

**R20.28ISMS SRI Registration Survey for**

 **ISO/IEC 27001**

This survey is to be used to obtain a cost proposal for ISO/IEC 27001 Information Security Management System registration services by SRI. **To be used in conjunction with the R20.28 ISMS risk assessment form.**

1. **Company Information**
	1. Company Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	2. Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Proposal to be issued to: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Same address as above? Yes  No  If No, please provide mailing address.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-mail Address: Web Site Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telephone: Fax: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Primary language(s) spoken other than English \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. Which version:  27001:2013 (can use up to 04/30/24: registration decision date)  27001:2022

1. **Complete the following questions to obtain a cost proposal**

**Registration Approach** - Which of the following audit approaches would you like proposed?

|  |  |
| --- | --- |
|  | “**Site**” (a stand alone location **OR** multiple locations in close proximity to one another, operating and addressing all |
|  | requirements of the standard collectively, and issued one certificate) |
|  | “**Multi-site**” (an organization with multiple sites conducting similar operations, similar scopes, operating under the same |
|  | management manual and centrally managed. Issued one certificate listing all locations.)  |
|  | “**Corporate**\*” (all sites, regardless of proximity, are audited collectively and are under one certificate. If the scope/ |
|  | product/processes differ, separate scopes will be required.) |
|  | “**Progressive**\*” (each site audited separately then added to the corporate certificate, when registered. If the scope/ |
|  | product/processes differ, separate scopes will be required.)  |

**Please provide the requested information for each site in the following table:\***

|  |  |  |  |
| --- | --- | --- | --- |
| **Location and Organization (Sites)** **including addresses for all buildings, etc.** | **#****Shifts / times** | **# Employees, incl. temps& contractors fully in scope\*1** | **Products and/or Services** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**\*Attach additional page(s) if more space is necessary**

\*1 Manages the ISMS and/or manages/executes controls identified in Annex A of ISO/IEC 27001

1. Are there any exclusions from the scope of certification (i.e., location, product, service)? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. How many organization users do they support in addition to themselves? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Are there a large number of remote organization users? \_\_\_\_\_\_ Are the systems used 24/7? \_\_\_\_\_\_\_
4. How many significant/critical systems exist? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Describe the volume of information processed. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Describe the sensitivity of the information processed. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Estimate the amount of electronic transactions (as a %) from external sources. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. What percent of development and support is done off-site by outside service providers? \_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. How many non-organization “consumers” use the system? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Are the transactions by consumers similar or across varying applications? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Does continuity or back-up management include separate, off-site operations? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Do a wide variety of technologies provide access to sensitive data (mobile, network, web, etc.)?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Describe the network and encryption technology used (encryption/digital signature/PKI). \_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Are ISMS services centralized? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_If no, how many locations?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. How long has the ISMS been in place? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Are there any additional requirements outside the standard (legal, regulatory, contractual) that apply under the scope of the ISO/IEC 27001certification? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Is application or system design and development done by the organization? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* If so, on average, what percentage of the organization performs development? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Will it be included in the scope of the ISO/IEC 27001 certification? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
1. Are any controls from Appendix A. of the ISO/IEC 27001 standard excluded from the scope of the certification? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Have the associated risks been reviewed and approved? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
1. List the current Statement of Applicability (SOA) Date \_\_\_\_\_\_\_\_\_\_\_ Revision \_\_\_\_\_\_\_\_\_\_\_ TBD: \_\_\_\_\_\_\_

 **Please provide a current copy of SOA for record purposes**. If not currently available, a copy is required at the Stage 1 event.

1. Has a risk assessment been completed? \_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ TBD:\_\_\_\_\_\_\_\_\_\_\_
2. Will more than one language (English) be spoken during the audit? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Desired "scope of registration" as it is to appear on the certificate of registration. You must consider the product and/or services in the scope when those processes, products, or services have influence.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. What is your target date for registration? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Are you ITAR responsible? Yes \_\_\_\_ No \_\_\_\_\_ Classified material or export control requirements related to SRI access, must be disclosed. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. SRI auditors may not be U.S. citizens. Does your organization restrict foreign national entry to its site(s)? Yes \_\_\_\_ No \_\_\_\_\_ Please describe these restrictions. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. Additional Space: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Other Management Systems**
2. Are you certified to other Management System Standards, e.g., ISO 9001, ISO 14001, ISO/IEC 20000-1? (Y/N) Which Standard(s)? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If not, would you like to discuss other certifications with SRI? Yes \_\_\_\_ No \_\_\_\_\_

1. Have you developed an integrated system*?* Yes \_\_\_\_ No \_\_\_\_

 Which Standards are integrated? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Does the manual include/meet all cited Standards? Yes \_\_\_\_ No \_\_\_\_\_
* Do internal audits address requirements of all standards/conducted in a combined effort? Yes \_\_ No\_\_\_
* Do management reviews address required inputs & outputs from all Standards? Yes \_\_\_\_ No \_\_\_\_\_
* Are required procedures common to all Standards? (doc & record control, training) Yes \_\_\_ No \_\_\_
* Is the corrective and preventive action system common to all cited Standards? Yes \_\_\_\_ No \_\_\_\_\_
* Is the Management Rep the same for all Standards? Yes \_\_\_\_ No \_\_\_\_\_

If the answer to all the above is yes, your system is integrated, and SRI will quote accordingly. Depending on the systems that are integrated, other information may be required. SRI will advise.

1. **For Our Information**
2. Does your company belong to any professional industry organization(s)? Yes  No 
	1. If yes, what association(s)? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. How did you hear about SRI? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. Indicate any processes outsourced. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
5. Indicate the name of your Consultant. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 This survey is provided to assist SRI Quality System Registrar in defining the scope of registration and preparing a cost proposal. The receipt of this survey by SRI does not acknowledge our acceptance and/or approval of any aspect of possible registration.

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Respondent’s Signature Title Date

*Thank you for completing this survey for a cost proposal. Please return to SRI via mail, e-mail, or facsimile.*

**SRI Quality System Registrar, a PRI Company**

**161 Thorn Hill Road, Warrendale, PA 15086**

**Tel.: 724-934-9000 • survey\_info@SRIRegistrar.com**