. What happens at this company when people fail?
<--- Score

95. What are the Key enablers to make this Information Security Management move?
<--- Score

96. Are we making progress? and are we making progress as Information Security Management leaders?
<--- Score

97. We have defined Information Security Management's Process Activities, Methods and Techniques
<--- Score

98. What knowledge, skills and characteristics mark a good Information Security Management project manager?
<--- Score

99. What does fisma tell me to do?
<--- Score

100. Are security group representatives involved in all stages of the project life cycle for new projects?
<--- Score

101. Do you keep 50% of your time unscheduled?
<--- Score

102. What are the short and long-term Information Security Management goals?
<--- Score

103. What is our competitive advantage?
<--- Score

104. If no one would ever find out about my accomplishments, how would I lead differently?
<--- Score

105. Whats our perimeter?
<--- Score

106. What is our Big Hairy Audacious Goal?
<--- Score

107. Which individuals, teams or departments will be involved in Information Security Management?
<--- Score

108. Legal and contractual - are we allowed to do this?
<--- Score

109. How do we engage the workforce, in addition to satisfying them?
<--- Score

110. What is it like to work for me?
<--- Score

111. Does anyone know how many people are using the organisations systems?
<--- Score

112. Are we changing as fast as the world around us?
<--- Score

113. Economic -do we have the time and money?
<--- Score

114. Information Security Management's Security Controls are defined
<--- Score

115. What happens if you do not have enough funding?
<--- Score

116. How will we know if we have been successful?
<--- Score

117. Whos responsible for the day-to-day security stuff?
<--- Score

118. What is Tricky About This?
<--- Score

119. Do I know what I'm doing? And who do I call if I don't?
<--- Score

120. Think about the kind of project structure that would be appropriate for your Information Security Management project. should it be formal and complex, or can it be less formal and relatively simple?
<--- Score

121. What should we stop doing?
<--- Score

122. If I had to leave my organization for a year and the only communication I could have with employees was a single paragraph, what would I write?
<--- Score

123. How can we incorporate support to ensure safe and effective use of Information Security Management into the services that we provide?
<--- Score

124. If we weren't already in this business, would we enter it today? And if not, what are we going to do about it?
<--- Score

125. Is there a ciso or officer specifically charged with managing information security in the organization?
<--- Score

126. How do you govern and fulfill your societal responsibilities?
<--- Score

127. What are specific Information Security Management Rules to follow?
<--- Score

128. How much does Information Security Management help?
<--- Score

129. Who do we think the world wants us to be?
<--- Score

130. How do we ensure that implementations of Information Security Management products are done in a way that ensures safety?
<--- Score

131. Are you satisfied with your current role? If not, what is missing from it?
<--- Score

132. How can you negotiate Information Security Management successfully with a stubborn boss, an irate client, or a deceitful coworker?
<--- Score

133. How should we bring in consultants, for which jobs and for how long?
<--- Score

134. What is our question?
<--- Score

135. Which functions and people interact with the supplier and or customer?
<--- Score

136. Does fisma apply to me?
<--- Score

137. How to Secure Information Security Management?
<--- Score

138. How does the organisation detect security incidents?
<--- Score

139. What will be the consequences to the business (financial, reputation etc) if Information Security Management does not go ahead or fails to deliver the objectives?
<--- Score

140. How can we become more high-tech but still be high touch?
<--- Score

141. How does the organization detect security incidents?
<--- Score

142. In the past year, what have you done (or could you have done) to increase the accurate perception of this company/brand as ethical and honest?
<--- Score

143. Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including for organization systems and services residing in a cloud external to the organization?
<--- Score

