Giunta Regione Toscana

Attività di controllo su fornitori di servizi IT

(relazione Titolare-Responsabile)

Linee Guida

Indice

1 Scopo del documento

Lo scopo del presente documento è quello di fornire delle linee guida per la definizione dei controlli da effettuare nei confronti del Responsabile da parte del Titolare, nel caso specifico di fornitori di servizi IT o di altri soggetti che si configurano in tale ruolo.

2 Premessa

Nel caso di utilizzo di procedure IT il Titolare può avvalersi di strutture interne alla propria organizzazione, fornitori esterni attraverso specifici contratti di fornitura di altri enti o seggetti nell'ambito di convenzioni. In ognuno di questi casi il Titolare, sia esso la Giunta regionale o un ente dipendente, è tenuto a svolgere la sua funzione di controllo in merito al puntuale rispetto da parte del Responsabile delle misure di sicurezza adottate, proposte dal Responsabile e ritenute adeguate dal Titolare.

Quindi premessa fondamentale è che nel rapporto Titolare Fornitore siano esplicitate nel Data Protection Agreement le misure di sicurezza adottate in relazione al "valore dei dati trattati".

Qualora i Responsabili siano fornitori, essi saranno soggetti, a cura del Titolare, a degli audit periodici (ai sensi dell'art. 28 comma 1 lett. H del GDPR), finalizzati a verificare il rispetto dell'agreement sottoscritto.

Nel caso della Giunta regionale toscana e degli enti che si avvalgono della stessa struttura di Security Manager, i controlli sono ad essa demandati nell'ambito del piano annuale che deve predisporre (vedi Data Protection Policy). Rimane comunque in carico al Titolare verificare che i controlli siano pianificati e poi eseguiti.

3 Analisi preliminare della fornitura IT

Gli aspetti di rilievo in ambito GDPR, che emergono in relazione alla fornitura di servizi IT appaltata presso outsorcers, sono di duplice natura e si sviluppano su due piani.

Sul piano **soggettivo**, individuando i ruoli "Data Protection" da attribuire:

In prima istanza, andrà stabilito se l'outsourcer andrà o meno identificato nel ruolo di responsabile del trattamento (ovvero, in linea teorica, se sia identificabile come titolare autonomo o contitolare del trattamento). Tale ricorrenza sussiste se l'outsourcer è incaricato di effettuare uno o più trattamenti (art. 4, comma 1 nr. 2 GDPR: *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;"*) ricompresi nella definizione *ex* art. 4 comma 1 nr. 8 *("la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"*) per conto della Regione Toscana, quale titolare del trattamento.

Per identificare correttamente la sussistenza o meno, inoltre, del ruolo di amministratore di sistema (rete, infrastruttura, software o data base), dovranno ricorrere le circostanze previste dal provvedimento generale del Garante per la protezione dei dati personali "**Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008**" e successive modifiche ed integrazioni. Per quanto attiene alla figura dell'amministratore di sistema, ruoli e compiti, si rimanda allo specifico disciplinare.

Sul piano **oggettivo**, indicando la tipologia di servizio da erogare e le specifiche tecniche che caratterizzano la prestazione, identificando nel contempo eventuali condizioni vincolanti (ad es., preesistente infrastruttura su cui innestare determinati tipi di software, ovvero caratteristiche della rete che vincolano nella scelta dei software etc.).

I risultati delle suddette valutazioni confluiranno nel capitolato di gara, ovvero nella documentazione pre-contrattuale nel caso delle altre tipologie di affidamento previste dal Codice degli Appalti o infine nei contratti di fornitura o in specifici Data Protection Agreement.

4 La Titolarità del trattamento

La titolarità del trattamento, per quanto concerne le presenti linee guida, spetta comunque all'Ente (Regione toscana, Consiglio regionale, enti dipendenti), quale soggetto deputato a stabilire finalità e mezzi del trattamento di dati personali.

