

# Questionario Cyber Enterprise Risk Management

## 1. Identificazione dell'azienda richiedente

<b>Ragione sociale</b>	CONSIP S.p.A. a socio unico
<b>Indirizzo</b>	Via Isonzo, 19/E - 00198 ROMA
<b>Codice Fiscale/Partita IVA</b>	05359681003
<b>Sito/i Web:</b>	www.consip.it
<b>Numero di dipendenti:</b>	420
<b>Fatturato annuale:</b>	74.413.117,00
<b>Margine netto annuo:</b>	5.800.000,00

### Percentuale di Fatturato generato in:

USA/Canada: \_\_\_\_\_ UK: \_\_\_\_\_  
Unione Europea: \_\_\_\_\_ Resto del Mondo: \_\_\_\_\_

## 2. Profilo dell'azienda/delle aziende da assicurare

### 2.1 Attività dell'azienda

[Si prega di descrivere le principali attività dell'azienda da assicurare]

Consip è una Società per Azioni con azionista unico il Ministero dell'Economia e delle Finanze (MEF).
Consip S.p.A. esegue direttamente o tramite soggetti terzi, le funzioni istituzionali afferenti ai seguenti ambiti:
▪ attività di realizzazione del Programma di razionalizzazione degli acquisti;
▪ attività di centrale di committenza per amministrazioni aggiudicatrici, sulla base di previsioni normative o apposite convenzioni;
▪ attività di e-procurement;
▪ attività relative all'affidamento di concessioni;
▪ supporto al ministero dell'economia e delle finanze per le attività relative alla tenuta del registro dei revisori legali e dei tirocinanti;
▪ attività di supporto in tema di gestione, valorizzazione e privatizzazione delle partecipazioni del Ministero dell'economia e delle finanze;
▪ realizzazione del Programma di dismissione dei beni mobili;
▪ supporto al ministero dell'economia e delle finanze in tema di governance dei sistemi di gestione e controllo degli interventi di politica
▪ supporto alle amministrazioni per attività di sviluppo e innovazione della PA o per la realizzazione per specifici progetti formazione, organizzazione di seminari ed eventi con utilizzo di sedi esterne ed interne, proprie o di terzi.

### 2.2 Società Controllate

[Si prega di fornire l'elenco delle società controllate da assicurare e descrizione dell'attività. Se l'azienda ha filiali al di fuori dell'UE, si prega di fornire i dettagli]

Nome	Sede	Attività
NESSUNA		

### 2.3 Criticità dei sistemi informativi

[Si prega di valutare il periodo di interruzione durante il quale l'azienda subirà un impatto significativo sulla sua attività.]

Settori (o Attività) negativo	Massimo periodo di interruzione prima di avere un impatto				
	Immediato	>12h	>24h	>48h	>5 giorni

>2h

Per la gestione del Portale Servizi Revisione Legale di proprietà del Ministero dell'economia e delle finanze

### 3. Sistemi informativi

	<100	101-1000	>1000
Numero di utenti del sistema informativo			X
Numero di Laptop	n.a.		
Numero di Server	X		

Disponete/Siete proprietari di un sito web? (Gestione per conto MEF) ☒ SI ☐ NO

Disponete/Siete proprietari di un servizio di e-commerce? ☐ SI ☒ NO

In caso affermativo:

Qual è la quota di fatturato generata dal sito web? \_\_\_\_\_ (% o effettivo)

### 4. Sistema di Sicurezza delle Informazioni (SSI) (Policy definite da Consip)

#### 4.1 Security policy e risk management

- Una politica di SSI è stata formalizzata e approvata dalla direzione aziendale e/o sono state definite e comunicate a tutto lo staff regole di sicurezza approvate dai rappresentanti dello staff ☒ SI ☐ NO
- Sono formalizzati ed effettuati regolari training (almeno annuali) agli utenti sull'uso sicuro del sistema informativo ☐ SI ☒ NO
- Sono identificati i rischi inerenti i sistemi informativi critici e sono implementati opportuni controlli per mitigarli ☒ SI ☐ NO
- Sono condotti audit regolari del SSI ed è assegnata priorità all'implementazione delle raccomandazioni risultanti ☒ SI ☐ NO
- Le risorse informative sono classificate in accordo alla loro criticità e sensibilità ☒ SI ☐ NO
- I requisiti di sicurezza che si applicano alle risorse informative sono definiti in accordo alla loro classificazione ☒ SI ☐ NO

