Data Loss Prevention

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

Data Loss Prevention
Complete Self-Assessment Guide

The guidance in this Self-Assessment is based on Data Loss Prevention 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.

Notice of rights

You are permitted to use the Self-Assessment contents in your presentations and materials for internal use and customers without asking us - we are here to help.

The information in this book is distributed on an "As Is" basis without warranty. While every precaution has been taken in the preparation of he book, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the products described in it.

Trademarks

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified throughout this book are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this book.

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

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 Data Loss Prevention 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 Data Loss Prevention 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 Data Loss Prevention, 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 Data Loss Prevention 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 Data

Loss Prevention, 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 Data Loss Prevention 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.

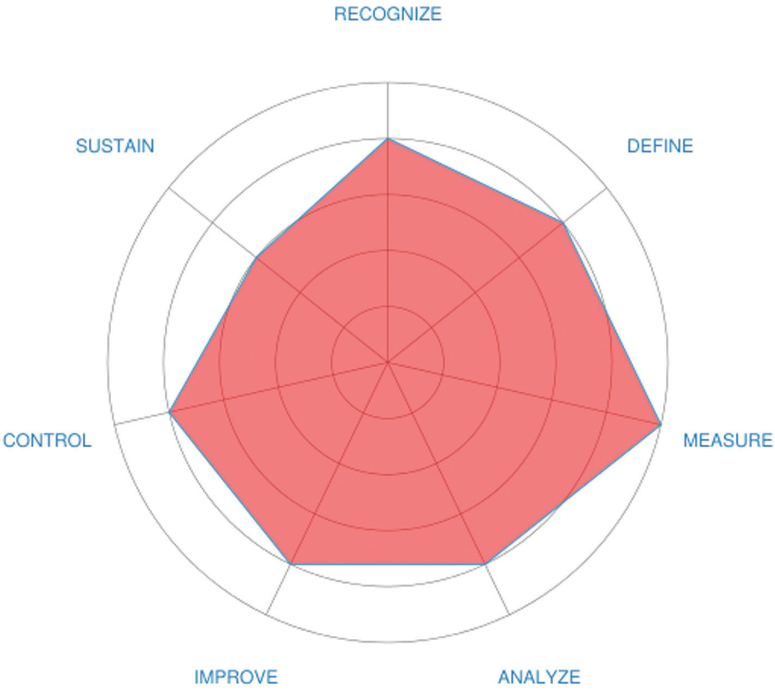
A score of '1' would mean that the answer is not clear at all, where a '5' would mean the answer is crystal clear and defined. Leave emtpy when the question is not applicable or you don't want to answer it, you can skip it without affecting your score. Write your score in the space provided.

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 Data Loss Prevention Scorecard on the second next page of the Self-Assessment.

Your completed Data Loss Prevention Scorecard will give you a clear presentation of which Data Loss Prevention areas need attention.

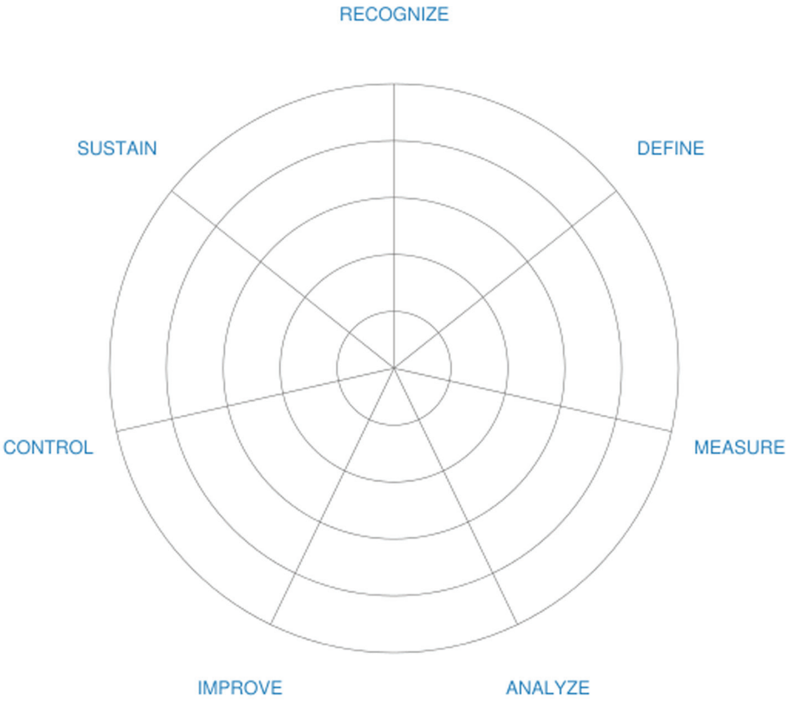
Data Loss Prevention Scorecard Example

Example of how the finalized Scorecard can look like:



Data Loss Prevention 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 is the smallest subset of the problem we can usefully solve?
<--- Score