Pur tuttavia, nell'ambito delle forniture IT, è possibile che la determinazione dei mezzi del trattamento non sia di agevole definizione. La definizione dei mezzi del trattamento potrebbe, in effetti; essere demandata a soluzioni tecniche elaborate direttamente dal fornitore, oppure potrebbe essere richiesto al fornitore di elaborare soluzioni tecniche entro specifici limiti di importo a base d'asta. Tale circostanza, tuttavia, secondo posizione ormai consolidata del WP art. 29 (attuale Gruppo dei Garanti Data Protection europei), deve ritenersi non incidente sul ruolo di titolare del trattamento in capo all'ente. E' ammesso che un responsabile possa limitarsi a seguire orientamenti generali dati dal titolare principalmente sulle finalità senza intervenire nei dettagli per quanto riguarda gli strumenti.

Ai sensi del WP 169, *"per quanto riguarda la determinazione degli strumenti, va detto innanzitutto che il termine "strumenti" comprende evidentemente vari tipi di elementi (…). In altri termini, "strumenti" non si riferisce solo ai mezzi tecnici per trattare i dati personali, ma anche al "come" del trattamento, cioè "quali dati saranno trattati", "quali terzi avranno accesso ai dati", "quando tali dati saranno eliminati", ecc. La determinazione degli "strumenti" ingloba quindi questioni sia tecniche che organizzative la cui decisione può anche essere delegata ai responsabili del trattamento (…). In tale ottica, è del tutto possibile che i mezzi tecnici ed organizzativi siano determinati esclusivamente dal responsabile del trattamento."*

5 La contrattualizzazione dei doveri del Responsabile del trattamento

Gli audit sui fornitori sono un gravame spettante al titolare del trattamento (si veda l'art. 28 comma 1, *"lett. H: messa a disposizione del titolare del trattamento "tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28", nonché consentire e contribuire "alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato"*).

Dunque, gli audit dovranno vertere su ciascun aspetto previsto dall'agreement stipulato ai sensi dell'art. 28, in particolare:

1. rispetto di ogni istruzione del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento;
2. garanzia che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
3. adozione di tutte le misure richieste ai sensi dell'articolo 32;
4. rispetto delle condizioni generali o speciali di sub-affidamento dei trattamenti;
5. assistenza al titolare del trattamento con l'adozione delle misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III GDPR;
6. assistenza al titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

7. assistenza su rispetto degli obblighi del responsabile in relazione a cancellazione o restituzione dei dati affidati.

Peculiare attenzione deve essere rivolta ai controlli sulle misure di sicurezza, sia tecniche che organizzative, perché:

1. Aleatorie, in quanto dipendenti da fattori non solo endogeni, ma anche esogeni, come ad es. il livello accertato di cyberisk;
2. Dinamiche, dal momento che il livello di rischio muta periodicamente, ad es. con l'evoluzione tecnologica e delle tecniche di hacking.

Pertanto, le misure stabilite per effettuare i trattamenti affidati al fornitore dovranno essere oggetto di rivalutazione periodica, disciplinata dall'art. 32 GDPR secondo regole vincolanti sia per il titolare sia per il responsabile.
Tali misure coinvolgeranno e vincoleranno anche i sub-responsabili eventualmente individuati, sui quali verteranno distinti audit ad opera del responsabile.

Nota bene: *Le misure di sicurezza possono imporre gravami economici non indifferenti; per tale ragione è necessario regolamentare preliminarmente gli eventuali limiti di budget (o, in teoria, le clausole di invarianza) per la gestione delle eventuali ulteriori misure di sicurezza necessarie per rispettare i parametri di "idoneità" delle misure rispetto ai trattamenti affidati.*

6 Quando svolgere gli audit

Nel contesto degli appalti pubblici, si rinvengono due momenti fondamentali in cui è opportuno effettuare controlli sulla sussistenza delle misure a garanzia dei trattamenti affidati in outsourcing:

1. Il primo è rinvenibile nel momento dell'aggiudicazione, fase in cui è necessario verificare la veridicità delle dichiarazioni rese – tra cui quelle relative alle misure di garanzia determinate a tutela dei dati il cui trattamento è appaltato.
2. L'insussistenza delle misure determinate configurerebbe non solo mendace dichiarazione in ordine alle caratteristiche del servizio reso alla stazione appaltante, ma anche carente garanzia dei trattamenti, del che si deduce la possibilità di revoca dell'aggiudicazione dell'appalto;
3. Il secondo ricorre ciclicamente, la periodicità è determinata dal titolare – deve essere perlomeno annuale - in base alle strategie di controllo globale fissate sui propri fornitori.

