

ISO IEC 27001 2005 TRANSLATED INTO PLAIN ENGLISH

8. IMPROVE YOUR INFORMATION SECURITY MANAGEMENT SYSTEM

8.1 CONTINUALLY IMPROVE YOUR ISMS

1	Improve the effectiveness of your ISMS.	TODO	DONE	
2	Use your information security policy to continually improve the effectiveness of your ISMS.	TODO	DONE	
3	Use your information security objectives to continually improve the effectiveness of your ISMS.	TODO	DONE	
4	Use your information security audit results to continually improve the effectiveness of your ISMS.	TODO	DONE	
5	Use your management reviews to continually improve the effectiveness of your ISMS.	TODO	DONE	See section 7 for more detail.
6	Use your corrective actions to continually improve the effectiveness of your ISMS.	TODO	DONE	
7	Use your preventive actions to continually improve the effectiveness of your ISMS.	TODO	DONE	
8	Use your monitoring process to continually improve the effectiveness of your ISMS.	TODO	DONE	
9	Analyze monitored events in order to identify ways to improve the effectiveness of your ISMS.	TODO	DONE	

8.2 CORRECT ACTUAL ISMS NONCONFORMITIES

10	Establish a corrective action procedure to prevent the <i>recurrence</i> of actual nonconformities.	TODO	DONE	The term <i>recurrence</i> is used because the nonconformity has already occurred.
11	Make sure that your corrective action procedure expects you to identify <i>actual nonconformities</i> .	TODO	DONE	<i>Corrective actions</i> are steps that are taken to address existing nonconformities and make improvements. <i>Corrective actions</i> deal with <i>actual nonconformities</i> (problems), ones that have already occurred. They solve existing problems by removing their causes. In general, the <i>corrective action</i> process can be thought of as a problem solving process.
12	Make sure that your corrective action procedure expects you to identify the causes of nonconformities.	TODO	DONE	
13	Make sure that your procedure expects you to evaluate whether you need to take action.	TODO	DONE	
14	Make sure that your procedure expects you to develop corrective actions when they are needed.	TODO	DONE	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	
MAR 2006	COPYRIGHT © 2006 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.		VERSION 1.0
PART 8	IMPROVE YOUR INFORMATION SECURITY MANAGEMENT SYSTEM		PAGE 49

ISO IEC 27001 2005 TRANSLATED INTO PLAIN ENGLISH

8. IMPROVE YOUR INFORMATION SECURITY MANAGEMENT SYSTEM

15	Make sure that your procedure expects you to prevent the <i>recurrence</i> of actual nonconformities.	TODO	DONE	
16	Make sure that your corrective action procedure expects you to eliminate the causes of your organization's nonconformities.	TODO	DONE	
17	Make sure that your procedure expects you to record the results of any corrective actions taken.	TODO	DONE	Also see section 4.3.3.
18	Make sure that your procedure expects you to review the results of any corrective actions taken.	TODO	DONE	
19	Document your corrective action procedure.	TODO	DONE	
20	Implement your corrective action procedure.	TODO	DONE	Whenever ISO IEC 27001 wants you to develop a " <i>documented procedure</i> " it also wants you to establish, implement, and maintain that procedure (per 4.3.1 Note 1).
21	Use your organization's corrective action procedure to identify nonconformities.	TODO	DONE	
22	Use your organization's corrective action procedure to identify causes.	TODO	DONE	
23	Use your procedure to evaluate whether or not you need to take corrective action.	TODO	DONE	
24	Use your procedure to develop corrective actions whenever corrective actions are actually needed.	TODO	DONE	
25	Use your procedure to take corrective actions.	TODO	DONE	
26	Use your procedure to prevent the <i>recurrence</i> of actual nonconformities.	TODO	DONE	
27	Use your procedure to eliminate the causes of actual nonconformities.	TODO	DONE	
28	Use your procedure to record the results of any corrective actions taken.	TODO	DONE	
29	Use your procedure to review the corrective actions that have been taken.	TODO	DONE	
30	Maintain your corrective action procedure.	TODO	DONE	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	
MAR 2006	COPYRIGHT © 2006 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.		VERSION 1.0
PART 8	IMPROVE YOUR INFORMATION SECURITY MANAGEMENT SYSTEM		PAGE 50