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

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

4. Think about the people you identified for your Data Loss Prevention 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

5. What tools and technologies are needed for a custom Data Loss Prevention project?
<--- Score

6. How do we Identify specific Data Loss Prevention investment and emerging trends?
<--- Score

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

8. What are the expected benefits of Data Loss Prevention to the business?
<--- Score

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

10. Will new equipment/products be required to facilitate Data Loss Prevention delivery for example is new software needed?
<--- Score

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

12. Verbal handover reports: what skills are needed?
<--- Score

13. Will Data Loss Prevention deliverables need to be tested and, if so, by whom?
<--- Score

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

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

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

17. For your Data Loss Prevention project, identify and describe the business environment. is there more than one layer to the business environment?
<--- Score

18. Does our organization need more Data Loss Prevention education?
<--- Score

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

20. Does the tool we use provide the ability to prevent the forwarding of secure email?

<--- Score

21. Are there recognized Data Loss Prevention problems?
<--- Score

22. Can Management personnel recognize the monetary benefit of Data Loss Prevention?
<--- Score

23. Do you need to pre-filter traffic?
<--- Score

24. What are the business objectives to be achieved with Data Loss Prevention?
<--- Score

25. Does Data Loss Prevention create potential expectations in other areas that need to be recognized and considered?
<--- Score

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

27. What vendors make products that address the Data Loss Prevention needs?
<--- Score

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

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

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

31. How much are sponsors, customers, partners, stakeholders involved in Data Loss Prevention? In other words, what are the risks, if Data Loss Prevention does not deliver successfully?
<--- Score

32. What prevents me from making the changes I know will make me a more effective Data Loss Prevention leader?
<--- Score

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

34. What would happen if Data Loss Prevention weren't done?
<--- Score

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

36. When a Data Loss Prevention manager recognizes a problem, what options are available?
<--- Score

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

38. Are there any specific expectations or concerns about the Data Loss Prevention team, Data Loss Prevention itself?
<--- Score

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

40. What does Data Loss Prevention success mean to the stakeholders?
<--- Score

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

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

43. What problems are you facing and how do you consider Data Loss Prevention will circumvent those obstacles?
<--- Score

44. What situation(s) led to this Data Loss Prevention Self Assessment?
<--- Score

45. Do any copies need to be off-site?
<--- Score

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

47. What else needs to be measured?

<--- Score

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

49. Does the tool in use allow the ability to use Smart number identifiers (e.g., the ability to recognize that 999 99 9999 is not a valid Social Security number)?
<--- Score

50. How are the Data Loss Prevention's objectives aligned to the organization's overall business strategy?
<--- Score

51. Are there Data Loss Prevention problems 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 Data Loss Prevention 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. Is there a completed SIPOC representation, describing the Suppliers, Inputs, Process, Outputs, and Customers?
<--- Score

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

3. Is the team formed and are team leaders (Coaches

and Management Leads) assigned?
<--- Score

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

5. Does Data Loss Prevention 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

6. What are the compelling business reasons for embarking on Data Loss Prevention?
<--- Score

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

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

9. Is there a critical path to deliver Data Loss Prevention results?
<--- Score

10. Is the scope of Data Loss Prevention defined?
<--- Score

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

representation?
<--- Score

12. Are accountability and ownership for Data Loss Prevention clearly defined?
<--- Score

13. How can the value of Data Loss Prevention be defined?
<--- Score

14. How would one define Data Loss Prevention leadership?
<--- Score

15. Does the tool we use allow the ability to assign different weightings to specific words, wild card operators and case sensitivity/insensitivity indicators?
<--- Score

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

17. How does the Data Loss Prevention manager ensure against scope creep?
<--- Score

18. Has the direction changed at all during the course of Data Loss Prevention? If so, when did it change and why?
<--- Score

19. Are there encryption requirements, especially of off-line copies?

<--- Score

20. Is the Data Loss Prevention scope manageable?
<--- Score

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

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

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

24. Are improvement team members fully trained on Data Loss Prevention?
<--- Score

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

26. Has the Data Loss Prevention 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

27. Has a high-level ‘as is’ process map been completed, verified and validated?
<--- Score

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

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

30. What key business process output measure(s) does Data Loss Prevention leverage and how?
<--- Score

31. Have the customer needs been translated into specific, measurable requirements? How?
<--- Score

32. Does the tool we use provide the ability to delegate role-based user administration by scope?
<--- Score

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

34. Are there any constraints known that bear on the ability to perform Data Loss Prevention work? How is the team addressing them?
<--- Score

35. How often are the team meetings?
<--- Score

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

37. What are the rough order estimates on cost

savings/opportunities that Data Loss Prevention brings?
<--- Score

38. 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

39. Will team members regularly document their Data Loss Prevention work?
<--- Score

40. When was the Data Loss Prevention start date?
<--- Score

41. Is a fully trained team formed, supported, and committed to work on the Data Loss Prevention improvements?
<--- Score