7 Modalità di svolgimento degli audit

In relazione ad i controlli ciclici, alcuni indici utili a determinare le priorità del piano di audit sono:

1. Forniture critiche, la criticità delle forniture si rinviene da indici non tassativamente previsti, inerenti a fattori che possono riguardare o direttamente il trattamento dei dati personali, come il livello di rischio del trattamento affidato in appalto o fattori esterni come l'importo dell'appalto.
2. Forniture per le quali, in precedenti audit, sono state segnalate azioni di remediation per l'adeguamento delle misure di sicurezza (follow up)
3. Forniture selezionate a campione (a seguito della verifica delle precedenti forniture prioritarie)
4. Le modalità di audit, secondo le best practices consolidate, possono essere ricondotte a scenari:
    1. Ricognizione generale delle misure adottate, anche tramite autodichiarazione resa dal fornitore
    2. Verifica delle dichiarazioni rese ai sensi del precedente punto

3. Verifica in loco delle misure adottate (azione aggiuntiva o sostitutiva delle modalità sub 1\2)

8 L'audit report e il remediation plan

Al termine dell'audit il Titolare del trattamento fornirà al Responsabile auditato, un audit report, contenente le carenze riscontrate in materia di protezione dei dati personali, in relazione agli aspetti controllati ed elencati nei precedenti paragrafi.
In base alle risultanze dell'audit report, sarà opportuna, a cura del Responsabile, l'elaborazione di un "piano di remediation" finalizzato a colmare le carenze evidenziate. Lo stesso sarà condiviso con il Titolare, che effettuerà il follow up conseguente, per verificare la corretta implementazione degli aspetti risultati non ottimali.
Il piano di remediation dovrà contenere il dettaglio delle attività di adeguamento che il fornitore si impegna ad integrare e le relative scadenze, concordate con il Titolare. Su tale contenuto il Titolare del trattamento, come già sopra specificato, effettuerà successivi controlli per verificare il compimento delle azioni correttive.

9 Avvalimento di altri enti

Nel caso in cui un Ente si avvalga di un altro per lo svolgimento di alcune funzioni proprie, vedasi il caso di enti strumentali della Regione che utilizzano strutture tecniche ed organizzative di settori della Regione Toscana per la gestione del personale, per la sicurezza dei luoghi di lavoro, su progetti speciali, ecc.., valgono le seguenti indicazioni:

1. Il settore competente per la materia della giunta regionale (es. personale) con il supporto del settore IT ha l'obbligo di pubblicare e rendere noto agli enti, a cui eroga servizi sulla base di un atto convenzionale, le misure di sicurezza tecniche ed organizzative adottate. Tali misure debbono essere dichiarate e mantenute aggiornate secondo le linee guida "Definizione e descrizione delle misure di sicurezza in materia di protezione dei dati personali",
2. Il registro dei trattamenti dell'Ente che eroga il servizio (es. regione toscana settore del personale) deve essere aggiornato nella sezione Responsabile, mentre analoga registrazione deve essere presente nel registro dell'ente Titolare indicando l'altro come responsabile,
3. Il personale del Responsabile deve essere debitamente informato ed autorizzato in merito al trattamento di dati svolti per conto di un altro titolare (ente),
4. Il responsabile deve programmare periodici controlli sulle misure di sicurezza ed attuare gli interventi di miglioramento e deve comunicarne sia la pianificazione sia l'esito al titolare all'interno di un processo di condivisione e trasparenza.