144. Is there any existing Information Security Management governance structure?
<--- Score

145. Who is nist, and what does nist have to do with fisma and information security?
<--- Score

146. Do we have the right people on the bus?
<--- Score

147. Information Security Management within Service Operation is a mature practice
<--- Score

148. We have defined Information Security Management's Information Management reporting
<--- Score

149. Who uses our product in ways we never expected?
<--- Score

150. Are assumptions made in Information Security Management stated explicitly?
<--- Score

151. Why don't our customers like us?
<--- Score

152. What is the overall business strategy?
<--- Score

153. Operational - will it work?
<--- Score

154. We have defined Information Security Management's Policies, Principles and basic concepts
<--- Score

155. Will there be any necessary staff changes (redundancies or new hires)?
<--- Score

156. What may be the consequences for the performance of an organization if all stakeholders are not consulted regarding Information Security Management?
<--- Score

157. Who will provide the final approval of Information Security Management deliverables?
<--- Score

158. Can unmanaged devices attach to our network?
<--- Score

159. What are the usability implications of Information Security Management actions?
<--- Score

160. Do we have the right capabilities and capacities?
<--- Score

161. Instead of going to current contacts for new ideas, what if you reconnected with dormant contacts--the people you used to know? If you were going reactivate a dormant tie, who would it be?
<--- Score

162. How do we foster innovation?
<--- Score

163. What Is Information Security Governance?
<--- Score

164. What is the mission of the organization?
<--- Score

165. Are there appropriate training and awareness programmes to ensure that personnel are aware of their security responsibilities and the expectations of management?

<--- Score

166. Which models, tools and techniques are necessary?
<--- Score

167. What is the enterprise security board (esb)?
<--- Score

168. The challenge to any information security manager is therefore to do the right things right. the question asked by many such managers is: how do I know what the right things are?
<--- Score

169. What counts that we are not counting?
<--- Score

170. Who will use it?
<--- Score

171. Which criteria are used to determine which projects are going to be pursued or discarded?
<--- Score

172. Who sets the Information Security Management standards?
<--- Score

173. What are the long-term Information Security Management goals?
<--- Score

174. What would I recommend my friend do if he were facing this dilemma?
<--- Score

175. Has the organisation suffered a major security incident?
<--- Score

176. If there were zero limitations, what would we do differently?
<--- Score

177. What Should the Board of Directors/Trustees and Senior Executives Be Doing?
<--- Score

178. How can we become the company that would put us out of business?
<--- Score

179. Do you have any supplemental information to add to this checklist?
<--- Score

180. We picked a method, now what?
<--- Score

181. Who are four people whose careers I've enhanced?
<--- Score

182. What new services of functionality will be implemented next with Information Security Management ?
<--- Score

183. Have there been intrusions?
<--- Score

184. Is a Information Security Management Team Work effort in place?
<--- Score

185. Are enterprise security policies updated on at least an annual basis, employees educated on changes, and consistently enforced?
<--- Score

186. Are you on schedule?
<--- Score

187. What was the last experiment we ran?
<--- Score

188. Among our stronger employees, how many see themselves at the company in three years? How many would leave for a 10 percent raise from another company?
<--- Score

189. Is security considered an afterthought or a prerequisite?
<--- Score

190. You may have created your customer policies at a time when you lacked resources, technology wasn't up-to-snuff, or low service levels were the industry norm. Have those circumstances changed?
<--- Score

191. What is fisma?
<--- Score

192. What is our Information Security Management

Strategy?
<--- Score

193. How do I stay inspired?
<--- Score

194. Ask yourself: how would we do this work if we only had one staff member to do it?
<--- Score

195. Who are you going to put out of business, and why?
<--- Score

196. What are your key business, operational, societal responsibility, and human resource strategic challenges and advantages?
<--- Score