#### 4.2 Protezione dei sistemi informativi (Sistema in outsourcing)

- |     |   |  |  |
|-----|---|--|--|
| 1.  | L'accesso ai sistemi informativi critici richiede un sistema di doppia autenticazione   | <input type="checkbox"/> SI            | <input checked="" type="checkbox"/> NO |
| 2.  | Agli utenti è richiesto di aggiornare regolarmente le password  | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |
| 3.  | Le autorizzazioni di accesso al sistema si basano sui ruoli dei singoli utenti ed esiste una procedura per la gestione delle autorizzazioni   | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |
| 4.  | Sono definiti riferimenti di configurazione sicura per workstation, laptop, server e dispositivi mobili   | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |
| 5.  | E' attuata la gestione centralizzata dei sistemi informatici e il monitoraggio delle configurazioni   | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |
| 6.  | I laptop sono protetti da un personal firewall  | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |
| 7.  | Un software antivirus è installato su tutti i sistemi e sono monitorati gli aggiornamenti   | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |
| 8.  | Sono regolarmente distribuite ed installate le security patches   | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |
| 9.  | Un DRP (Disaster Recovery Plan) è implementato e aggiornato regolarmente  | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |
| 10. | I backup dei dati sono portati a termine quotidianamente, sono testati regolarmente e copie di essi sono depositate regolarmente in una località remota rispetto a quella ove risiedono i sistemi | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |

#### 4.3 Sicurezza della rete e delle operazioni (Sistema in outsourcing)

- |    |   |  |                             |
|----|---|--|-----------------------------|
| 1. | E' installato ed operativo un firewall per il filtraggio del traffico tra la rete interna e internet con un controllo aggiornato del flusso di informazioni in entrata ed in uscita | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |
| 2. | Un IDS/IPS (Intrusion Detection/Prevention System) è implementato, aggiornato e monitorato regolarmente   | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |
| 3. | Gli utenti interni all'azienda hanno accesso a Internet attraverso dispositivi di rete protetti da antivirus e sistemi di monitoraggio del traffico web                             | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |
| 4. | È implementata la segmentazione della rete per separare le aree critiche dalle aree non critiche  | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |
| 5. | Sono effettuati regolarmente penetration test ed è implementato un remediation plan ove necessario  | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |
| 6. | Sono effettuati regolarmente vulnerability assessment ed è implementato un remediation plan ove necessario  | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |
| 7. | Sono rese effettive procedure di incident management e change management  | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |
| 8. | Eventi riguardanti la sicurezza, come rilevazioni di virus, tentativi di accesso, e simili, sono registrati (tramite log file) e monitorati regolarmente                            | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |

#### 4.4 Sicurezza fisica della sala computer (Sistema in outsourcing)

- |    |  |  |                             |
|----|--|--|-----------------------------|
| 1. | I sistemi critici sono collocati in almeno una sala computer dedicata con accesso limitato e allarmi operativi funzionanti sono inviati ad una sede di monitoraggio          | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |
| 2. | I CED che ospitano sistemi critici hanno un'infrastruttura resiliente che include ridondanza dei sistemi di alimentazione, impianti di condizionamento e connessioni di rete | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |
| 3. | I sistemi critici sono duplicati in funzione di un'architettura Active/Passive o Active/Active   | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |
| 4. | I sistemi critici sono duplicati in due sedi separate  | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |
| 5. | Sono implementati rilevatori antincendio e sistemi automatici di estinzione in aree critiche   | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |
| 6. | L'alimentazione è protetta da UPS e batterie, entrambi sottoposti a regolari programmi di manutenzione   | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |
| 7. | L'alimentazione è sostenuta da generatore elettrico soggetto a regolare contratto di manutenzione e testato regolarmente   | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO |

#### 4.5 Outsourcing

[Si prega di compilare in caso una o più funzioni del sistema informativo è data in outsourcing]

- |    |  |  |  |
|----|--|--|--|
| 1. | Il contratto di outsourcing include requisiti di sicurezza che devono essere osservati dall'outsourcer   | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |
| 2. | I Service Level Agreements (SLA) sono definiti con l'outsourcer al fine di gestire gli incidenti e vengono applicate penalità all'outsourcer in caso di non conformità con i SLA | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |
| 3. | Il/I comitato/i di direzione e controllo si coordina con il service provider per la gestione e il perfezionamento del servizio   | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |
| 4. | L'assicurato ha rinunciato al diritto di ricorso contro l'outsourcer nel contratto di outsourcing  | <input type="checkbox"/> SI            | <input checked="" type="checkbox"/> NO |

Quali sono le funzioni del sistema informativo date in outsourcing?

