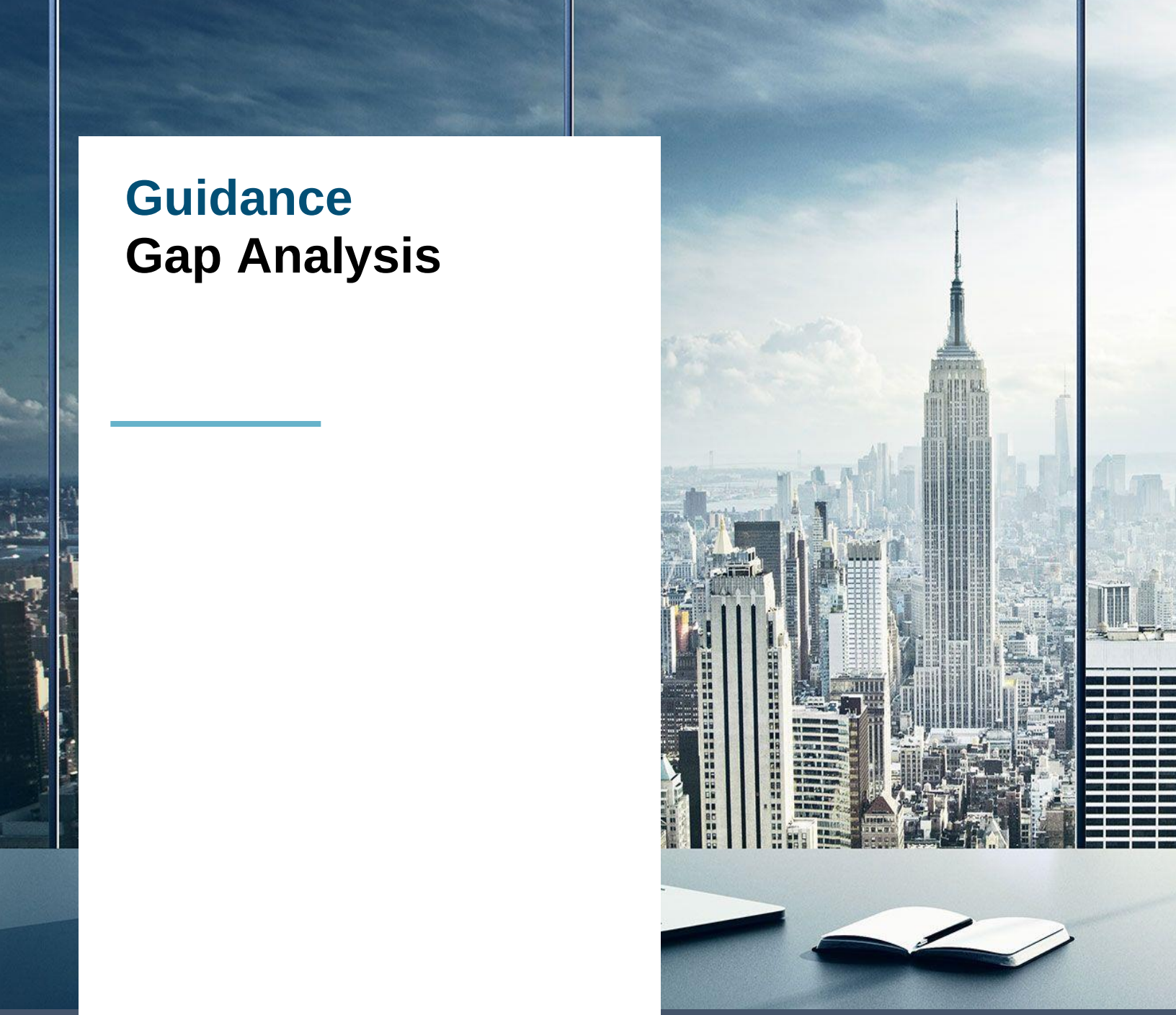

Guidance
Gap Analysis

ISO 27001

COMPANY NAME

Authored by: Your Name

Online ISO

Do we comply?	*Y/N*
4.0 CONTEXT OF THE ORGANISATION	
4.1 Understanding The Organisation And Its Context	
1. Have you determined the purpose(s) of the ISMS?	
2. Have you determined the internal and external issues that are relevant to the ISMS's purpose?	
3. Have you determined how internal and external issues could influence the ISMS's ability to achieve its intended outcomes?	
4.2 Understanding The Needs And Expectations Of Interested Parties	
4. Have you determined interested parties?	
5. Does the list of all of interested parties' requirements exist?	
6. Is the scope documented with clearly defined boundaries and applicability?	
4.4 Information Security Management System	
7. Have you established, documented, implemented, maintained, and continually improved an information security management system per ISO 27001 requirements?	
5.0 LEADERSHIP	
5.1 Leadership And Commitment	
8. Are the general ISMS objectives compatible with the strategic direction?	
9. Does management ensure the necessary ISMS resources are available as needed?	
10. Does management ensure that ISMS achieves its intended outcomes?	
5.2 POLICY	
11. Does an Information Security Policy exist with included objectives or a framework for setting objectives?	
12. Is the Information Security Policy documented and communicated within the company and to other interested parties?	
5.3 ORGANISATIONAL ROLES, RESPONSIBILITIES AND AUTHORITIES	
13. Are roles, responsibilities, and authorities for information security assigned and communicated?	
6.0 PLANNING	
6.1 Actions To Address Risks And Opportunities 6.1.1 General	
14. Are internal and external issues, as well as interested parties' requirements, considered while addressing risks and opportunities?	
6.1.2 Information Security Risk Assessment	
15. Is there a documented process to identify information security risks, including the risk acceptance criteria and criteria for risk assessment?	
6.1.3 Information Security Risk Treatment	
16. Is the risk treatment process documented, including the risk treatment options and how to create a Statement of Applicability?	
6.2 Information Security Objectives And Planning To Achieve Them	
17. Are information security objectives and targets established at relevant functions of the organisation, measured where practical, and consistent with the information security policy?	