197. Expenditures justified?
<--- Score

198. How are we doing compared to our industry?
<--- Score

199. Potential changes that would encourage innovation?
<--- Score

200. How do we maintain Information Security Management's Integrity?
<--- Score

201. Who are the key stakeholders?
<--- Score

202. Do we have bad profits?
<--- Score

203. How long will it take to change?
<--- Score

204. What does your signature ensure?
<--- Score

205. How will we recover from a disaster?
<--- Score

206. Who will determine interim and final deadlines?
<--- Score

207. If we got kicked out and the board brought in a new CEO, what would he do?
<--- Score

208. Do we underestimate the customer's journey?
<--- Score

209. What are the challenges?
<--- Score

210. Does management know who is responsible for security?
<--- Score

211. Does anyone know how many people are using the organizations systems?
<--- Score

212. How do we manage Information Security Management Knowledge Management (KM)?

<--- Score

213. What did we miss in the interview for the worst hire we ever made?
<--- Score

214. Who Should Be Concerned With Information Security Governance?
<--- Score

215. How to deal with Information Security Management Changes?
<--- Score

216. Whom among your colleagues do you trust, and for what?
<--- Score

217. Did the organization take the necessary remediation actions to address the most important weaknesses and deficiencies in the information system and its environment of operation based on the findings and recommendations in the security assessment report?
<--- Score

218. How is this enforced?
<--- Score

219. What am I trying to prove to myself, and how might it be hijacking my life and business success?
<--- Score

220. Are the assumptions believable and achievable?

<--- Score

221. What does the company expect?
<--- Score

222. What rules do we expect our employees to follow?
<--- Score

223. Whose voice (department, ethnic group, women, older workers, etc) might you have missed hearing from in your company, and how might you amplify this voice to create positive momentum for your business?
<--- Score

224. What trouble can we get into?
<--- Score

225. What trophy do we want on our mantle?
<--- Score

226. Do you have an implicit bias for capital investments over people investments?
<--- Score

227. What is a feasible sequencing of reform initiatives over time?
<--- Score

228. What is something you believe that nearly no one agrees with you on?
<--- Score

229. Has implementation been effective in reaching specified objectives?

<--- Score

230. What are the top 3 things at the forefront of our Information Security Management agendas for the next 3 years?
<--- Score

231. Who is On the Team?
<--- Score

232. Information Security Management's Management of security breaches and incidents is defined
<--- Score

233. What do we do when new problems arise?
<--- Score

234. What role does communication play in the success or failure of a Information Security Management project?
<--- Score

235. How do we go about Securing Information Security Management?
<--- Score

236. Have new benefits been realized?
<--- Score

237. Does the organization have a security strategy?
<--- Score

238. Has the organization registered the information system for purposes of management,

accountability, coordination, and oversight?
<--- Score

239. How will we insure seamless interoperability of Information Security Management moving forward?
<--- Score

240. Why should people listen to you?
<--- Score

241. How do we provide a safe environment -physically and emotionally?
<--- Score

242. What stupid rule would we most like to kill?
<--- Score

243. What Can Be Done to Successfully Implement Information Security Governance?
<--- Score

244. Did my employees make progress today?
<--- Score

245. Would you rather sell to knowledgeable and informed customers or to uninformed customers?
<--- Score

246. If our customer were my grandmother, would I tell her to buy what we're selling?
<--- Score

247. Who will manage the integration of tools?
<--- Score

248. Has the organization suffered a major security incident?
<--- Score

249. What is an information asset?
<--- Score

250. What External Factors Influence Our Success?
<--- Score

251. Who is responsible for what?
<--- Score

252. What information assets do we have?
<--- Score

253. What is Effective Information Security Management?
<--- Score

254. What is the range of capabilities?
<--- Score

255. How important is Information Security Management to the user organizations mission?
<--- Score

256. Is the impact that Information Security Management has shown?
<--- Score

257. What have we done to protect our business from competitive encroachment?
<--- Score

258. What are internal and external Information

Security Management relations?
<--- Score

259. What could go wrong?
<--- Score

260. What are the threats to information security?
<--- Score

261. How will we build a 100-year startup?
<--- Score

262. How would our PR, marketing, and social media change if we did not use outside agencies?
<--- Score

263. Why should we adopt a Information Security Management framework?
<--- Score

264. What will drive Information Security Management change?
<--- Score

265. Is management prepared to recover from a major security incident?
<--- Score

266. What is the extent of computer crime?
<--- Score

267. Is the Information Security Management organization completing tasks effectively and efficiently?
<--- Score

268. Who will be responsible for deciding whether Information Security Management goes ahead or not after the initial investigations?
<--- Score

