

# ISO IEC 27001 2013 TRANSLATED INTO PLAIN ENGLISH

## 9. EVALUATION REQUIREMENTS IN PLAIN ENGLISH

### 9.1 MONITOR, MEASURE, ANALYZE, AND EVALUATE YOUR INFORMATION SECURITY

1	Figure out how you're going to assess the performance of your information security and determine the effectiveness of your ISMS.	TODO	DONE	The purpose of <i>information security</i> is to protect and preserve information. It's central purpose is to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable.
2	Figure out how you're going to <i>monitor</i> the performance of your organization's information security and the effectiveness of its ISMS.	TODO	DONE	
3	Determine what needs to be monitored.	TODO	DONE	An <i>ISMS (information security management system)</i> includes all of the policies, procedures, plans, processes, practices, roles, responsibilities, resources, and structures that organizations use to protect and preserve information and to manage and control information security risks. An <i>ISMS</i> is part of your larger management system.
4	Figure out which information security processes need to be monitored.	TODO	DONE	
5	Figure out which information security controls need to be monitored.	TODO	DONE	
6	Select your monitoring methods.	TODO	DONE	
7	Make sure that your monitoring methods are capable of producing valid results.	TODO	DONE	
8	Figure out how you're going to ensure that your monitoring methods will produce results that are comparable and reproducible.	TODO	DONE	
9	Establish when monitoring should be performed.	TODO	DONE	
10	Decide who should carry out the monitoring.	TODO	DONE	
11	Maintain a record of your monitoring results.	TODO	DONE	These records are "documented information". Therefore they must be controlled (per 7.5.3).
12	Control your monitoring records.	TODO	DONE	
13	Figure out how you're going to <i>measure</i> the performance of your organization's information security and the effectiveness of its ISMS.	TODO	DONE	
14	Determine what needs to be measured.	TODO	DONE	
15	Figure out which information security processes need to be measured.	TODO	DONE	

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

NOV 2013

PLAIN ENGLISH INFORMATION SECURITY MANAGEMENT STANDARD

EDITION 1.1

PART 9

COPYRIGHT © 2013 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.

PAGE 56

# ISO IEC 27001 2013 TRANSLATED INTO PLAIN ENGLISH

## 9. EVALUATION REQUIREMENTS IN PLAIN ENGLISH

16		Figure out which information security controls need to be measured.	TODO	DONE	
17		Select your measurement methods.	TODO	DONE	
18		Make sure that your measurement methods are capable of producing valid results.	TODO	DONE	
19		Figure out how you're going to ensure that your measurement methods will produce results that are comparable and reproducible.	TODO	DONE	
20		Establish when measurements should be performed.	TODO	DONE	
21		Decide who should carry out measurements.	TODO	DONE	
22		Maintain a record of your measurement results.	TODO	DONE	These records are "documented information". Therefore they must be controlled (per 7.5.3).
23		Control your measurement records.	TODO	DONE	
24		Figure out how you're going to <i>analyze</i> the performance of your organization's information security and the effectiveness of its ISMS.	TODO	DONE	
25		Select your analytical methods.	TODO	DONE	
26		Make sure that your analytical methods are capable of producing valid results.	TODO	DONE	
27		Figure out how you're going to ensure that your analytical methods will produce results that are comparable and reproducible.	TODO	DONE	
28		Decide when your monitoring and measurement results should be analyzed.	TODO	DONE	
29		Determine who should analyze your monitoring and measurement results.	TODO	DONE	
30		Figure out how you're going to <i>evaluate</i> the performance of your organization's information security and the effectiveness of its ISMS.	TODO	DONE	

