

## ISO IEC 27001 2005 GAP ANALYSIS TOOL

### 7. ISMS MANAGEMENT REVIEW GAP ANALYSIS QUESTIONNAIRE

#### 7.1 PERFORM MANAGEMENT REVIEWS

|    |  |     |    |   |
|----|--|-----|----|---|
| 1  | Do you carry out management reviews of your ISMS?  | YES | NO | The purpose of a <i>management review</i> is to evaluate the overall performance of an organization's information security management system and to identify improvement opportunities. |
| 2  | Does your management carry out management reviews of your ISMS at planned intervals?             | YES | NO |   |
| 3  | Does your management carry out management reviews of your ISMS at least once a year?             | YES | NO |   |
| 4  | Do you review the performance of your ISMS?  | YES | NO |   |
| 5  | Do you review the ongoing suitability of your ISMS?  | YES | NO |   |
| 6  | Do you review the ongoing adequacy of your ISMS?   | YES | NO |   |
| 7  | Do you review the ongoing effectiveness of the ISMS?   | YES | NO |   |
| 8  | Do you assess whether or not your organization's ISMS should be changed or improved?             | YES | NO |   |
| 9  | Do you assess whether or not your information security policy should be changed or improved?     | YES | NO |   |
| 10 | Do you assess whether or not your information security objectives should be changed or improved? | YES | NO |   |
| 11 | Do you maintain a record of your management reviews?   | YES | NO | Also see section 4.3.3.   |
| 12 | Do you record the results of management reviews?   | YES | NO |   |

#### 7.2 EXAMINE MANAGEMENT REVIEW INPUTS

|    |   |     |    |   |
|----|---|-----|----|---|
| 13 | Do you examine information about your ISMS (inputs)?    | YES | NO | <i>Inputs</i> include products, services, information, documents, reports, records, results, needs, expectations, requirements, complaints, comments, feedback, decisions, measurements, authorizations, plans, solutions, proposals, and instructions. |
| 14 | Do you examine the results of prior management reviews? | YES | NO |   |
| 15 | Do you examine management review follow-up actions?     | YES | NO |   |
| 16 | Do you examine the results of previous ISMS audits?     | YES | NO |   |
| 17 | Do you examine previous ISMS measurement results?       | YES | NO |   |

|               |  |                 |                |
|---------------|--|-----------------|----------------|
| ORGANIZATION: |  | YOUR LOCATION:  |                |
| COMPLETED BY: |  | DATE COMPLETED: |                |
| REVIEWED BY:  |  | DATE REVIEWED:  |                |
| JUN 2006      | COPYRIGHT © 2006 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED. |                 | VERSION 1.0    |
| <b>PART 7</b> | <b>ISMS MANAGEMENT REVIEW GAP ANALYSIS QUESTIONNAIRE</b>                 |                 | <b>PAGE 45</b> |

## ISO IEC 27001 2005 GAP ANALYSIS TOOL

### 7. ISMS MANAGEMENT REVIEW GAP ANALYSIS QUESTIONNAIRE

|    |   |     |    |  |
|----|---|-----|----|--|
| 18 | Do you examine effectiveness measurements results?  | YES | NO |  |
| 19 | Do you examine the status of previous remedial actions?   | YES | NO |  |
| 20 | Do you examine the status of previous corrective actions?   | YES | NO |  |
| 21 | Do you examine the status of previous preventive actions?   | YES | NO |  |
| 22 | Do you examine security issues that were inadequately addressed during the previous risk assessment?  | YES | NO |  |
| 23 | Do you examine security threats that were inadequately addressed during the previous risk assessment? | YES | NO |  |
| 24 | Do you examine vulnerabilities that were inadequately addressed during the previous risk assessment?  | YES | NO |  |
| 25 | Do you examine opportunities to improve your ISMS?  | YES | NO |  |
| 26 | Do you examine recommendations to improve the performance and effectiveness of your ISMS?             | YES | NO |  |
| 27 | Do you examine security feedback from other parties?  | YES | NO |  |
| 28 | Do you examine things that could be used to improve the performance and effectiveness of your ISMS?   | YES | NO |  |
| 29 | Do you examine products that might be used to improve your organization's ISMS?                       | YES | NO |  |
| 30 | Do you examine procedures that might be used to improve your organization's ISMS?                     | YES | NO |  |
| 31 | Do you examine techniques that might be used to improve your organization's ISMS?                     | YES | NO |  |
| 32 | Do you examine changes that might affect your ISMS?   | YES | NO |  |

|               |  |                 |                |
|---------------|--|-----------------|----------------|
| ORGANIZATION: |  | YOUR LOCATION:  |                |
| COMPLETED BY: |  | DATE COMPLETED: |                |
| REVIEWED BY:  |  | DATE REVIEWED:  |                |
| JUN 2006      | COPYRIGHT © 2006 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED. |                 | VERSION 1.0    |
| <b>PART 7</b> | <b>ISMS MANAGEMENT REVIEW GAP ANALYSIS QUESTIONNAIRE</b>                 |                 | <b>PAGE 46</b> |