Desktop management ☐ SI ☒ NO

Server management ☒ SI ☐ NO

Network management ☒ SI ☐ NO

Network security management ☒ SI ☐ NO

Application management ☒ SI ☐ NO

Utilizzo di cloud computing ☐ SI ☒ NO

Se sì, si prega di specificarne la natura

Software as a Service ☐ SI ☐ NO

Platform as a Service ☐ SI ☐ NO

Infrastructure as a Service ☐ SI ☐ NO

Altro, si prega di specificare:

#### Outsourcer

Almaviva S.p.A.

5. Il contratto di outsourcing contiene una disposizione che richiede al service provider di sostenere una polizza assicurativa coprente indennità professionale, errori e omissioni ☒ SI ☐ NO

## 5. Dati personali trattenuti dall'azienda

### 5.1 Tipo e numero di record (archivi/documenti/registri) (Si intende numero di soggetti di cui si conservano i dati)

Il numero di record contenenti informazioni personali trattenuti per l'attività da assicurare:

Totale:	ca. 150.000	Per nazione:	Italia	UK/I:	
Europe (EU):	qualche unità	USA/Canada:		Resto del mondo:	

Categorie di dati personali raccolti/trattati:

			Quantità
Informazioni commerciali e di marketing	<input type="checkbox"/> SI <input checked="" type="checkbox"/> NO		
Carte di credito o informazioni sulle transazioni finanziarie	<input checked="" type="checkbox"/> SI <input type="checkbox"/> NO		ca. 55.000 transazioni /anno
Informazioni di natura sanitaria	<input checked="" type="checkbox"/> SI <input type="checkbox"/> NO		qualche unità
Altro, si prega di specificare:			

I dati sono trattati: ☐ Per fini propri ☒ Per conto di terze parti (Per conto MEF)

### 5.2 Politica di protezione delle informazioni personali (Policy definite da Consip)

1. E' stata formalizzata ed approvata dall'amministrazione una politica sulla privacy e/o sono definite e comunicate allo staff interessato regole per la sicurezza dei dati personali ☒ SI ☐ NO
2. Sono forniti corsi di formazione e sensibilizzazione almeno annualmente al personale autorizzato ad accedere a o a trattare con dati personali ☒ SI ☐ NO
3. È nominato un funzionario incaricato della protezione dei dati personali ☒ SI ☐ NO
4. Viene firmato nel contratto di assunzione, da parte dello staff interessato, un accordo o una clausola di riservatezza ☒ SI ☐ NO
5. Gli aspetti legali relativi alla politica sulla privacy sono convalidati da un avvocato o dalla divisione legale ☒ SI ☐ NO
6. Sono implementate misure di monitoraggio per garantire la conformità con le leggi e regolamentazioni per la protezione dei dati personali ☒ SI ☐ NO
7. Le pratiche/prassi aziendali relative alle informazioni personali sono state sottoposte a auditing da un ispettore esterno negli ultimi due anni ☐ SI ☒ NO
8. Un Data Breach Response Plan è implementato e i ruoli sono stati comunicati con chiarezza ai membri della squadra operativa ☐ SI ☒ NO

### 5.3 Raccolta di dati personali

- |   |   |  |                                  |
|---|---|--|----------------------------------|
| 1.  | Avete notificato al Garante per la protezione dei dati personali il Responsabile del trattamento dei dati personali nominato in azienda e avete ottenuto la rispettiva autorizzazione | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO      |
| Se non applicabile, si prega di spiegare: _____ |   |  |                                  |
| 2.  | E' stata pubblicata sul sito aziendale una politica sulla privacy revisionata da un legale/dipartimento legale  | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO      |
| 3.  | È richiesto il consenso prima di raccogliere i dati personali e gli interessati possono accedere e, se necessario, correggere o cancellare i loro dati personali                      | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO      |
| 4.  | Ai proprietari è fornita in modo chiaro la possibilità di rinunciare ad operazioni mirate di marketing  | <input type="checkbox"/> SI            | <input type="checkbox"/> NO n.a. |
| 5.  | Trasferite i dati personali a terzi: (Trasferiti secondo obblighi di legge)   | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO      |
| Se sì, si prega di rispondere alle seguenti:    |   |  |                                  |
| 5.a.  | I terzi sono contrattualmente obbligati a trattare i dati personali esclusivamente per conto vostro e secondo le vostre istruzioni  | <input type="checkbox"/> SI            | <input type="checkbox"/> NO n.a  |
| 5.b.  | I terzi sono contrattualmente obbligati a implementare sufficienti misure di sicurezza per proteggere i dati personali  | <input type="checkbox"/> SI            | <input type="checkbox"/> NO n.a  |

