

Royal Impact Certification Ltd.

Application Form for ISMS / ITSMS Certification

(Also fill Annexure A of this form)

1	Client Reference Number:
2	Organization Name:
3	Legal Status:
4	Authorized Representative:
5	Contact Information (Mobile: / Phone No: / Email: / Website Address):
6	Standards required:
7	Type of audit (single or integrated):
8	Proposed Scope of Certification:
9	Complete Correspondence Address with Pin Code:
10	Total No. of Sites (If more than 1 site then all addresses of all sites to be covered by this certification):
11	No. of Shifts at each site:
12	No. of Employees – Full Time: / Part Time: / Temporary at each site in each shift:
13	Significant Business Processes & Products / Services:
14	Legal / Statutory Requirements:
15	Language Spoken:
16	Outsourced Processes:
17	Do you consider any ISMS / ITSMS related information confidential or sensitive which cannot be made available for review by the audit team? If yes provide details:
18	Have you hired Services of Consultant? If yes provide details:
19	Details of Registration already held:
20	Status of ISO 27001 documentation and its implementation:
21	Are you ready to allow access to RICL audit team to internal audit reports and reports of independent reviews of information security? Note: If answer is no then we cannot process your application for certification.
22	Have you conducted at least one management review and one internal ISMS audit covering the scope of certification post system implementation? Note: If answer is no then we cannot process your application for certification.

23	Signed By (with applicant stamp): Date:
----	--

For Office Use	Remarks	Initials of receiving authority
Application received and forwarded for review		

Annexure A

ISMS / ITSMS Application for Certification

1. Does your company have a documented system which fully addresses requirements of ISO 27001:2013 (including Statement of Applicability) / ISO 20000-1:2018?
2. Number of critical assets:
3. Number of processes and services:
4. Number of Contract Staff:
5. Number of Users:
6. Number of Disaster Recovery (DR) sites:
7. Number of Servers:
8. Number of Application Development & Maintenance Staff:
9. Extent and diversity of technology utilized:
 - Highly standardized environment with low diversity (few IT-platforms, servers, databases etc)
 - Standardized but diverse IT platforms, servers, databases, networks etc
 - High diversity of complexity of IT
10. Previously demonstrated performance of the ISMS / ITSMS
 - Recently certified or not certified but ISMS / ITSMS fully implemented over several audit and improvement cycles
 - Recent surveillance audit or not certified but partially implemented ISMS / ITSMS
 - No certification and no recent audits or ISMS / ITSMS is new and not fully established
11. Applicability of sector specific risk
 - Low risk business without regulatory requirements
 - High regulatory requirements
 - High risk business with (only) limited regulatory requirements

12. Extent of outsourcing and third-party arrangements:

- no outsourcing and little dependency on suppliers
- well-defined, managed and monitored outsourcing arrangements
- outsourcer has a certified ISMS / ITSMS
- relevant independent assurance reports are available
- several partly managed outsourcing arrangements
- high dependency on outsourcing or suppliers with high impact
- unknown amount or extent of outsourcing or several unmanaged outsourcing arrangements

13. Extent of information system development:

- no in-house system development or use of standardized software platforms
- use of standardized software platforms with complex configuration or highly customized software or some development activities (in- house/outsourced)
- extensive internal software development activities with several ongoing projects for important business purposes

14. Are other parties involved in the provision of services for the client? If yes, provide evidence about how they are identified & controlled as specified in ISO/IEC 20000-1?