SECTION F - ISO 27001:2013

Only complete this section if applying for certification against this standard.

1. How long has your management system been in place?

2. Are you aware of any standards, regulations or laws with which your company or industry must comply? If so list these below.

Legal (e.g. Data Protection Act, Computer Misuse Act etc):

Regulatory (e.g. PCI DSS, Information Governance Statement of Compliance (IG SoC)):

3. Risk level & complexity:

Type	Criteria	Examples	Yes	No	Comments
Government Classifcation	Information handled includes government classification at or above secret.	E.g. military bases, defence supply chain, government departments.			
Nature of information managed	Nature of information held would result in a breach or loss having material financial, personal or reputational impact to any interested party. Information handled includes: • Customers, end users, staff contractors or others sensitive personal information e.g. health records or financial information • Intellectual property (e.g. designs, software source code)	E.g. Solicitors, law firms, banks, insurers, credit agencies (regulated by FCA), organizations providing payroll services or pension administration etc.			
Volume of data managed - aggregated data sets	Information held includes a large set of sensitive personal information that could be used for identity theft or fraud. This can include individuals' usernames and passwords used to access web portals or other systems .	E.g. E-commerce websites, utility companies, online payment websites, organizations collecting individual's data via web portals, organizations processing and analysing customer data.			
Complexity of technology used	Technology used includes a diverse or complex infrastructure: many servers (>100 physical or virtual servers). OR "Bring your own device" (BYOD) is permitted.	E.g. Large IT infrastructure, many servers, multiple different platforms, any organization permitting BYOD ("bring your own device") is included in this criterion, regardless of size.			
Regulation	Your organization is regulated (e.g. regulated by Financial Conduct Authority, Ofcom, Ofsted, Oftel, Solictors Regulatory Authority, Law Society, GMC). OR subject to sector specific rules e.g. Cheque Printers Accreditation Scheme C &CCC Standard 55, UK Health Service's Information Governance Statement of Compliance (IG SoC), ADISA (Asset Disposal and Information Security Alliance), PCI DSS.	E.g. Banking, cheque printers, hospitals, education.			

Type	Criteria	Examples	Yes	No	Comments
Complex tasks	Your organization develops software				
National importance of products/services & high availability requirements	Your services are: Part of critical national infrastructure (e.g. emergency services, communications, financial services, health, transport, utilities) or an essential part of national infrastructure supply chain (e.g. data centre hosting national infrastructure systems) OR potential terrorist target OR Non-availability of your services or product may severely affect the health, well-being, safety or security of people	E.g. broadcasting support providers, utilities (power, water, gas), internet and mobile service providers, air traffic control, examination boards Or banking services, borders and immigration controls, health management systems.			
Supply Chain	Sensitive information is shared with third parties e.g: - Customers'/end users'/staff or others personal information .e.g. outsourced payroll, third party vetting services (criminal records, credit checks) - Intellectual property (designs, source code or other sensitive proprietary information)	E.g. Criminal records, credit checks, outsourced payroll etc.			
Importance of integrity of information	If the information produced by your organization is incorrect or incomplete there is a threat to individual or collective health/wellbeing/safety/ security/miscarriage of justice or risk of fraud	E.g. Organizations such as secure printers (passport/visa printers/ prescription/medical instruction printers), health providers (clinical information/medical record systems), gambling service providers.			
Susceptibility to fraud or targeted disruption	Theft of information (by staff/contractors or others) managed by your organization could result in fraud or targeted disruption, for example: - Theft of personal information by staff working in finance/insurance, call centres, clinics (e.g. theft of customer lists), pharmacies - Hacking of software/website/IT systems	E.g. Organizations susceptible to fraud (e.g. by theft or misuse of data) or heightened risk of attempted fraud.			
Information not available to audit	Do you hold any ISMS related information that cannot be made available for review by the audit team because it contains confidential or sensitive information	N/A			
Clearance	Does the audit team require security clearance to attend the site				

4. At what stage in the implementation of your ISMS are you?

Please indicate your progress in relation to the following phases:

Phase:	Description:	Completed: Yes	Completed: No	Planned completion date:	Required for Stage 1	Required for Stage 2
Step 1	Definition of Policy Statement				Y	Y
Step 2	Defined the scope of your ISMS				Y	Y
Step 3	Completed your Risk Assessment				Y	Y
Step 4	Completed your Risk Treatment Plan document				Y	Y
Step 5	Selected control objectives and controls to be implemented				Y	Y
Step 6	Prepared a Statement of Applicability				Y	Y
Step 7	Completed security awareness training				Preferable	Y
	Completed Internal Audit Of The Isms				Preferable	Y
	Completed management review of the ISMS				Preferable	Y
	Completed and test business continuity plans				Preferable	Y
	Operated the ISMS for at least 3 months				Preferable	Y

(If YES to Step 7 b) how long has your ISMS been implemented?

If you choose to give us any personal information (for example your e-mail address) we will treat this information in line with our privacy notice which can be located here: https://www.nqa.com/en-gb/privacy We will only use the information provided to respond to your enquiry and provide you with any information or materials requested. By submitting this information you are requesting a quote for services from NQA and a subsequent quote letter will be issued to you based on the information provided within this form.