**ISO 20000-1:2018 CLIENT GAP ANALYSIS TOOL**

**Instructions For Use**

This gap analysis document provides a simple framework for evaluating your IT service management system against the requirements of ISO 20000-1:2018. It is to be used in conjunction with the NQA ISO20000-1:2018 Gap Guide.

* **Part 1: Annex SL Changes, excluding changes to service management processes (clause 8)**
* **Part 2: ISO 20000-1:2018 Service Management Processes – New & Changed Requirements**
* Please complete each table by recording the evidence acquired from one full internal audit against the requirements of ISO 20000-1:2018.

If you are unable to provide evidence of compliance, you may not be ready to complete the transition to ISO 20000-1:2018. In this case, please inform NQA that you need additional time to prepare for the transition – we will work with you to select a mutually agreeable date to complete the transition.

**Please ensure that this completed document and relevant internal audit records are available to your auditor at the opening meeting of your transition audit**.

Sections marked as ***(Assessor to Complete)*** will be completed by the assessor during the transition audit.

|  |  |
| --- | --- |
| **Client name:** |  |
| **Certificate number:** |  |
| **Date of completion:** |  |

**Part 1: Annex SL Changes, excluding changes to service management processes (clause 8)**

**Tip:** Ensure that these new concepts are implemented in a manner that supports the *Process Approach* and *Risk Based Thinking*.

| **New Concepts** | **Phase** | **Clause** | **Requirement** | **Evidence of Compliance** | ***(Assessor to Complete)***  ***Has the Client demonstrated that they have met the requirements of this clause?*** | | ***(Assessor to Complete)***  ***Comments if required*** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | ***Yes*** | ***No*** |  |
| 4.1 Understanding the organization and its context | Plan | 4.1 | Determine external and internal issues |  | **√** | **X** |  |
| Plan  Check | 4.1 | Determine intended outcome(s) of the SMS |  |  |  |  |
| 4.2 Understanding the needs and expectations of interested parties | Plan | 4.2 | Determine Interested parties |  |  |  |  |
| Plan | 4.2 | Determine the relevant requirements of these interested parties. |  |  |  |  |
| 4.3 Determining the scope of the service management system | Plan | 4.3 | The SMS scope is documented |  |  |  |  |
| 5 Leadership:  5.1 Leadership and commitment | Plan | 5.1 | Top management ensures what constitutes value for the organization and its customers is determined; |  |  |  |  |
|  | Plan | 5.1 | Top management ensures there is control of other parties involved in the service lifecycle; |  |  |  |  |
|  | Plan | 5.1 | Top management ensures the integration of the SMS requirements into the organization’s business processes; |  |  |  |  |
|  |  | 5.1 | Top management ensures |  |  |  |  |
| **6 Planning**  **6.1 Actions to address risks and opportunities** |  | 6.1.1 | Consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the ***risks and opportunities*** that need to be addressed to  a) give assurance that the SMS can achieve its intended outcome(s);  b) prevent, or reduce, undesired effects;  c) achieve continual improvement of the SMS and the services. |  |  |  |  |
|  |  | 6.1.2 | Document risks, including risk related to:   * The organization * Not meeting the service requirements. * The involvement of other parties in the service lifecycle |  |  |  |  |
|  |  | 6.1.2 | Document risk acceptance criteria & approach to be taken for the management of risks. |  |  |  |  |
|  |  | 6.1.3 | Plan actions to address these risks and opportunities and their priorities & evaluate the effectiveness of these actions. |  |  |  |  |
| 6.2 Service management objectives and planning to achieve them;  6.2.1 Establish objectives |  | 6.2.1 | Establish service management objectives **at relevant functions and levels** |  |  |  |  |
| 6.2.2 Plan to achieve objectives |  | 6.2.2 | Determination (when planning objectives)of what will be done, what resources are required, who will be responsible, when it will be completed how the results will be evaluated. |  |  |  |  |
| 6.3 Plan the service management system |  | 6.3 | The organisation has created, implemented and maintained a service management plan shall including or containing a reference to a list of services |  |  |  |  |
| 7 Support of the service management system; 7.3 Awareness |  | 7.3 | Persons doing work under the organisation’s control are aware of their contribution to the effectiveness of the SMS, including the benefits of improved performance |  |  |  |  |
| 7.4 Communication |  | 7.4 | Determine internal and external communication relevant to the SMS and the services including: a) on what it will communicate, b) when to communicate, c) with whom to communicate, d) how to communicate, e) who will be responsible for the communication. |  |  |  |  |
| 7.5 Documented information;  7.5.3 Control of documented information |  | 7.5.3 | Documented information required by the SMS and ISO20000-1:2018 is available and suitable for use, where and when it is needed |  |  |  |  |
|  |  |  | Documented information required by the SMS and ISO20000-1:2018 is adequately protected (e.g. from loss of confidentiality, improper use or loss of integrity). |  |  |  |  |
| 7.5.4 Service management system documented information |  |  | The documented information for the SMS shall include: |  |  |  |  |
|  |  |  | scope of the SMS; |  |  |  |  |
|  |  |  | policy and objectives for service management; |  |  |  |  |
|  |  |  | service management plan |  |  |  |  |
|  |  |  | change management policy, information security policy and service continuity plan(s); |  |  |  |  |
|  |  |  | processes of the organization’s SMS |  |  |  |  |
|  |  |  | service requirements |  |  |  |  |
|  |  |  | service catalogue(s) |  |  |  |  |
|  |  |  | service level agreement(s) (SLA) |  |  |  |  |
|  |  |  | ***contracts with external suppliers*** |  |  |  |  |
|  |  |  | ***agreements with internal suppliers or customers acting as a supplier*** |  |  |  |  |
|  |  |  | procedures that are required by ISO20000-1:2018 |  |  |  |  |
| 7.6 Knowledge |  |  | (Note: Knowledge is specific to the organization, its SMS, services and interested parties) |  |  |  |  |
|  |  |  | The organization shall determine and maintain the knowledge necessary to support the operation of the SMS and the services |  |  |  |  |
|  |  |  | The knowledge shall be relevant, usable and available to appropriate persons |  |  |  |  |
| 9 Performance evaluation;  9.3 Management review |  |  | The management review shall include consideration of:  changes in external and internal issues that are relevant to the SMS;  information on the performance and effectiveness of the SMS, including trends in monitoring and measurement results |  |  |  |  |
| 9.4 Service reporting |  |  | Less detailed … |  |  |  |  |
| 10 Improvement;  10.1 Nonconformity and corrective action |  |  | When a nonconformity occurs, the organization shall determine if similar nonconformities exist, or could potentially occur; |  |  |  |  |
| 10.2 Continual improvement |  |  | Evaluation criteria shall include alignment of the improvement with service management objectives. |  |  |  |  |