Il titolare deve sempre essere messo in grado di conoscere e rendere conto in merito alle misure di sicurezza adottate per i trattamenti sotto la propria titolarità.
L'adeguatezza delle misure di sicurezza in questo caso è assicurata dal soggetto Responsabile.
Il titolare deve comunque assicurarsi che il responsabile proceda alla continua manutenzione delle misure di sicurezza tramite controlli periodici di cui deve essere messo a conoscenza.
Nel caso in cui il Responsabile si avvalga di altri Responsabili risulta evidente la sua piena responsabilità nei confronti del Titolare.

10 Riepilogo dei controlli

In sintesi possiamo asserire che i controlli da porre in essere, siano sia formali sia di merito.
I controlli possono e debbono essere messi in atto, sia in un momento successivo alla stipula del contratto, data che deve essere dichiarata nel capitolato (nel contratto deve essere esplicitata la sua risoluzione in caso di verifica negativa), sia periodicamente secondo un piano temporale anch'esso indicato nel contratto, sia ogni qual volta si verifichi un incidente.
E' opportuno definire, per ogni Ente, con il supporto del Security manager, un piano pluriennale dei controlli che tenga conto delle criticità o meno dei servizi utilizzando come criterio guida la valutazione di rischio in relazione alla tipologia dei dati trattati, alle categorie degli interessati coinvolti, della numerosità degli stessi (elementi che determinano il "valore del dato" trattato).
I controlli possono sempre essere assistiti dal DPO o dalla sua struttura. Per alcuni controlli di merito occorre coinvolgere il Security Manager o persone da lui indicate con adeguata professionalità.
Gli esiti dei controlli debbono essere comunicati al DPO, al RUP e al DEC del contratto di fornitura ognuno per gli aspetti di propria competenza.

10.1 Controlli formali

I controlli formali debbono riguardare l'esistenza della documentazione richiesta per rispondere al principio della accountability e per consentire al Titolare di conoscere e saper documentare la corretta relazione con il Responsabile.

10.1.1 Data Protection Agreement

Il documento di Data Protection Agreement deve essere sottoscritto fra le parti prima della erogazione del servizio e deve essere aggiornato ogni qual volta cambino i trattamenti o le relative misure di sicurezza.

10.1.2 Registro dei trattamenti

Il registro dei trattamenti deve essere attivato e i trattamenti registrati e firmati prima della messa in esercizio del servizio. Il registro deve essere completo, deve cioè contenere tutti i trattamenti messi in atto, e per ogni trattamento devono essere compilate tutte le informazioni relative alla liceità, alla descrizione del trattamento, alla individuazione del titolare e del responsabile/sub responsabile, agli asset, alle misure di sicurezza, agli autorizzati, ecc.. Il registro deve essere firmato, deve consentire una ricostruzione storica delle registrazioni, deve essere facilmente accessibile e consultabile in fase di ispezione da parte del titolare o del garante.

10.1.3 Autorizzati

Deve essere immediatamente disponibile, su richiesta e tramite estrazione dal registro dei trattamenti, l'elenco degli autorizzati e dei relativi profili per ogni trattamento. Il formato dei dati deve essere elaborabile con strumenti digitali.

10.1.4 Amministratori di sistema

Deve essere disponibile l'elenco degli amministratori di sistema con indicazione degli asset di riferimento. (Data Base amministrator, System Amministrator, ecc..). L'elenco deve essere immediatamente disponibile su richiesta e deve essere consegnato con un formato elaborabile con strumenti digitali.

10.1.5 Informazioni agli operatori

Occorre verificare che tutti gli operatori (amministratori di sistema, autorizzati, altro personale), che possono venire a vario titolo in contatto con i dati personali, abbiano ricevuto adeguata informazione, che siano impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

10.1.6 Gestione degli Asset

Verificare l'esistenza del catalogo degli asset con i seguenti contenuti:

a) Descrizione complessiva dell'architettura tecnologica, IaaS, PaaS, SaaS del Responsabile nella quale si evidenzino le diverse zone (ambiti architetturali), a diversa intensità di misure di sicurezza,
b) Descrizione dei servizi in Modalità SaaS
c) Descrizione dei servizi applicativi eventualmente gestiti da altri fornitori ma ospitati nell'infrastruttura del Responsabile o viceversa.
d) Collegamento con le misure di sicurezza
e) Collegamento con i trattamenti.
f) Descrizione dei processi organizzativi che sovraintendono la gestione degli asset ed il loro continuo aggiornamento

