Roles, Responsibilities and Authorities

For the support of ISO/IEC 20000-1, ISO 9001 and ISO/IEC 27001 certifications in [Company]

# General Structure

*[Add an org chart if this helps understanding the remainder of this document; a graphical overview of roles and interactions may be helpful as well]*

# Role Descriptions

## [Top Manager]

**Role Description**

The [Top Manager] is accountable overall for the operational, tactical and strategic direction of the [COMPANY] organisation. The Managing Director is considered “Top Management” in the context of the ISO standards for the whole organisation.

**Key Responsibilities**

* Sign off policies, processes, plans and resources for the design, implementation, operation and improvement of the organisation’s QMS and ISMS.
* Development of strategies and objectives for Quality and Information Security Management within EMEA Managed Service Operations.

**Authorities**

* End-to-end direction across the whole organisation in all matters related to the operation of the business, resources, and Quality and Information Security.

## [Department Manager]

**Role Description**

The [Department Manager] is accountable overall for the operational, tactical and strategic direction of the own team, part of the [COMPANY] organisation. The [Department Manager] is considered “Top Management” in the context of the ISO standards for the own team.

**Key Responsibilities**

* Sign off policies, processes, plans and resources for the design, implementation, operation and improvement of the local team’s Quality and Information Security operations.
* Development of strategies and objectives for Quality and Information Security Management within the local team.

**Authorities**

* Direction across the own team in all matters related to the operation of the business, resources, and Quality and Information Security.

## Quality and Information Security Manager

**Based at:** [Location]

**Position reports to:** Managing Director [COMPANY]

**FTE:** ~0.5 FTE

**Role description**

The Information Security and Quality Control Manager scope is the [COMPANY] organisation in [Locations].

The purpose of the function is to support participating departments with implementing quality and information security by using systems based on the ISO 9000 and ISO/IEC 27000 series of standards. Additionally, the Manager is a member of the operational organisations’ management teams and interfaces with all organisations outside of [COMPANY].

**Key Responsibilities**

* Leadership and direction for a matrix-team of Information Security & Quality Management Representatives.
* Lead the design, implementation, operation and maintenance of the Information Security Management System (ISMS) based on the ISO 27000 series standards as well as the related corporate standards, including certification against ISO 27001.
* Lead the design, implementation, operation and maintenance of the Quality Management System (QMS) based on the ISO 9000 series standards as well as the related corporate standards, including certification against ISO 9001.
* Drive global operations compliance in accordance with company policies, business requirements, laws and regulations.
* Ensure a balanced approach, taking into account both security and commercial requirements.
* Ensure compliance with external/customer requirements and specifications within global operations.
* Keep up to date with best practice and advancements with regard to Industry Standards and applicable technologies.
* Primary information security and quality management contact for [COMPANY] in EMEA
* Support departments in the effort to successfully complete internal and external compliance audits.
* Support the departmental representatives performing their Quality and Information Security role.
* Provide strategic direction on information security management and quality management for the organisation.

**Working relationships**

* Work with participating departments’ senior management, information security officers and quality management representatives on local implementations of the QMS and ISMS.
* Work with and co-ordinate audits together with the Global Quality Management Team.
* Liaise with relevant parties to identify what impact system, process and procedural changes will have on the organisation in relation to the ISMS & QMS and advice prior to implementation.
* Liaise with the BCEM team with regard to disaster recovery plans and the management of business continuity.
* Within the scope of the ISMS and QMS, liaise with internal suppliers such as HR, IT, Facilities, Legal, etc.
* Responsible for the identification, classification, treatment and resolution of threats.

**Authorities**

* Authority to guide and direct the organisation in matters relating to Quality and Information Security Management on behalf of the Managing Director.

**Technical expertise and qualifications**

|  |  |
| --- | --- |
|  **Qualifications and Experience** | **Essential or Desired** |
| Knowledge in Service Management, Quality Management, Information Security Management, business compliance and security standards e.g. Risk Management & IT Governance, Threat & Vulnerability Management, Security Policy Development or Information Security Governance | **E** |
| ITIL 2011 Expert certified | **E** |
| Extensive Knowledge of ISO/IEC 20000-1, preferably certified | **E** |
| Extensive Knowledge of ISO 9001, preferably certified | **E** |
| Extensive Knowledge of ISO/IEC 27001, preferably certified | **E** |
| Project Management skills or experience in successful delivery of complex projects | **E** |
| Strong communication skills both written and spoken | **E** |
| Background in an operational environment | **D** |
| Detailed knowledge and experience in dealing with large complex (Managed) services solutions | **D** |
| Detailed knowledge of the departmental services, processes and procedures | **D** |

## Compliance Management Representative

**Based at:** [Location]

**Position reports to:** [Department Manager]

**Position reports with a dotted line to:** Quality and Information Security Manager

**FTE:** On average 0.1 FTE per department

**Role description**

Acts as the departmental procedural expert and representative on the departments’ information security and quality management system.

Working closely together with the [Company] Quality and Service Improvement Manager and peers in other global operations departments in order to implement, certify and manage departmental specific industry standard and company policy requirements.

**Key responsibilities and accountabilities:**

* Assist with the implementation of Industry Standard Management Systems, including (but not restricted to) ISO 9001 and ISO/IEC 27001 within the respective department.
* Assist with co-ordination and facilitating departmental ISO certification.
* Manage local non-conformities and resolve within the required timescales.
* Host and document Management System Reviews.
* Provide and present monthly status reports to global operation information security & quality control manager.
* Ensure departmental compliance with company requirements utilizing company policies, procedures, and Code of Conduct as a framework.
* Represent the department during internal, external and customer audits.
* Assist with contract preparation (pre-sales) and the finalisation process in relation to non-standard security /quality requirements.
* Ensure departmental compliance with external customer requirements and specifications.
* Liaise with various internal and external organisations and counterparts on departmental “industry” or “company standard” compliance matters.
* Apprise Quality Manager and local management of potential issues and discuss new direction and requirements prior to taking action.
* Provide expertise, coaching and training to departmental employees and management when needed.
* Responsible for the identification, classification, treatment and resolution of threats at the local team’s level.

**Authorities**

* Authority to guide and direct the local team in matters relating to Quality and Information Security Management on behalf of the Quality and Information Security Manager or the team’s [Department Manager].

**Key skills, qualifications & experience:**

|  |  |
| --- | --- |
|  **Qualifications and Experience** | **Essential or Desired** |
| Knowledge in Quality Management, Information Security Best Practices, business compliance and security standards e.g. Risk Management & IT Governance, Threat & Vulnerability Management, Security Policy Development or Information Security Governance | **E** |
| ITIL 2011 Foundation certified | **E** |
| Knowledge of ISO/IEC 20000-1, preferably certified | **E** |
| Knowledge of ISO 9001, preferably certified | **E** |
| Knowledge of ISO/IEC 27001, preferably certified | **E** |
| Project Management skills or experience in successful delivery of complex projects. | **D** |
| Strong communication skills both written and spoken | **D** |
| Background in an operational environment | **D** |
| Detailed knowledge and experience in dealing with large complex (Managed) services solutions | **D** |
| Detailed knowledge of the departmental services, processes and procedures | **D** |

**Revision Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comments** |
| 1.0 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Approved By** | **Team/Function** |
| 1.0 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |