# Annex D

INFORMAZIONI SUL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI- ISMS

Information Security Management Information ISO/IEC 27001

**Questo vale solo per Organizzazioni / Aziende che richiedono la certificazione secondo lo standard ISO / IEC 270001.**

This applies only to Organizations / Companies which apply for certification to ISO/IEC 270001 Standard.

**Si prega di compilare le seguenti informazioni. Per le sezioni da 1 a 7 barrare l’opzione (a, b, c) che meglio descrive la propria organizzazione. In caso di più siti, con differenze significative tra di loro, si prega di compilare un modulo ANNEX D per ogni sito**.

Please fill-in the following information. For sections 1 to 7 check the description (a, b, c) which best describes your organization. In case of multiple sites, which have significant differences between them, please fill in a separate Annex D form for each different site.

|  |
| --- |
| Fattori legati al COMMERCIO e all'organizzazione (DIVERSO da)Factors related to business and organization (other than IT) |
| 1. **Complessità del ISMS (ad esempio criticità delle informazioni, situazione di rischio dell'ISMS, etc.)**

Complexity of the ISMS (e.g. criticality of information, risk situation of the ISMS, etc.) | Check |
| a) | **Solo poche informazioni sensibili o riservate, requisiti con bassa disponibilità** **Poche attività critiche** **Solo un processo chiave di business con poche interfacce e poche unità coinvolte**Only little sensitive or confidential information, low availability requirementsFew critical assets (in terms of CIA)Only one key business process with few interfaces and few business units involved | ... |
| b) | **Altissima disponibilità di requisiti o informazioni sensibili / confidenziali****Alcune attività critiche****2-3 processi di business semplici con poche interfacce e poche unità coinvolte**Higher availability requirements or some sensitive / confidential informationSome critical assets2-3 simple business processes with few interfaces and few business units involved | ... |
| c) | **Elevata quantità di informazioni sensibili o confidenziali (ad esempio salute, dati personali, assicurazioni, banche) o altissima disponibilità di requisiti****Molte attività critiche****Più di 2 processi complessi con molte interfacce e unità coinvolte**Higher amount of sensitive or confidential information (e.g. health, personally identifiable information, insurance, banking) or high availability requirementsMany critical assetsMore than 2 complex processes with many interfaces and business units involved | ... |
| 1. **Il tipo (i) di attività svolta nel campo di applicazione del ISMS**

The type(s) of business performed within scope of the ISMS |
| a) | **Attività a basso rischio senza requisiti normativi** Low risk business without regulatory requirements | ... |
| b) | **Requisiti normativi alti**High regulatory requirements | ... |
| c) | **Attività ad alto rischio con (solo) limitati requisiti normativi** High risk business with (only) limited regulatory requirements | ... |
| 1. **Prestazioni precedentemente dimostrate del Sistema di Gestione dell’informazione**

Previously demonstrated performance of the ISMS |
| a) | **Recentemente certificato****Sistema di gestione non certificato ma pienamente attuato attraverso diversi audit e miglioramento dei cicli, tra cui audit interni documentati, riesami e sistema efficace di miglioramento continuo** Recently certifiedNot certified but ISMS fully implemented over several audit and improvement cycles, including documented internal audits, management reviews and effective continual improvement system | ... |
| b) | **Audit di sorveglianza recenti****Sistema di gestione non certificato ma parzialmente implementato: Alcuni strumenti del sistema di gestione sono disponibili e attuati; Alcuni processi di miglioramento continuo sono attuati ma parzialmente documentati**Recent surveillance auditNot certified but partially implemented ISMS: Some management system tools are available and implemented; some continual improvement processes are in place but partially documented | ... |
| c) | **Nessuna certificazione e nessun audit recenteIl sistema di gestione è nuovo e non del tutto stabilito (ad esempio mancano specifici meccanismi di controllo del sistema di gestione, i processi di miglioramento continuo sono non maturi, realizzazione dei processi ad hoc)**No certification and no recent auditsISMS is new and not fully established (e.g. lack of management system specific control mechanisms, immature continual improvement processes, ad hoc process execution) | ... |

--- continues to page 3 ---

|  |
| --- |
| Fattori legati all'ambiente informatico - Factors related to IT environment |
| 1. **Estensione e diversità della tecnologia utilizzata nella realizzazione dei vari componenti del Sistema di gestione dell’informazione (ad esempio numero di differenti piattaforme, numero di reti segregate)**