Do we comply?	*Y/N*
18. Is there a plan, or group of plans, in place to achieve the information security objectives and targets including designated responsibility, evaluation method, and the means & timeframe for the plan(s)?	
7.0 SUPPORT	
7.1 Resources	
19. Are adequate resources provided for all the elements of the ISMS?	
7.2 Competence	
20. Is appropriate competence assessed, and training provided where needed, for personnel doing tasks that can affect the information security? Are records of competences maintained?	
7.3 Awareness	
21. Is the personnel aware of the Information Security Policy, of their role, and consequences of not complying with the rules?	
22. Is there a process for communication related to information security, including the responsibilities and what to communicate, to whom and when?	
7.5 Documented Information	
23. Does the documentation of the ISMS include the Information Security Policy, objectives & targets, the scope of the ISMS, the main elements and their interaction, documents and records of ISO 27001 and those identified by the company?	
24. Is it ensured that managing of documents and records exists, including who reviews and approves documents, and where and how they are published, stored, and protected?	
25. Is documented information of external origin controlled?	
8.0 OPERATIONS	
8.1 Operational Planning And Control	
26. Does the organisation have the necessary documented information to be confident that its processes are being carried out as planned?	
27. Are planned changes controlled? Are consequences of unplanned changes reviewed to identify mitigation actions if necessary?	
28. Are outsourced processes identified and controlled?	
8.2 Information Security Risk Assessment	
29. Are the risks, their owners, likelihood, consequences, and the level of risk identified? Are these results documented?	
8.3 Information Risk Treatment	
30. Does a risk treatment plan exist, approved by risk owners?	
31. Is there a documented list with all controls deemed as necessary, with proper justification and implementation status?	
9.0 PERFORMANCE EVALUATION	
9.1 Monitoring, Measurement, Analysis And Evaluation	
32. Is it defined what needs to be measured, by which method, who is responsible, who will analyse and evaluate the results?	
33. Are the results of measurement documented, analysed, and evaluated by responsible persons?	