42. What would be the goal or target for a Data Loss Prevention's improvement team?
<--- Score

43. Have all basic functions of Data Loss Prevention been defined?
<--- Score

44. Who are the Data Loss Prevention improvement team members, including Management Leads and Coaches?
<--- Score

45. Does the tool in use have a quarantine that

includes the ability to collect reports into cases?
<--- Score

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

47. Is Data Loss Prevention currently on schedule according to the plan?
<--- Score

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

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

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

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

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

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

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

55. How would you define the culture here?
<--- Score

56. How did the Data Loss Prevention manager receive input to the development of a Data Loss Prevention improvement plan and the estimated completion dates/times of each activity?
<--- Score

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

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

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

60. If substitutes have been appointed, have they been briefed on the Data Loss Prevention goals and received regular communications as to the progress to date?
<--- Score

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

62. What sources do you use to gather information for a Data Loss Prevention study?
<--- Score

63. How was the 'as is' process map developed,

reviewed, verified and validated?
<--- Score

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

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

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

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

68. 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

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

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

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

72. Has the improvement team collected the 'voice of the customer' (obtained feedback – qualitative and

quantitative)?
<--- Score

73. 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

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

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

76. Is Data Loss Prevention linked to key business goals and objectives?
<--- Score

77. Is there a Data Loss Prevention management charter, including business case, problem and goal statements, scope, milestones, roles and responsibilities, communication plan?
<--- Score

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

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

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

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

82. Do the problem and goal statements meet the SMART criteria (specific, measurable, attainable, relevant, and time-bound)?
<--- Score

83. How will variation in the actual durations of each activity be dealt with to ensure that the expected Data Loss Prevention results are met?
<--- Score

84. Will team members perform Data Loss Prevention work when assigned and in a timely fashion?
<--- Score

85. 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

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

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

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

89. Is it clearly defined in and to your organization

what you do?
<--- Score

90. How will the Data Loss Prevention team and the organization measure complete success of Data Loss Prevention?
<--- Score

91. Do we all define Data Loss Prevention in the same way?
<--- Score

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

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

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

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

96. Are there different segments of customers?
<--- 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 Data Loss Prevention 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. What is measured?
<--- Score

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

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

4. Is data collected on key measures that were identified?
<--- Score

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

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

7. Does the Data Loss Prevention task fit the client's priorities?
<--- Score

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

9. Meeting the challenge: are missed Data Loss Prevention opportunities costing us money?
<--- Score

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

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

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

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

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

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

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

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

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

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

20. Do we aggressively reward and promote the people who have the biggest impact on creating excellent products?
<--- Score

21. What potential environmental factors impact the Data Loss Prevention effort?
<--- Score

22. Why Measure?
<--- Score

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

24. Which customers cant participate in our Data Loss Prevention domain because they lack skills, wealth, or convenient access to existing solutions?
<--- Score

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

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

27. Does Data Loss Prevention analysis show the relationships among important Data Loss Prevention factors?
<--- Score

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

29. How can you measure Data Loss Prevention in a systematic way?
<--- Score

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

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

32. How do we do risk analysis of rare, cascading, catastrophic events?

<--- Score

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

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

35. Are there any easy-to-implement alternatives to Data Loss Prevention? Sometimes other solutions are available that do not require the cost implications of a full-blown project?
<--- Score

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

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

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

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

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

41. Does Data Loss Prevention analysis isolate the fundamental causes of problems?
<--- Score

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

43. Do we identify maximum allowable downtime for critical business functions, acceptable levels of data loss and backlogged transactions, RTOs, RPOs, recovery of the critical path (i.e., business processes or systems that should receive the highest priority), and the costs associated with downtime? Are the approved thresholds appropriate?
<--- Score

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

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

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

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

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

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

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

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

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

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

54. You don’t want to be informed of a data loss incident from the users themselves or from the data protection authority. Do you have technology that can detect breaches that have taken place; forensics available to investigate how the data was lost (or changed); and can you go back in time with full user logs and identify the incident to understand its scope and impact?
<--- Score

55. When was your last SWOT analysis for Internal Audit?
<--- Score

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

57. How has the economy impacted how we determine ongoing vendor viability?
<--- Score

58. What are measures?
<--- Score

59. What is the right balance of time and resources

between investigation, analysis, and discussion and dissemination?
<--- Score

60. Among the Data Loss Prevention product and service cost to be estimated, which is considered hardest to estimate?
<--- Score

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

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

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

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

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

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

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

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

69. What Causes Data Loss?
<--- Score

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

71. Does Data Loss Prevention systematically track and analyze outcomes for accountability and quality improvement?
<--- Score

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

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

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

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

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

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

78. 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

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

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

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

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

83. Do we aggressively reward and promote the people who have the biggest impact on creating excellent Data Loss Prevention services/products?
<--- Score