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

**NOV 2013**

**PLAIN ENGLISH INFORMATION SECURITY MANAGEMENT STANDARD**

**EDITION 1.1**

**PART 9**

**COPYRIGHT © 2013 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.**

**PAGE 57**

# ISO IEC 27001 2013 TRANSLATED INTO PLAIN ENGLISH

## 9. EVALUATION REQUIREMENTS IN PLAIN ENGLISH

31		Select your evaluation methods.	TODO	DONE	
32		Make sure that your evaluation methods are capable of producing valid results.	TODO	DONE	
33		Figure out how you`re going to ensure that your evaluation methods will produce results that are comparable and reproducible.	TODO	DONE	
34		Establish when your monitoring and measurement results should be evaluated.	TODO	DONE	
35		Decide who should evaluate your monitoring and measurement results.	TODO	DONE	
36		Assess the performance of your information security and determine the effectiveness of your ISMS.	TODO	DONE	
37		<i>Monitor</i> the performance of your organization's information security and the effectiveness of its ISMS.	TODO	DONE	
38		<i>Measure</i> the performance of your organization's information security and the effectiveness of its ISMS.	TODO	DONE	
39		<i>Analyze</i> the performance of your organization's information security and the effectiveness of its ISMS.	TODO	DONE	
40		<i>Evaluate</i> the performance of your organization's information security and the effectiveness of its ISMS.	TODO	DONE	

### 9.2 SET UP AN INTERNAL AUDIT PROGRAM AND USE IT TO EVALUATE YOUR ISMS

41		Plan the development of an internal ISMS audit program for your organization.	TODO	DONE	<p>An <i>audit</i> is an evidence gathering process. Evidence is used to evaluate how well audit criteria are being met. Audits must be objective, impartial, and independent, and the audit process must be systematic and documented.</p> <p>Use the ISO 19011 2011 auditing standard to help establish your internal audit program. See <a href="http://www.praxiom.com/19011.htm">http://www.praxiom.com/19011.htm</a></p>
42		Make sure that your audit program is capable of determining whether or not your ISMS conforms to requirements.	TODO	DONE	
43		Make sure that your audit program is capable of determining whether or not your organization's ISMS conforms to its own ISMS requirements.	TODO	DONE	

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

NOV 2013

PLAIN ENGLISH INFORMATION SECURITY MANAGEMENT STANDARD

EDITION 1.1

PART 9

COPYRIGHT © 2013 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.

PAGE 58

## ISO IEC 27001 2013 TRANSLATED INTO PLAIN ENGLISH

### 9. EVALUATION REQUIREMENTS IN PLAIN ENGLISH

44	Make sure that your audit program is capable of determining whether or not your ISMS conforms to the ISO IEC 27001 2013 information security requirements.	TODO	DONE	
45	Make sure that your audit program is capable of determining whether or not your ISMS has been implemented effectively.	TODO	DONE	
46	Make sure that your program is capable of determining whether or not your ISMS is being properly maintained.	TODO	DONE	
47	Establish your internal ISMS audit program.	TODO	DONE	
48	Establish your internal audit methods.	TODO	DONE	
49	Establish internal audit responsibilities.	TODO	DONE	
50	Establish internal audit planning requirements.	TODO	DONE	
51	Make sure that each internal audit studies the results of previous audits.	TODO	DONE	
52	Make sure that each internal audit considers the importance of the processes being audited.	TODO	DONE	
53	Make sure that each internal audit preserves the objectivity and impartiality of the audit process.	TODO	DONE	
54	Establish your internal audit schedules.	TODO	DONE	
55	Specify how often internal audits should be done.	TODO	DONE	
56	Conduct internal audits at planned intervals.	TODO	DONE	
57	Consider the results of previous audits when you schedule your organization's internal audits.	TODO	DONE	
58	Establish internal audit reporting requirements.	TODO	DONE	
59	Make sure that internal audit results are reported to the appropriate members of management.	TODO	DONE	