10.1.7 Misure di sicurezza

Occorre verificare che esista la documentazione che descriva per ogni asset le misure di sicurezza adottate valutate e dichiarate adeguate in relazione alla tipologia di dati personali trattati (livello di rischio definito sulla base della tipologia di dati, categorie di interessati, numerosità degli interessati). Questo richiede che il Responsabile tenga strettamente correlati i trattamenti con gli asset attraverso i quali avviene il trattamento stesso.

Particolare attenzione e descrizione deve essere posta alle misure di sicurezza adottate per il processo di identificazione e attribuzione dei ruoli e dei profili agli autorizzati.
Le misure di sicurezza debbono sempre riferirsi per la loro adeguatezza ai dati contenuti e trattati, pertanto occorre considerare le misure di sicurezza complessivamente applicate ai dati partendo da quelle applicative fino a quelle logistiche.

10.1.8 Gestione degli incidenti

Occorre verificare che il Responsabile abbia messo in esercizio il "registro degli incidenti" e definito una procedura organizzativa interna idonea ad intercettare gli incidenti e gestire efficacemente il processo di rilevamento, di comunicazione al titolare e di conduzione della gestione dell'incidente stesso ivi compresa la formulazione e la messa in atto di un remediation plan.

10.1.9 Piano di qualità della fornitura

Deve esistere un piano di qualità della fornitura nel quale occorre che insieme ad altre cose che possono riguardare la fornitura dei servizi, siano descritti:

1. L'organizzazione del responsabile con riferimento alle figure di presidio dei processi GDPR
2. Relazioni con sub responsabili o con altri soggetti nella gestione della conduzione dei servizi che prevedono il trattamento di dati personali e dei processi GDPR,
3. Processi messi in atto per il rispetto del GDPR (rispetto della DPA, Accountability, Data Protection by Default by Design, Diritti degli interessati, Gestione degli incidenti),
4. Processo di deployment dei servizi applicativi e non,
5. Registro delle applicazioni e dei profili di accesso e autorizzazione (quali azioni e su quali dati),
6. Processo di audit interno per la verifica delle misure di sicurezza,
7. Modalità di gestione congiunta di asset con altri soggetti con particolare riferimento a:
    a. Processi produttivi,
    b. Gestione degli asset,
    c. Gestione del registro dei trattamenti,
    d. Gestione del registro, degli incidenti e relativi processi di detection, notifica, problem determination, remediation plan,
    e. Gestione complessiva delle misure di sicurezza e dichiarazione della loro adeguatezza
    f. Gestione congiunta degli audit interni.

10.1.10 Check list controlli formali

Controlli Formali	***Esistenza*** *(Si/No)*	***Livello completezza/aggiornamento*** *(Basso, Medio, Alto)*	***Note*** *(Carenze da superare)*
Data Protection Agreement			
Registro dei Trattamenti			
Elenco Autorizzati			
Elenco amministratori di sistema			
Informazione agli operatori			
Gestione degli Asset			
Misure di sicurezza			
Gestione degli incidenti			
Piano di qualità della fornitura			

10.2 Controlli di merito

10.2.1 Data Protection Agreement

Occorre verificare che quanto descritto nel DPA sia conforme ed aggiornato a quanto risulta dal registro dei trattamenti, e in eventuali sub forniture che siano nel frattempo intervenute o modificate.

10.2.2 Registro dei trattamenti

Occorre verificare in relazione alle applicazioni effettivamente in esercizio, tramite la rilevazione sul campo (es. elenco dei servizi indirizzati dagli application server), se esse siano presenti nel catalogo degli asset e questi collegati ai relativi trattamenti e alle relative misure di sicurezza. Occorre verificare la coerenza dei nomi fra gli asset applicativi nel registro dei trattamenti e quanto effettivamente gestito.