**Notes:**

**Part 2: ISO 20000-1:2018 Service Management Processes – New & Changed Requirements**

Tip: ensure that you can demonstrate that each requirement of ISO 20001-1:2018 has been addressed within the SMS.

Multi-site organisations should ensure that the requirements have been considered for all relevant locations, especially where such locations have unique circumstances or different services/contracts/SLAs/resource models/toolsets.

| **ISO 20001-1:2018** | **ISO 20000-1:2011 Cross Reference and the significant changes from the 2011 version** | **Evidence to support compliance** | ***(Assessor to Complete)***  ***Has the Client Demonstrated they have Met the requirements of this clause?*** | | ***(Assessor to Complete)***  ***Comments if Required*** |
| --- | --- | --- | --- | --- | --- |
|  | | | ***Yes*** | ***No*** |  |
| 8 Operation of the service management system |  |  |  |  |  |
| 8.1 Operational planning and control | 4.1.4 Management representative  4.2 Governance of processes operated by other parties  4.5.3 Implement and operate the SMS (Do)  9.2 Change management  The organization shall control planned changes **to the SMS** and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary |  |  |  |  |
| 8.2.1 Service delivery | 4.5.3 Implement and operate the SMS) Determine the criticality of services based on the needs of the organization, customers, users and other interested parties |  |  |  |  |
| 8.2.3 Control of parties involved in the service lifecycle | 4.2 Governance of processes operated by other Parties  5.2 Plan new or changed services  The organization shall determine and apply criteria for the evaluation and selection of other parties involved in the service lifecycle. Other parties can be an external supplier, an internal supplier or a customer acting as a supplier |  |  |  |  |
| 8.2.4 Service catalogue management | 6.1 Service catalogue management  The service catalogue(s) shall include information for the organization, customers, users and other interested parties to **describe the services, their intended outcomes** and dependencies between the services. |  |  |  |  |
| 8.2.6 Configuration management | **9.1 Configuration management (note: this clauses refers to configuration information – there are no references to CMDB)**  Services shall be classified as CIs. |  |  |  |  |
|  | Configuration information shall be recorded to a level of detail appropriate to the criticality and type of services |  |  |  |  |
| 8.3 Relationship and agreement | 6.1 Service level management  6.2 Service reporting  7 Relationship processes |  |  |  |  |
|  |  |  |  |  |  |
| 8.5.1.2 Change management initiation | 5.1 Design and transition of new or changed services    9.2 General Change management  Requests for change, including proposals to add, remove or transfer services, shall be recorded and classified. In particular:  e) transfer of an existing service from the organization to a customer or other party;  f) transfer of an existing service from a customer or other party to the organization. |  |  |  |  |
| 8.5.1.3 Change management activities | 6.3.2 Service continuity and availability plans 6.6.3 Service continuity and availability monitoring  and testing  9.2 Change management  9.3 Release and deployment management  Decision making shall also consider potential impacts of the change on:   1. existing services 2. customers, users and other interested parties; 3. policies and plans required by this document; 4. capacity, service availability, service continuity and information security 5. other requests for change, releases and plans for deployment. |  |  |  |  |
| 8.6.1 Incident management | 6.2 Service reporting  8.1 Incident and service request management  Records of incidents shall be updated with actions taken including their **resolution (now an explicit requirement)** |  |  |  |  |
| 8.6.2 Service request management | 6.2 Service reporting  8.1 Incident and service request management  Records of service requests shall be updated with actions taken including actions for their **closure (now an explicit requirement)** |  |  |  |  |
| 8.6.3 Problem management | 8.2 Problem management  Records of problems shall be updated with actions taken including for their **closure** |  |  |  |  |
| 8.7.1 Service availability management | 6.3 Service continuity and availability management  Availability plan requirement is dropped BUT availability requirements *shall be documented* |  |  |  |  |
| 8.7.3.2 Information security controls | 6.6.2 Information security controls  **At planned intervals**, the information security risks to the SMS and the services shall be assessed and documented |  |  |  |  |
| 8.7.3.2 Information security controls | 6.6.2 Information security controls  Implement information security controls to address information security risks related to external organizations. |  |  |  |  |
| 8.7.3.3 Information security incidents | 6.6.2 Information security controls  The requirement for IS incidents to berecorded/classified/prioritised/resolved/Closed & analysed/reviewed remains but the **requirement to manage them using the incident management procedure is dropped**. |  |  |  |  |

**Areas for further**