## ISO IEC 27001 2005 GAP ANALYSIS TOOL

### 7. ISMS MANAGEMENT REVIEW GAP ANALYSIS QUESTIONNAIRE

#### 7.3 GENERATE MANAGEMENT REVIEW OUTPUTS

|    |  |     |    |  |
|----|--|-----|----|--|
| 33 | Do you generate management review decisions and actions (outputs)?   | YES | NO | <i>Outputs</i> include products, services, information, documents, reports, records, results, needs, expectations, requirements, complaints, comments, feedback, decisions, measurements, authorizations, plans, solutions, proposals, and instructions. |
| 34 | Do you generate management review decisions and actions to improve your organization's ISMS?                           | YES | NO |  |
| 35 | Do you generate decisions and actions to improve the effectiveness of your organization's ISMS?                        | YES | NO |  |
| 36 | Do you generate decisions and actions to improve the methods used to measure how effective your security controls are? | YES | NO |  |
| 37 | Do you generate management review decisions and actions to update your organization's ISMS?                            | YES | NO |  |
| 38 | Do you update your risk assessment?  | YES | NO |  |
| 39 | Do you update your risk treatment plan?  | YES | NO |  |
| 40 | Do you generate management review decisions and actions to respond to events that affect your ISMS?                    | YES | NO |  |
| 41 | Do you generate decisions and actions to respond to changes in your business requirements?                             | YES | NO |  |
| 42 | Do you modify your information security procedures in response to changes in business requirements?                    | YES | NO |  |
| 43 | Do you modify your information security controls in response to changes in business requirements?                      | YES | NO |  |
| 44 | Do you generate decisions and actions to respond to changes in business processes?                                     | YES | NO |  |
| 45 | Do you modify your information security procedures in response to changes in business processes?                       | YES | NO |  |

|               |  |                 |                |
|---------------|--|-----------------|----------------|
| ORGANIZATION: |  | YOUR LOCATION:  |                |
| COMPLETED BY: |  | DATE COMPLETED: |                |
| REVIEWED BY:  |  | DATE REVIEWED:  |                |
| JUN 2006      | COPYRIGHT © 2006 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED. |                 | VERSION 1.0    |
| <b>PART 7</b> | <b>ISMS MANAGEMENT REVIEW GAP ANALYSIS QUESTIONNAIRE</b>                 |                 | <b>PAGE 47</b> |

## ISO IEC 27001 2005 GAP ANALYSIS TOOL

### 7. ISMS MANAGEMENT REVIEW GAP ANALYSIS QUESTIONNAIRE

|    |  |   |     |    |  |
|----|--|---|-----|----|--|
| 46 |  | Do you modify your information security controls in response to changes in business processes?        | YES | NO |  |
| 47 |  | Do you generate decisions and actions to respond to changes in your security requirements?            | YES | NO |  |
| 48 |  | Do you modify your information security procedures in response to changes in security requirements?   | YES | NO |  |
| 49 |  | Do you modify your information security controls in response to changes in security requirements?     | YES | NO |  |
| 50 |  | Do you generate decisions and actions to respond to changes in legal requirements?                    | YES | NO |  |
| 51 |  | Do you modify your information security procedures in response to changes in legal requirements?      | YES | NO |  |
| 52 |  | Do you modify your information security controls in response to changes in legal requirements?        | YES | NO |  |
| 53 |  | Do you generate decisions and actions to respond to changes in your regulatory requirements?          | YES | NO |  |
| 54 |  | Do you modify your information security procedures in response to changes in regulatory requirements? | YES | NO |  |
| 55 |  | Do you modify your information security controls in response to changes in regulatory requirements?   | YES | NO |  |
| 56 |  | Do you generate decisions and actions to respond to changes in your contractual obligations?          | YES | NO |  |
| 57 |  | Do you modify your information security procedures in response to changes in contractual obligations? | YES | NO |  |

|               |  |                 |                |
|---------------|--|-----------------|----------------|
| ORGANIZATION: |  | YOUR LOCATION:  |                |
| COMPLETED BY: |  | DATE COMPLETED: |                |
| REVIEWED BY:  |  | DATE REVIEWED:  |                |
| JUN 2006      | COPYRIGHT © 2006 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED. |                 | VERSION 1.0    |
| <b>PART 7</b> | <b>ISMS MANAGEMENT REVIEW GAP ANALYSIS QUESTIONNAIRE</b>                 |                 | <b>PAGE 48</b> |

## ISO IEC 27001 2005 GAP ANALYSIS TOOL

### 7. ISMS MANAGEMENT REVIEW GAP ANALYSIS QUESTIONNAIRE

|    |  |  |     |    |  |
|----|--|--|-----|----|--|
| 58 |  | Do you modify your information security controls in response to changes in contractual obligations?    | YES | NO |  |
| 59 |  | Do you generate decisions and actions to respond to changes in your organization's levels of risk?     | YES | NO |  |
| 60 |  | Do you modify your information security procedures in response to changes in your levels of risk?      | YES | NO |  |
| 61 |  | Do you modify your information security controls in response to changes in your levels of risk?        | YES | NO |  |
| 62 |  | Do you generate decisions and actions to respond to changes in your risk acceptance criteria?          | YES | NO |  |
| 63 |  | Do you modify your information security procedures in response to changes in risk acceptance criteria? | YES | NO |  |
| 64 |  | Do you modify your information security controls in response to changes in risk acceptance criteria?   | YES | NO |  |
| 65 |  | Do you generate management review decisions and actions to address ISMS resource needs?                | YES | NO |  |

Consider each question and select a response. A YES answer means you're in compliance, while a NO answer points to a security gap. NO answers point to the gaps that exist between the ISO IEC 27001 2005 standard and your organization's ISMS. In order to comply with this standard, you must fill each one of these gaps.

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:  |                |
| JUN 2006      | COPYRIGHT © 2006 BY PRAXIOM RESEARCH GROUP LIMITED. ALL RIGHTS RESERVED. |                 | VERSION 1.0    |
| <b>PART 7</b> | <b>ISMS MANAGEMENT REVIEW GAP ANALYSIS QUESTIONNAIRE</b>                 |                 | <b>PAGE 49</b> |