10.2.3 Autorizzati

Devono, a richiesta, essere immediatamente resi disponibili:

a) i log degli accessi degli utenti alle applicazioni,
b) gli autorizzati presenti nel registro dei trattamenti con riferimento alle applicazioni quali asset,

ambedue in formato elaborabile digitalmente in modo da confrontarli.

Per ogni autorizzato deve essere possibile ottenerne il profilo autorizzativo di accesso all'applicazione (autorizzazione) ma anche e soprattutto di accesso alle funzioni interne dell'applicazione (profilo applicativo) attraverso il quale sia possibile risalire in modo semplice alle azioni che l'autorizzato può fare sui dati e su quali dati.

Il controllo dovrà verificare che tutti gli utenti presenti sui log devono essere anche presenti nella lista degli autorizzati e che il profilo di accesso sia compatibile con la descrizione del trattamento a cui sono autorizzati.

10.2.4 Amministratori di sistema

Occorre controllare che le credenziali di accesso siano univocamente assegnate ad una ed una sola persona e che esistano dei file di log che possano indicare per ogni persona l'accesso inidcando i parametri temporali e i contenuti.

Occorre ottenere:

a) I file di log dei sistemi con l'indicazione della persona,
b) L'elenco degli amministratori di sistema.

Sulla base di questi elenchi occorre verificare che tutte le persone che hanno operato come amministratori di sistema siano presenti nell'elenco.

10.2.5 Informazioni agli operatori

Occorre verificare, tramite interviste, se gli operatori hanno effettivamente recepito le indicazioni di riservatezza delle quali sono stati informati e quali comportamenti hanno adottato in conseguenza delle informazioni ricevute.

10.2.6 Misure di sicurezza

Per la verifica nel merito delle misure di sicurezza si rimanda al documento di audit e non possono che essere demandate a personale specializzato. Tale controllo è finalizzato ai seguenti scopi:

a) Verificare se le misure dichiarate siano effettivamente messe in campo,
b) Verificare che i processi di aggiornamento delle misure di sicurezza siano attivi,
c) Verificare l'adeguatezza delle misure di sicurezza in relazione al livello di rischio dei dati trattati.

10.2.7 Gestione degli incidenti

Occorre prendere visione del registro e farne:

a) Una valutazione complessiva di rispondenza alla realtà,
b) Una verifica di completezza delle informazioni riportate,
c) Una verifica se i remediation plan siano poi stati attuati.

10.2.8 Piano di qualità della fornitura

Occorre verificare se quanto dichiarato nel piano di qualità della fornitura risponde, nell'organizzazione e nei processi ,a quanto rilevabile sul campo

10.2.9 Check list controlli di merito

Controlli di Merito	*(Si/No)*	***Livello*** *(Basso, Medio)*	***Note*** *(Carenze da superare)*
Data Protection Agreement: 1. Congruenza con registro trattamenti 2. Congruenza con misure di sicurezza			
Registro dei Trattamenti 1. Congruenza dei trattamenti con le applicazioni in esercizio 2. Congruenza delle applicazioni con gli Asset registrati			
Elenco Autorizzati 1. Congruenza degli autorizzati dichiarati con quelli effettivi nei log			
Elenco amministratori di sistema 1. Congruenza degli Amministratori di sistema dichiarati con quelli effettivi nei log.			
Informazione agli operatori 1. Verifica, tramite interviste, che gli operatori siano stati effettivamente informati			
Gestione degli Asset 1. Verifica che gli asset rilevati siano presenti nel catalogo con adeguato livello di descrizione			
Misure di sicurezza 1. Verifica se le misure dichiarate siano effettivamente messe in campo, 2. Verifica che i processi di aggiornamento delle misure di sicurezza siano attivi, 3. Verifica della adeguatezza delle misure di sicurezza in relazione al livello di rischio dei dati trattati.			
Gestione degli incidenti 1. Una valutazione complessiva di rispondenza alla realtà, 2. Una verifica di completezza delle informazioni riportate 3. Una verifica se i remediation plan siano poi stati attuati			
Piano di qualità della fornitura 1. Verifica dell'attuazione organizzativa 2. Verifica dell'attuazione dei processi			