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

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

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

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

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

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

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

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

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

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

94. How will you measure your Data Loss Prevention effectiveness?
<--- Score

95. Meeting the Challenge: Are Missed Data Loss Prevention opportunities Costing you Money?
<--- Score

96. How is the value delivered by Data Loss Prevention being measured?
<--- Score

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

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

99. Is performance measured?
<--- Score

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

101. Have the types of risks that may impact Data Loss Prevention been identified and analyzed?
<--- Score

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

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

104. Have you found any 'ground fruit' or 'low-hanging fruit' for immediate remedies to the gap in performance?
<--- Score

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

106. What about Data Loss Prevention Analysis of

results?
<--- Score

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

108. How do you identify and analyze stakeholders and their interests?
<--- 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 Data Loss Prevention 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. How often will data be collected for measures?
<--- Score

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

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

4. Where is your data going?

<--- Score

5. What is the retention period of the data?
<--- Score

6. Where is the data?
<--- Score

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

8. What can you do to prevent data loss?
<--- Score

9. How does the organization define, manage, and improve its Data Loss Prevention processes?
<--- Score

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

11. What other organizational variables, such as reward systems or communication systems, affect the performance of this Data Loss Prevention process?
<--- Score

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

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

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

15. What sensitive data do you hold?
<--- Score

16. Record-keeping requirements flow from the records needed as inputs, outputs, controls and for transformation of a Data Loss Prevention process. ask yourself: are the records needed as inputs to the Data Loss Prevention process available?
<--- Score

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

18. What other jobs or tasks affect the performance of the steps in the Data Loss Prevention process?
<--- Score

19. Is the Data Loss Prevention process severely broken such that a re-design is necessary?
<--- Score

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

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

22. Do you have a policy in place to deal with data being lost or stolen (e.g., who needs to be notified, what steps need to be taken to mitigate damages)?
<--- Score

23. What are the risks associated with third party processing that are of most concern?
<--- Score

24. 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

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

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

27. Where can I store sensitive data?
<--- Score

28. Where does your sensitive data reside, both internally and with third parties?
<--- Score

29. Downtime and Data Loss: How Much Can You Afford?
<--- Score

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

31. What types of transactional activities and data mining are being used and where do we see the greatest potential benefits?
<--- Score

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

33. What are the physical location requirements for each copy of our data?
<--- Score

34. What is considered sensitive data?
<--- Score

35. 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

36. What are the best open source solutions for data loss prevention?
<--- Score

37. 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

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

39. Does management recognize that there is an increased motivation for fraud and data crimes, concurrent with expectations on audit departments to recognize such activities despite reduced budgets?
<--- Score

40. Who has (or can have) access to my data?
<--- Score

41. Will the Deployment be applied to all of the traffic of data in use, or in motion, or at rest?
<--- Score

42. What is your company doing to take advantage of automation to improve data & information integrity?
<--- Score

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

44. Are we protecting our data properly at rest if an attacker compromises our applications or systems?
<--- Score

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

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

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

48. How can hashes help prevent data loss from dos or ddos attacks?
<--- Score

49. What are the minimum data security requirements for a database containing personal financial transaction records?
<--- Score

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

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

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

53. How is the complex digital supply chain -where multiple downstream providers provide

services for each other and data residence and transmission points are increasingly obscure -being dealt with from an audit perspective?
<--- Score

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

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

56. How is third party processing being audited by organizations -e.g., right to audit clauses vs. reliance on SAS 70 reports?
<--- Score

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

58. Confidence -what is the data loss rate when the system is running at its required throughput?
<--- Score

59. 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

60. What processes are in place to govern the informational flow?
<--- Score

61. Why Data Loss Prevention?
<--- Score

62. How do mission and objectives affect the Data Loss Prevention processes of our organization?
<--- Score

63. What are your current levels and trends in key measures or indicators of Data Loss Prevention 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

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

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

66. Are reusable policy objects separate, referenced databases, files, or subroutines so that they can be reused in multiple policies, but centrally updated?
<--- Score

67. Can you afford the exposure created by the inadvertent loss of data resulting in fraudulent use of secretive, sensitive and personal data?

<--- Score

68. What is your most important data?
<--- Score

69. Does the tool in use provide the ability for role-based administration for sub-administrators (e.g., administrators for a specific domain) to restrict access and visibility into system data and system changes (if applicable)?
<--- Score

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

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

72. Do you know where your organizational data comes from, where it is stored, and how it is used?
<--- Score

73. What is Data Protection?
<--- Score

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

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

76. How do we see data loss prevention evolving?

<--- Score

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

78. Are there Data Dependencies or Consistency Groups?
<--- Score

79. What types of controls and associated technologies are considered essential to auditing third party processing?
<--- Score

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

81. What are the disruptive Data Loss Prevention technologies that enable our organization to radically change our business processes?
<--- Score

82. Does the tool in use allow the ability to search for registered data (e.g., database data) or specific files by name, hash marks, or watermarks, and to detect partial-file-content matches?
<--- Score