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

**NOV 2013**

**PLAIN ENGLISH INFORMATION SECURITY MANAGEMENT STANDARD**

**EDITION 1.1**

**PART 9**

**COPYRIGHT © 2013 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.**

**PAGE 59**

# ISO IEC 27001 2013 TRANSLATED INTO PLAIN ENGLISH

## 9. EVALUATION REQUIREMENTS IN PLAIN ENGLISH

60	Implement your internal ISMS audit program.	TODD	DONE	
61	Define the scope for each internal audit.	TODD	DONE	
62	Specify audit criteria for each internal audit.	TODD	DONE	
63	Select impartial and objective internal auditors.	TODD	DONE	
64	Carry out regular internal information security audits.	TODD	DONE	
65	Report your internal audit results to management.	TODD	DONE	
66	Maintain your internal ISMS audit program.	TODD	DONE	
67	Maintain documents that can prove that you've implemented your internal ISMS audit program.	TODD	DONE	
68	Maintain a record of internal audit implementation.	TODD	DONE	These records are "documented information". Therefore they must be controlled (per 7.5.3).
69	Control records that show audits are being done.	TODD	DONE	
70	Maintain a record of internal audit results.	TODD	DONE	These records are "documented information". Therefore they must be controlled (per 7.5.3).
71	Control your record of internal audit results.	TODD	DONE	

### 9.3 REVIEW PERFORMANCE OF YOUR ORGANIZATION'S ISMS AT PLANNED INTERVALS

72	Establish a management review process.	TODD	DONE	A <i>review</i> is an activity. Its purpose is to figure out how well the thing being reviewed is capable of achieving established objectives. <i>Reviews</i> ask the following question: is the subject of the review a suitable, adequate, effective, and efficient way of achieving your organization's objectives?
73	Use reviews to ensure that your ISMS is still suitable.	TODD	DONE	
74	Use reviews to ensure that your ISMS is still adequate.	TODD	DONE	
75	Use reviews to ensure that your ISMS is still effective.	TODD	DONE	
76	Plan your organization's ISMS review process.	TODD	DONE	
77	Schedule ISMS reviews at planned intervals.	TODD	DONE	
78	Review the performance of your ISMS.	TODD	DONE	
79	Review your risk assessment results.	TODD	DONE	

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

NOV 2013

PLAIN ENGLISH INFORMATION SECURITY MANAGEMENT STANDARD

EDITION 1.1

PART 9

COPYRIGHT © 2013 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.

PAGE 60

# ISO IEC 27001 2013 TRANSLATED INTO PLAIN ENGLISH

## 9. EVALUATION REQUIREMENTS IN PLAIN ENGLISH

80		Review the status of risk treatment plans.	TODO	DONE	
81		Review the status of actions that were taken after previous management reviews.	TODO	DONE	
82		Review security performance feedback.	TODO	DONE	
83		Review information security objectives and achievements.	TODO	DONE	
84		Review monitoring and measurement results, evaluations, and analyses.	TODO	DONE	
85		Review previous nonconformities and the corrective actions that were taken.	TODO	DONE	
86		Review information security audit results.	TODO	DONE	
87		Review information security performance trends.	TODO	DONE	
88		Review feedback from interested parties.	TODO	DONE	
89		Review continual improvement opportunities.	TODO	DONE	
90		Generate management review outputs.	TODO	DONE	
91		Make decisions which take advantage of continual improvement opportunities or which address the need to change your organization's ISMS.	TODO	DONE	
92		Document the results of your management reviews.	TODO	DONE	These records are "documented information". Therefore they must be controlled (per 7.5.3).
93		Maintain and control your management review records.	TODO	DONE	

Consider each task and select a response. If you haven't done it, select *TODO*. If you've already done it, select *DONE*.  
In the spaces below, enter the name and location of your organization, who completed this section, who reviewed it, and the dates.

ORGANIZATION:

YOUR LOCATION:

COMPLETED BY:

DATE COMPLETED:

REVIEWED BY:

DATE REVIEWED:

**NOV 2013**

**PLAIN ENGLISH INFORMATION SECURITY MANAGEMENT STANDARD**

**EDITION 1.1**

**PART 9**

**COPYRIGHT © 2013 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.**

**PAGE 61**