Do we comply?	*Y/N*
9.2 INTERNAL AUDIT	
34. Does an audit program exist that defines the timing, responsibilities, reporting, audit criteria, and scope?	
35. Are internal audits performed according to an audit program, results reported through an internal audit report, and relevant corrective actions raised?	
36. Is management review regularly performed, and are the results documented in minutes of the meeting?	
37. Did management decide on all the crucial issues important for the success of the ISMS?	
10.0 IMPROVEMENT	
10.1 Continual Improvement	
38. Is the ISMS continuously adjusted to maintain its suitability, adequacy, and effectiveness?	
10.2 Nonconformity And Corrective Action	
39. Does the organisation react to every nonconformity?	
40. Does the organisation consider eliminating the cause of the nonconformity and, where appropriate, take corrective action?	
41. Are all nonconformities recorded, together with corrective actions?	

Do we comply?	*Y/N*
ANNEX A. **(Note: only the controls marked as applicable in the Statement of Applicability need to be implemented.)**	
A.5 Organizational Controls	
42. Are there published policies, approved by management, to support information security ?	
43. Are information security policies reviewed and updated?	
44. Are all information security responsibilities defined?	
45. Are duties and responsibilities properly segregated considering situations of conflict of interest?	
46. Are contacts with relevant authorities defined?	
47. Are contacts with special interest groups or professional associations defined?	
48. Do projects consider information security aspects?	
49. Are rules for secure handling of mobile devices defined?	
50. Are there rules defining how the organisation's information is protected considering teleworking sites?	
51. Does an inventory of assets exist?	
52. Does every asset in the inventory of assets have a designated owner?	
53. Are rules for handling of information and assets defined?	
54. Are company assets returned by employees and contractors when their employment is terminated?	
55. Are there procedures which define how to label and handle classified information?	
56. Are there procedures which define how to handle assets?	

Do we comply?	*Y/N*
57. Are there procedures which define how to handle removable media in line with the classification rules?	
58. Are there formal procedures for disposing of the media?	
59. Is the media that contains sensitive information protected during transportation?	
60. Is there an access control policy?	
61. Do the users have access only to the resources they are allowed to?	
62. Are access rights provided via a formal registration process?	
63. Is there a formal access control system when logging into information systems?	
64. Are privileged access rights managed with special care?	
65. Are passwords and other secret authentication information provided in a secure way?	
66. Do asset owners periodically check all the privileged access rights?	
67. Are access rights updated when there is a change in the user situation (e.g.: organisational change or termination)?	
68. Are there rules for users on how to protect passwords and other authentication information?	
69. Is the access to information in systems restricted according to the access control policy?	
70. Is secure log-on required on systems according to the Access Control Policy?	
71. Do the password management systems used by the organisation help users to securely manage their authentication information?	
72. Is the use of utility tools controlled and limited to specific employees?	
73. Is the access to source code restricted to authorised persons?	
74. Are security requirements for network services defined, and included in agreements?	
75. Are the networks segregated considering risks and assets classification?	
76. Is the information transfer properly protected?	
77. Do agreements with third parties consider the protection during information transfer?	
78. Are the messages that are exchanged over the networks properly protected?	
79. Does the organization list all the confidentiality clauses that need to be included in agreements with third parties?	
80. Is there a policy on how to treat the risks related to suppliers and partners?	
81. Are relevant security requirements included in the agreements with the suppliers and partners?	
82. Do the agreements with providers and suppliers include security requirements?	
83. Are suppliers regularly monitored?	
84. Are changes involving arrangements and contracts with suppliers and partners taking into account risks and existing processes?	
85. Are requirements for continuity of information security defined?	
86. Do procedures exist that ensure the continuity of information security during a crisis or a disaster?	
87. Is exercising and testing of continuity performed?	
88. Does IT infrastructure have redundancy (e.g.: secondary location) included in its planning and operation?	
89. Are legislative, regulatory, contractual, and other security requirements known?	