83. What are the revised rough estimates of the financial savings/opportunity for Data Loss Prevention improvements?
<--- Score

84. Are IT and executive management cognizant and being responsive to protecting organizations

from data loss breaches?
<--- Score

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

86. Think about some of the processes you undertake within your organization. which do you own?
<--- Score

87. Are there automated audit tools being used to determine the effectiveness of data loss prevention programs?
<--- Score

88. Do we have Data Protection Service Level Agreements?
<--- Score

89. Do you store a copy of backed up data off-site?
<--- Score

90. What is the data?
<--- Score

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

92. Who are the data loss prevention vendors?
<--- Score

93. Where does your sensitive data reside?
<--- Score

94. What tools were used to generate the list of possible causes?
<--- 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 Data Loss Prevention 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. Where do you want to be a first mover, a fast follower or wait for industry solutions?
<--- Score

2. 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

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

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

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

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

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

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

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

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

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

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

13. How can skill-level changes improve Data Loss Prevention?
<--- 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. What error proofing will be done to address some of the discrepancies observed in the 'as is' process?
<--- Score

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

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

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

20. How significant is the improvement in the eyes of the end user?

<--- Score

21. How do we measure improved Data Loss Prevention service perception, and satisfaction?
<--- Score

22. What tools do you use once you have decided on a Data Loss Prevention strategy and more importantly how do you choose?
<--- Score

23. How do we keep improving Data Loss Prevention?
<--- Score

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

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

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

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

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

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

30. What is the risk?
<--- Score

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

32. Who will be responsible for documenting the Data Loss Prevention requirements in detail?
<--- Score

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

34. 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

35. Risk factors: what are the characteristics of Data Loss Prevention that make it risky?
<--- Score

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

37. How to Improve?
<--- Score

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

39. Was a pilot designed for the proposed solution(s)?

<--- Score

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

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

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

43. Are we Assessing Data Loss Prevention and Risk?
<--- Score

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

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

46. Who will be responsible for making the decisions to include or exclude requested changes once Data Loss Prevention is underway?
<--- Score

47. 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

48. What is Data Loss Prevention’s impact on utilizing the best solution(s)?
<--- Score

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

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

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

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

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

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

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

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

57. Is there a high likelihood that any recommendations will achieve their intended results?

<--- Score

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

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

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

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

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

63. How do we Improve Data Loss Prevention service perception, and satisfaction?
<--- Score

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

65. Are there effective automation solutions available to help with this?
<--- Score

66. 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

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

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

69. What is your risk level compared to that of peer companies or competitors?
<--- Score

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

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

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

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

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

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

76. Who are the people involved in developing and implementing Data Loss Prevention?
<--- Score

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

78. What needs improvement?
<--- Score

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

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

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

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

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

84. How do we go about Comparing Data Loss Prevention approaches/solutions?
<--- Score

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

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

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

88. Is Supporting Data Loss Prevention documentation required?
<--- Score

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

90. How can we improve Data Loss Prevention?
<--- Score

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

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

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

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

95. To what extent does management recognize Data Loss Prevention as a tool to increase the results?
<--- Score

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

97. Is there a policy in place for passwords (e.g., changing, documenting, etc.)?
<--- 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 Data Loss Prevention 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. Are controls in place and consistently applied?
<--- Score

2. Are Incident response plans documented?
<--- Score

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

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

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

6. Does Data Loss Prevention appropriately measure and monitor risk?
<--- Score

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

8. Are audit plans and programs being modified / created to address data loss prevention?
<--- Score

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

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

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

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

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

14. Are there any other areas of CCM that could be used for more effective audits and timely identification of aberrant activities -e.g., monitoring IT controls?
<--- Score

15. How might the organization capture best practices and lessons learned so as to leverage improvements across the business?
<--- Score

16. What about policies and standards?
<--- Score

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

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

19. What is a standard data flow, and what should be the source and destination of the identified data?
<--- Score

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

21. Do the decisions we make today help people and

the planet tomorrow?
<--- Score

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

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

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

25. The goal of a disaster recovery plan is to minimize the costs resulting from losses of, or damages to, the resources or capabilities of your IT facilities. The success of any disaster recovery plan depends a great deal on being able to determine the risks associated with data loss. What is the impact to our business if the data is lost?
<--- Score

26. Does our security program adequately protected against opportunistic and targeted attackers?
<--- Score

27. Whats the best design framework for Data Loss Prevention organization now that, in a post industrial-age if the top-down, command and control model is no longer relevant?
<--- Score

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

<--- Score

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

30. What should the next improvement project be that is related to Data Loss Prevention?
<--- Score

31. How will the day-to-day responsibilities for monitoring and continual improvement be transferred from the improvement team to the process owner?
<--- Score

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

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

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

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

36. The goal of a disaster recovery plan is to minimize the costs resulting from losses of, or damages to, the resources or capabilities of your IT facilities. The success of any database disaster recovery plan depends a great deal on being able to determine the risks associated with data loss.