Extent and diversity of technology utilized in the implementation of the various components of theISMS (e.g. number of different IT platforms, number of segregated networks) |
| a) | **Ambiente altamente standardizzato con bassa diversità (alcune piattaforme informatiche, server, sistemi operativi, database, reti, etc.)**Highly standardized environment with low diversity (few IT platforms, servers, operating systems, databases, networks, etc.) | ... |
| b) | **Piattaforme standardizzate ma diverse IT, server, sistemi operativi, database, reti**Standardized but diverse IT platforms, servers, operating systems, databases, networks | ... |
| c) | **Diversità o complessità alta di IT (ad esempio molti diversi segmenti di reti, i tipi di server o database, il numero di applicazioni chiave)**High diversity or complexity of IT (e.g. many different segments of networks, types of servers or databases, number of key applications) | ... |
| 1. **Estensione dell’esternalizzazione e accordi con terze parti utilizzate nell'ambito di attuazione del Sistema di gestione dell’informazione**

Extent of outsourcing and third party arrangements used within the scope of the ISMS |
| a) | **Nessun processo in outsourcing e poca dipendenza dai fornitori, o****Accordi di outsourcing ben definiti, gestiti e monitorati** **Outsourcer ha un sistema di gestione dell’informazione certificato****Sono disponibili report con aziende indipendenti** No outsourcing and little dependency on suppliers, orWell-defined, managed and monitored outsourcing arrangementsOutsourcer has a certified ISMSRelevant independent assurance reports are available | ... |
| b) | **Diversi accordi di esternalizzazione in parte gestiti**Several partly managed outsourcing arrangements | ... |
| c) | **Alta dipendenza di outsourcing o fornitori con grande impatto su importanti attività di business, o****quantità o estensione di outsourcing sconosciuta, o****Diversi accordi in outsourcing non gestiti** High dependency on outsourcing or suppliers with large impact on important business activities, orUnknown amount or extent of outsourcing, orSeveral unmanaged outsourcing arrangements | ... |
| 1. **Grado di sviluppo del sistema informativo** - Extent of information system development
 |
| a) | **Lo sviluppo del sistema non è “in casa”****L'utilizzo di piattaforme software standardizzate**No in-house system developmentUse of standardized software platforms | ... |
| b) | **L'utilizzo di un software standardizzato con una piattaforma di configurazione complessa / parametrizzazione****Software (altamente) su misura****Alcune attività sviluppate (in-casa o in outsourcing)**Use of standardized software platforms with complex configuration/ parameterization(Highly) customized software Some development activities (in-house or outsourced) | ... |
| c) | **Ampia attività di sviluppo software interni con numerosi progetti in corso per scopi importanti di business**Extensive internal software development activities with several ongoing projects for important business purpose | ... |
| INFORMAZIONI SUI MULTI-SITO -Multi-site Information |
| 1. **Numero di siti e numero di siti di Disaster Recovery (DR)**

Number of sites and number of Disaster Recovery (DR) sites |
| a) | **Requisiti di disponibilità bassi e nessuna o un sito alternativo di DR**Low availability requirements and no or one alternative DR site | ... |
| b) | **Requisiti di disponibilità media o alta e nessuna o un sito alternativo di DR**Medium or High availability requirements and no or one alternative DR site | ... |
| c) | **Requisiti di alta disponibilità dei servizi per esempio 24 ore su 24 / 7giorni su 7** **Diversi siti alternativi di DR****Diversi Data Center**High availability requirements e.g. 24h a day /7 day a week servicesSeveral alternative DR sitesSeveral Data Centers | ... |
| ALTRO- Other |
| 1. **Documentare altre informazioni significative / particolarità che potrebbero inficiare la certificazione**

Document other significant information / particularities which might affect the Certification |
| ... |

**Istruzioni** / Instructions:

* **Questo modulo è da inviare sempre insieme con il Costumer Profile (F-2503 form)**
* This form is always to be send along with Organization Profile (F-2503 form)

|  |  |  |
| --- | --- | --- |
| ... |  | ... |
| **Rappresentantedell’Organizzazione**Representative Name | **Firma** Signature | **Data** Date  |