### 5.4 Controlli per la protezione dei dati personali

- |    |   |  |  |
|----|---|--|--|
| 1. | L'accesso ai dati personali è limitato ai soli operatori che lo necessitano per svolgere il proprio incarico e le autorizzazioni di accesso sono revisionate regolarmente     | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |
| 2. | I dati personali sono criptati quando archiviati nei sistemi informatici, così come i relativi backup   | <input type="checkbox"/> SI            | <input checked="" type="checkbox"/> NO |
| 3. | I dati personali sono criptati quando trasmessi attraverso la rete  | <input type="checkbox"/> SI            | <input checked="" type="checkbox"/> NO |
| 4. | I dispositivi mobili e gli hard disk dei laptop sono criptati   | <input type="checkbox"/> SI            | <input checked="" type="checkbox"/> NO |
| 5. | La politica di sicurezza delle informazioni proibisce la copia di dati personali non criptati su dispositivi di archiviazione mobili o la trasmissione di tali dati via email | <input checked="" type="checkbox"/> SI | <input type="checkbox"/> NO            |

Se gli archivi di dati personali contengono dati relativi alle carte di credito, si prega di rispondere alle seguenti:

Il vostro livello PCI DSS è: (paragrafo n.a.)

Livello 1: \_\_\_\_\_ Livello 2: \_\_\_\_\_ Livello 3: \_\_\_\_\_ Livello 4: \_\_\_\_\_

Chi tratta i pagamenti (voi stessi o terzi) rispetta il PCI DSS ☐ SI ☐ NO

Se No:

I dati relativi alle carte di credito sono archiviati criptati o solo una parte di essi è archiviata ☐ SI ☐ NO

Il tempo di mantenimento dei dati relativi alle carte di credito non eccede la durata di pagamento e i requisiti legali/normativi ☐ SI ☐ NO

Il trattamento dei dati relativi alle carte di credito è esternalizzata

☒ SI ☐ NO

Se Sì:

E' richiesto a chi si occupa del trattamento i pagamenti di indennizzarvi in caso di violazione della sicurezza

☐ SI ☐ NO **Nodo AgID PagoPA**

Si prega di indicare il nome di chi si occupa del trattamento dei pagamenti, il tempo di mantenimento dei dati relativi alle carte di credito e ogni ulteriore misura di sicurezza:

---

---

---

---

## 5.5 Incidenti

Si prega di fornire una descrizione di qualunque incidente relativo alla sicurezza informatica o alla privacy accaduto nei precedenti 36 mesi. Gli incidenti includono qualunque accesso non autorizzato a qualunque computer, sistema informatico o database, intrusione o attacco, impossibilità d'utilizzo di qualunque computer o sistema, interruzione premeditata, corruzione, o distruzione di dati, programmi, o applicazioni, qualunque evento di cyber estorsione; o qualunque altro incidente simile ai precedenti, inclusi quelli che hanno generato una richiesta di risarcimento, azione amministrativa, o procedimento da parte di un'autorità di vigilanza.

Data:

Descrizione dell'incidente: nessun incidente registrato alla data

Commenti:

---

---

---

Nessun individuo o ente per cui è richiesta copertura è a conoscenza di alcun fatto, circostanza, o situazione, che ha ragione di supporre possa causare alcuna richiesta di risarcimento (**claim**) che possa ricadere nell'ambito della copertura proposta.

Nessuno o, tranne:

☒ 

---

Persona da contattare per ulteriori informazioni:

Nome: 

---

 Titolo: 

---

Telefono: 

---

 E-mail: 

---

Completato da: 

---

---

**Nome e Cognome del firmatario**

---

**Ruolo**

---

**Data**

---

**Firma**