What is the impact to your business if the data is lost?
<--- Score

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

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

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

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

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

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

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

44. Do the Data Loss Prevention decisions we make today help people and the planet tomorrow?
<--- Score

45. What are your results for key measures or indicators of the accomplishment of your Data Loss Prevention strategy and action plans, including building and strengthening core

competencies?
<--- Score

46. What are the key elements of your Data Loss Prevention performance improvement system, including your evaluation, organizational learning, and innovation processes?
<--- Score

47. Who sets the Data Loss Prevention standards?
<--- Score

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

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

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

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

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

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

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

55. What Client Control Considerations were

included?
<--- Score

56. 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

57. Does the Data Loss Prevention performance meet the customer's requirements?
<--- Score

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

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

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

61. Do you monitor the effectiveness of your Data Loss Prevention activities?
<--- Score

62. What is the impact of the economy on executing our audit plans?
<--- Score

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

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

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

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

67. Is there a recommended audit plan for routine surveillance inspections of Data Loss Prevention's gains?
<--- Score

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

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

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

71. Is a response plan in place for when the input,

process, or output measures indicate an ‘out-of-control’ condition?
<--- Score

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

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

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

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

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

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

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

79. What other areas of the organization might benefit from the Data Loss Prevention team’s improvements, knowledge, and learning?
<--- Score

80. How has the use of CCM affected legacy audit planning and procedures?

<--- Score

81. Is a technical solution for data loss prevention -i.e., systems designed to automatically monitor for data leakage -considered essential to enterprise risk management?
<--- Score

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

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

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

85. 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

86. Who is the Data Loss Prevention process owner?
<--- Score

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

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

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

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

91. Where do ideas that reach policy makers and planners as proposals for Data Loss Prevention strengthening and reform actually originate?
<--- 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 Data Loss Prevention 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. Are we doing adequate due diligence before contracting with third party providers -particularly in regards to involving audit departments prior to contractual commitments?
<--- Score

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

3. What does off-site mean in your organization?
<--- Score

4. How do we provide a safe environment

-physically and emotionally?
<--- Score

5. Is maximizing Data Loss Prevention protection the same as minimizing Data Loss Prevention loss?
<--- Score

6. Do employees use laptops or home computers to work on agency business outside of the office?
<--- Score

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

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

9. Does the tool we use provide the ability to combine multiple Boolean operators and regular expressions into policies?
<--- Score

10. What role does communication play in the success or failure of a Data Loss Prevention project?
<--- Score

11. What is Effective Data Loss Prevention?
<--- Score

12. If you had to rebuild your organization without any traditional competitive advantages how would your people have to approach their work and collaborate together in order to create the necessary conditions for success?
<--- Score

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

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

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

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

17. What are the Key enablers to make this Data Loss Prevention move?
<--- Score

18. Which individuals, teams or departments will be involved in Data Loss Prevention?
<--- Score

19. If we do not follow, then how to lead?
<--- Score

20. How likely is it that a customer would recommend our company to a friend or colleague?
<--- Score

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

22. What does your signature ensure?

<--- Score

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

24. How does Data Loss Prevention integrate with other business initiatives?
<--- Score

25. What is a feasible sequencing of reform initiatives over time?
<--- Score

26. Other than port blocking what sort of security does our host provider provide?
<--- Score

27. What are the success criteria that will indicate that Data Loss Prevention objectives have been met and the benefits delivered?
<--- Score

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

29. 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

30. Are the assumptions believable and achievable?
<--- Score

31. What is the range of capabilities?
<--- Score

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

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

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

35. Does the tool we use provide the ability for system-generated notification to arbitrator of email disposition?
<--- Score

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

37. 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

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

39. How will you know that the Data Loss Prevention project has been successful?

<--- Score

40. Does the tool we use provide the ability to print an easy-to-read policy summary for audit purposes?
<--- Score

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

42. 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

43. Do we have designated Privacy Officers?
<--- Score

44. What are your most important goals for the strategic Data Loss Prevention objectives?
<--- Score

45. What trophy do we want on our mantle?
<--- Score

46. 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

47. To whom do you add value?
<--- Score

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

49. Does the tool we use provide the ability to send and receive secure email without browser plug ins or client software?
<--- Score

50. Do we utilize security awareness training?
<--- Score

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

52. How will we know our systems have been hacked?
<--- Score

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

54. Does the tool in use provide the ability for administrators to access a graphical and table-based dashboard with click-through, drill-down detail (using percentage-based metrics, not definitive totals)?
<--- Score