Do we comply?	*Y/N*
90. Do procedures exist to protect intellectual property rights?	
91. Are records protected properly?	
92. Is personally identifiable information protected properly?	
93. Are cryptographic controls used properly?	
94. Is information security regularly reviewed by an independent auditor?	
95. Do the managers regularly review if the security policies and procedures are performed properly in their areas of responsibility?	
96. Are information systems regularly reviewed to check their compliance with the information security policies and standards?	
A.6 People Controls	
97. Does the organisation perform background checks on candidates for employment or for contractors?	
98. Are there agreements with employees and contractors that specify information security responsibilities?	
99. Is management actively requiring all employees and contractors to comply with information security rules?	
100. Do employees and contractors attend trainings to better perform their security duties, and do the awareness programs exist?	
101. Does the organisation have a formal disciplinary process?	
102. Are there agreements covering information security responsibilities that remain valid after the termination of employment?	
103. Are incidents managed properly?	
104. Are information security events reported in properly?	
105. Are employees and contractors reporting on security weaknesses?	
106. Are security events assessed and classified properly?	
107. Are procedures on how to respond to incidents documented?	
108. Are security incidents analyzed properly?	
109. Do procedures exist which define how to collect evidence?	
A.7 Physical Controls	
110. Do secure areas that protect sensitive information exist?	
111. Is the entrance to secure areas protected?	
112. Are secure areas located in a protected way?	
113. Are the alarms, fire protection, and other systems installed?	
114. Are working procedures for secure areas defined?	
115. Are delivery and loading areas protected?	
116. Is the equipment properly protected?	
117. Does the equipment have protection against energy variations?	
118. Are the power and telecommunication cables adequately protected?	
119. Is the equipment maintained regularly?	
120.cIs information and equipment removal to outside of the organization premises controlled?	
121. Are the organization assets properly protected when they are not at the organization premises?	

Do we comply?	*Y/N*
122. Is information properly removed from media or equipment that will be disposed of?	
123. Are there rules to protect equipment when not in physical possession of its users?	
124. Is there orientation for users about what to do when they are not present at their workstations?	
A.8 Technological Controls	
125. Do a policy to regulate encryption and other cryptographic controls exist?	
126. Are the cryptographic keys properly protected?	
127. Are operating procedures for IT processes documented?	
128. Are changes that could affect information security strictly controlled?	
129. Are resources monitored and plans made to ensure their capacity to fulfill users' demands?	
130. Are development, testing, and production environments separated?	
131. Are anti-virus software, and other software for malware protection installed and properly used?	
132. Is a backup policy defined and performed properly?	
133. Are relevant events from IT systems logged, and verified periodically?	
134. Are logs protected properly?	
135. Are administrator logs protected properly?	
136. Are clocks on all IT systems synchronized?	
137. Is installation of software strictly controlled?	
138. Are vulnerabilities' information and correction properly managed?	
139. Are there rules to define restrictions of software installation by users?	
140. Are audits of production systems planned and executed properly?	
141. Are security requirements defined for new information systems, or for any changes to them?	
142. Is application information transferred through public networks appropriately protected?	
143. Is transaction information transferred through the public networks appropriately protected?	
144. Are rules for the secure development of software and systems defined?	
145. Are changes to new or existing systems properly controlled?	
146. Are critical applications properly tested after changes made in operating systems?	
147. Are only necessary changes performed to information systems?	
148. Are principles for engineering secure systems applied to the organization system's development process?	
149. Is the development environment properly secured?	
150. Is the outsourced development of systems monitored?	
151. Are security requirements implementation tested during system development?	
152. Are criteria for accepting the systems defined?	
153. Are test data carefully selected and protected?	