269. What is the worst that could happen, or the worst that happened?
<--- Score

270. Do our employees really know whats expected of them?
<--- Score

271. Who is responsible for ensuring appropriate resources (time, people and money) are allocated to Information Security Management?
<--- Score

272. How much is being spent on information security?
<--- Score

273. Should we be doing background checks or credit checks on any employees?
<--- Score

274. Has, is the security management policy statement subject to review, update and approval?
<--- Score

275. What is industry best practice and how does the enterprise compare?
<--- Score

276. We have defined Information Security Management's Triggers, Imputs, Outputs and

interfaces
<--- Score

277. Are we paying enough attention to the partners our company depends on to succeed?
<--- Score

278. Who, on the executive team or the board, has spoken to a customer recently?
<--- Score

279. In what ways are Information Security Management vendors and us interacting to ensure safe and effective use?
<--- Score

280. What are the critical success factors?
<--- Score

281. Decryption at level ?
<--- Score

282. What are the business goals Information Security Management is aiming to achieve?
<--- Score

283. What management system can we use to leverage the Information Security Management experience, ideas, and concerns of the people closest to the work to be done?
<--- Score

284. Do we have job descriptions for the security team?
<--- Score

285. Who is going to care?
<--- Score

286. Am I failing differently each time?
<--- Score

287. Why are Information Security Management skills important?
<--- Score

288. If you had to rebuild your organization without any traditional competitive advantages (i.e., no killer a technology, promising research, innovative product/service delivery model, etc.), how would your people have to approach their work and collaborate together in order to create the necessary conditions for success?
<--- Score

289. Will I get fired?
<--- Score

290. What percentage of staff had security training last year?
<--- Score

291. Are new benefits received and understood?
<--- Score

292. What do we do when something goes wrong?
<--- Score

293. If our company went out of business tomorrow, would anyone who doesn't get a paycheck here care?
<--- Score

294. Why is it important to have senior management support for a Information Security Management project?
<--- Score

295. Who has fisma responsibilities?
<--- Score

296. What are we trying to achieve?
<--- Score

297. Who have we, as a company, historically been when we've been at our best?
<--- Score

298. Do Information Security Management rules make a reasonable demand on a users capabilities?
<--- Score

299. Who is the main stakeholder, with ultimate responsibility for driving Information Security Management forward?
<--- Score

300. If we do not follow, then how to lead?
<--- Score

301. Is our strategy driving our strategy? Or is the way in which we allocate resources driving our strategy?
<--- Score

302. What are we challenging, in the sense that Mac challenged the PC or Dove tackled the Beauty Myth?
<--- Score

303. What is senior management s security role?

<--- Score

304. What human safeguards are available?
<--- Score

305. How Should Training Be Timed?
<--- Score

306. Have benefits been optimized with all key stakeholders?
<--- Score

307. Are there any disadvantages to implementing Information Security Management? There might be some that are less obvious?
<--- Score

308. Where can we break convention?
<--- Score

309. Do we have enough freaky customers in our portfolio pushing us to the limit day in and day out?
<--- Score

310. To whom do you add value?
<--- Score

311. What is our formula for success in Information Security Management ?
<--- Score

312. We have defined Information Security Management's KPIs
<--- Score

313. How likely is it that a customer would

recommend our company to a friend or colleague?
<--- Score

314. Whats already gone wrong?
<--- Score

315. Is there any reason to believe the opposite of my current belief?
<--- Score

316. How do systems enter the organization?
<--- Score

Add up total points for this section:
_____ = Total points for this section

Divided by: _____ (number of statements answered) = _____
Average score for this section

Transfer your score to the Information Security Management Index at the beginning of the Self-Assessment.

Index