55. Does our tool have the ability to integrate with Digital Rights Management Client & Server?
<--- Score

56. Who is the main stakeholder, with ultimate responsibility for driving Data Loss Prevention forward?
<--- Score

57. Are all computer files backed up on a regular

basis?
<--- Score

58. How will the setup of endpoints with the DLP manager occur?
<--- Score

59. If applicable, is the wireless WEP or WPA encrypted?
<--- Score

60. Why should people listen to you?
<--- Score

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

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

63. What is something you believe that nearly no one agrees with you on?
<--- Score

64. If our company went out of business tomorrow, would anyone who doesn’t get a paycheck here care?
<--- Score

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

66. In what ways are Data Loss Prevention vendors and us interacting to ensure safe and effective use?

<--- Score

67. Why is it important to have senior management support for a Data Loss Prevention project?
<--- Score

68. Are we making progress? and are we making progress as Data Loss Prevention leaders?
<--- Score

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

70. How will we build a 100-year startup?
<--- Score

71. What trouble can we get into?
<--- Score

72. Does the tool we use have a quarantine that includes the ability to redact and/or highlight sensitive information?
<--- Score

73. What are specific Data Loss Prevention Rules to follow?
<--- Score

74. 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

75. How can we incorporate support to ensure safe

and effective use of Data Loss Prevention into the services that we provide?
<--- Score

76. What are the top 3 things at the forefront of our Data Loss Prevention agendas for the next 3 years?
<--- Score

77. Have benefits been optimized with all key stakeholders?
<--- Score

78. Ask yourself: how would we do this work if we only had one staff member to do it?
<--- Score

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

80. Does the tool we use provide a task-based help function with recommendation settings for mail configuration options?
<--- Score

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

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

83. Who are you going to put out of business, and why?

<--- Score

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

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

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

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

88. How do you contribute to the companies mission?
<--- Score

89. Where can we break convention?
<--- Score

90. Should the deployment occur in high availability mode or should we configure in bypass mode?
<--- Score

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

92. 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

93. Does the tool we use provide the ability to delegate role-based user administration to Agency Administrator by domain?
<--- Score

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

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

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

97. What are the challenges?
<--- Score

98. Does the tool we use allow the ability to add custom number templates (e.g., customer/client IDs)?
<--- Score

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

100. How do we maintain Data Loss Prevention's Integrity?
<--- Score

101. Who is sending confidential information?
<--- Score

102. Are new benefits received and understood?
<--- Score

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

104. What about spot-checking instead?
<--- Score

105. What stupid rule would we most like to kill?
<--- Score

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

107. What is our formula for success in Data Loss Prevention ?
<--- Score

108. Who have we, as a company, historically been when we've been at our best?
<--- Score

109. How do we go about Securing Data Loss Prevention?
<--- Score

110. How are we doing compared to our industry?
<--- Score

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

112. What is our Data Loss Prevention Strategy?
<--- Score

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

114. Whom among your colleagues do you trust, and for what?
<--- Score

115. Is there any reason to believe the opposite of my current belief?
<--- Score

116. What have we done to protect our business from competitive encroachment?
<--- Score

117. Does the tool we use provide the ability for a sender to specify a time limit for recipient to access a secure email?
<--- Score

118. Do handovers take place in a quiet room off the main ENT (ear nose throat) ?
<--- Score

119. Are there any disadvantages to implementing Data Loss Prevention? There might be some that are less obvious?
<--- Score

120. If we got kicked out and the board brought in a new CEO, what would he do?
<--- Score

121. How many copies must be off-line?
<--- Score

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

123. Who is responsible for ensuring appropriate resources (time, people and money) are allocated to Data Loss Prevention?
<--- Score

124. How long will it take to change?
<--- Score

125. 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

126. Who will provide the final approval of Data Loss Prevention deliverables?
<--- Score

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

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

129. 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

130. What are the business goals Data Loss Prevention is aiming to achieve?
<--- Score

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

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

133. Why are Data Loss Prevention skills important?
<--- Score

134. How can you negotiate Data Loss Prevention successfully with a stubborn boss, an irate client, or a deceitful coworker?
<--- Score

135. Why Bother With A DP SLA?
<--- Score

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

137. How do you determine the key elements that affect Data Loss Prevention workforce satisfaction? how are these elements determined for different workforce groups and segments?
<--- Score

138. Do we have bad profits?
<--- Score

139. Did my employees make progress today?
<--- Score

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

141. What may be the consequences for the performance of an organization if all stakeholders are not consulted regarding Data Loss Prevention?
<--- Score

142. What do we do when new problems arise?
<--- Score

143. Would you rather sell to knowledgeable and informed customers or to uninformed customers?
<--- Score

144. How do I stay inspired?
<--- Score

145. Do we have enough freaky customers in our portfolio pushing us to the limit day in and day out?
<--- Score

146. Who will be responsible for deciding whether Data Loss Prevention goes ahead or not after the initial investigations?
<--- Score

147. 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

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

149. Are all computers password protected?
<--- Score

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

151. What is the worst that could happen, or the worst that happened?
<--- Score

152. Is website access and maintenance information accessible by the ED and at least one other person (e.g., Board Chair)?
<--- Score

153. What are we challenging, in the sense that Mac challenged the PC or Dove tackled the Beauty Myth?
<--- Score

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

155. Does the tool we use have the ability to integrate with Enterprise Active Directory Servers to determine users and build user, role, and business unit policies?
<--- Score