ISO IEC 27001 2005 TRANSLATED INTO PLAIN ENGLISH

8. IMPROVE YOUR INFORMATION SECURITY MANAGEMENT SYSTEM

8.3 PREVENT POTENTIAL ISMS NONCONFORMITIES

31	Establish a preventive action procedure to prevent the <i>occurrence</i> of potential nonconformities.	TODO	DONE	The term <i>occurrence</i> is used because the nonconformity has not yet occurred.
32	Make sure that your preventive action procedure expects you to identify <i>potential nonconformities</i> .	TODO	DONE	<p><i>Preventive actions</i> are steps that are taken to avoid potential nonconformities and make improvements. <i>Preventive actions</i> address <i>potential nonconformities</i> (problems), ones that haven't yet occurred. <i>Preventive actions</i> prevent the <i>occurrence</i> of problems by removing their causes. In general, the preventive action process can be thought of as a risk management process.</p> <p>It's often cheaper to prevent potential nonconformities than to correct them after they've occurred.</p>
33	Make sure that your preventive action procedure expects you to identify significant changes in your organization's information security risk.	TODO	DONE	
34	Make sure that your procedure expects you to identify the causes of potential nonconformities.	TODO	DONE	
35	Make sure that your procedure expects you to evaluate whether or not your organization needs to take preventive action.	TODO	DONE	
36	Make sure that your procedure expects you to develop preventive actions when they are needed.	TODO	DONE	
37	Make sure that your procedure expects you to use the results of your risk assessment to prioritize your preventive actions.	TODO	DONE	
38	Make sure that your procedure expects you to prevent the <i>occurrence</i> of potential nonconformities.	TODO	DONE	
39	Make sure that your procedure expects you to eliminate the causes of potential nonconformities.	TODO	DONE	
40	Make sure that your procedure expects you to record the results of any preventive actions taken.	TODO	DONE	Also see section 4.3.3.
41	Make sure that your procedure expects you to review the results of any preventive actions taken.	TODO	DONE	
42	Document your preventive action procedure.	TODO	DONE	
43	Implement your preventive action procedure.	TODO	DONE	Whenever ISO IEC 27001 wants you to develop a " <i>documented procedure</i> " it also wants you to establish, implement, and maintain that procedure (per 4.3.1 Note 1).
44	Use your organization's preventive action procedure to identify <i>potential nonconformities</i> .	TODO	DONE	

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	
MAR 2006	COPYRIGHT © 2006 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.		VERSION 1.0
PART 8	IMPROVE YOUR INFORMATION SECURITY MANAGEMENT SYSTEM		PAGE 51

ISO IEC 27001 2005 TRANSLATED INTO PLAIN ENGLISH

8. IMPROVE YOUR INFORMATION SECURITY MANAGEMENT SYSTEM

45	Use your organization's preventive action procedure to identify significant changes in your information security risk.	TODO	DONE	
46	Use your preventive action procedure to identify the causes of potential nonconformities.	TODO	DONE	
47	Use your preventive action procedure to evaluate whether or not you need to take preventive action.	TODO	DONE	
48	Use your preventive action procedure to develop preventive actions whenever they are needed.	TODO	DONE	
49	Use the results of your risk assessment to prioritize your preventive actions.	TODO	DONE	
50	Use your procedure to take preventive actions.	TODO	DONE	
51	Make sure that your preventive actions deal with the impact the potential problems could have.	TODO	DONE	
52	Use your preventive action procedure to prevent the <i>occurrence</i> of potential nonconformities.	TODO	DONE	
53	Use your preventive action procedure to eliminate the causes of potential nonconformities.	TODO	DONE	
54	Use your preventive action procedure to record the results of any preventive actions taken.	TODO	DONE	Also see section 4.3.3.
55	Use your preventive action procedure to review the preventive actions that have been taken.	TODO	DONE	
56	Maintain your preventive action procedure.	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, please enter the name and location of your organization, who completed this page, who reviewed it, and the dates.

ORGANIZATION:		YOUR LOCATION:	
COMPLETED BY:		DATE COMPLETED:	
REVIEWED BY:		DATE REVIEWED:	
MAR 2006	COPYRIGHT © 2006 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED.		VERSION 1.0
PART 8	IMPROVE YOUR INFORMATION SECURITY MANAGEMENT SYSTEM		PAGE 52