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

157. Does the Executive Director and at least one other person (e.g., Board Chair) have access to all passwords?
<--- Score

158. What knowledge, skills and characteristics mark a good Data Loss Prevention project manager?
<--- Score

159. Does the tool we use have the ability to deep inspect a large number of file types for content matches (e.g., .pdf; .docx; .txt; .html; .xlsx, etc.)?
<--- Score

160. Is our strategy driving our strategy? Or is the way in which we allocate resources driving our strategy?
<--- Score

161. What External Factors Influence Our Success?
<--- Score

162. Is Data Loss Prevention dependent on the successful delivery of a current project?
<--- Score

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

164. Can we maintain our growth without

detracting from the factors that have contributed to our success?
<--- Score

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

166. What are all the egress points present in the network?
<--- Score

167. Are there audit areas that are candidates for elimination or reduced audit coverage to accommodate strained budgets?
<--- Score

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

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

170. What will be the consequences to the business (financial, reputation etc) if Data Loss Prevention does not go ahead or fails to deliver the objectives?
<--- Score

171. 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

172. If our customer were my grandmother, would I tell her to buy what we're selling?
<--- Score

173. Are there Data Loss Prevention Models?
<--- Score

174. What management system can we use to leverage the Data Loss Prevention experience, ideas, and concerns of the people closest to the work to be done?
<--- Score

175. Are assumptions made in Data Loss Prevention stated explicitly?
<--- Score

176. Are the files employees work on outside of the office transferred into the office system on a regular basis?
<--- Score

177. Do we underestimate the customer's journey?
<--- Score

178. Is Data Loss Prevention dependent on the successful delivery of a current project?
<--- Score

179. How do we maintaining integrity between communication ports and firewalls?
<--- Score

180. Who will manage the integration of tools?
<--- Score

181. Do we ask the question, What could go wrong and whats the worst that can happen?
<--- Score

182. What am I trying to prove to myself, and how might it be hijacking my life and business success?
<--- Score

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

184. Who are the key stakeholders?
<--- Score

185. Who will determine interim and final deadlines?
<--- Score

186. How do we ensure that implementations of Data Loss Prevention products are done in a way that ensures safety?
<--- Score

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

188. Does the tool we use support the ability to configure user content management alerts?
<--- Score

189. What will drive Data Loss Prevention change?
<--- Score

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

191. Has the investment re-baselined during the past fiscal year?

<--- Score

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

193. Are we paying enough attention to the partners our company depends on to succeed?
<--- Score

194. What do we hope to achieve with a DLP deployment?
<--- Score

195. Who, on the executive team or the board, has spoken to a customer recently?
<--- Score

196. 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

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

198. Do you have guidelines or a policy in place defining the parameters for employees working on files outside of the office?
<--- Score

199. Does the tool in use have the ability to integrate with Active Directory or sync directory on a scheduled basis, or do look-ups within a multi-domain forest in the sub-100-millisecond range?
<--- Score

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

201. How to deal with Data Loss Prevention Changes?
<--- Score

202. What are your key business, operational, societal responsibility, and human resource strategic challenges and advantages?
<--- Score

203. What did we miss in the interview for the worst hire we ever made?
<--- Score

204. Am I failing differently each time?
<--- Score

205. Who will determine interim and final deadlines?
<--- Score

206. Think about the kind of project structure that would be appropriate for your Data Loss Prevention project. should it be formal and complex, or can it be less formal and relatively simple?
<--- Score

207. Have new benefits been realized?
<--- Score

208. Do all computers have up-to-date antivirus protection?
<--- Score

209. Who is the System Administrator?
<--- Score

210. In a project to restructure Data Loss Prevention outcomes, which stakeholders would you involve?
<--- Score

211. How to Secure Data Loss Prevention?
<--- Score

212. Is the impact that Data Loss Prevention has shown?
<--- Score

213. How would our PR, marketing, and social media change if we did not use outside agencies?
<--- Score

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

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

216. What was the last experiment we ran?
<--- Score

217. Do you have an implicit bias for capital investments over people investments?
<--- Score

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

219. How do we Lead with Data Loss Prevention in Mind?
<--- Score

220. Is the use of CCM destined to become an important and requisite audit methodology best practice?
<--- Score

221. What are the critical success factors?
<--- Score

222. What are we trying to achieve?
<--- Score

223. Has implementation been effective in reaching specified objectives?
<--- Score

224. What are your most offensive protocols?
<--- Score

225. Do all computers have up-to-date anti-spam protection?
<--- Score

226. Do we have the the ability to create multiple quarantine queues?

<--- Score

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

228. Does the tool we use provide the ability for mobile devices to access critical portions of the management interface?
<--- Score

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

230. What business benefits will Data Loss Prevention goals deliver if achieved?
<--- 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 Data Loss Prevention Index at the beginning of the Self-Assessment.

Index