TAPA Facility Security Requirements Certification Framework Document - 2020

Un documento guida per TAPA FSR 2020

Riferimenti: TAPA FSR 2020 Standard

TAPA Americas

5030 Champion Blvd,
G-11 #266 Boca Raton,
Florida 33496
U.S.A.
www.tapaonline.org
Tel. (561) 617-0096

TAPA Asia Pacific

1 Gateway Drive, Westgate
Tower #07-01,
Singapore 608531

www.tapa-apac.org
Tel. (65) 6514 9648

TAPA EMEA

Rhijngeesterstraatweg 40D
2341 BV Oegstgeest
The Netherlands

www.tapaemea.org
Tel. +44 1633 251325

Indice FSR

1. Scopo del presente documento di Certificazione

Il presente documento di Certificazione TAPA FSR è la guida ufficiale TAPA per gli auditor autorizzati e gli LSP/Richiedenti per poter condurre audit conformi allo standard TAPA FSR 2020 e per poter ottenere la certificazione su tutte le sedi in cui è applicabile. Il processo di certificazione deve essere funzionale e pratico in termini sia economici che operativi.
Il documento è stato sviluppato esclusivamente per l'Organizzazione TAPA con l'intento di ottenere la conformità e la certificazione a una o più delle seguenti opzioni di Certificazione FSR:

2. Ambito di applicazione

Per fornire ulteriore flessibilità e incoraggiare le certificazioni TAPA, TAPA ha sviluppato tre opzioni a supporto della certificazione:

a) Certificazione di un singolo sito da parte di un Ente Certificatore (IAB). Ogni sito viene certificato in modo indipendente con l'attuale revisione FSR.

b) Certificazione multi-sito da parte dello IAB. I gestori di strutture con 3 o più siti possono ottenere una Certificazione Multi-sito (un unico certificato) per tutti i siti registrati nel sistema di certificazione.

c) Certificazione di self-audit da parte di Auditor Autorizzati (AA), da parte dell'LSP/Richiedente o dello IAB. Ogni sito è autocertificato in modo indipendente dal gestore con il livello C dell'attuale revisione FSR.

3. Applicazione del Sistema di Certificazione TAPA FSR

Nello sviluppo del presente documento per la certificazione TAPA FSR, TAPA riconosce le molteplici differenze nel modo in cui i servizi di stoccaggio sono forniti a livello globale, regionale e anche all'interno delle aziende, e che i vari standard TAPA possono essere applicati a tutti o a parte dei servizi forniti da un LSP/Richiedente. A seconda della complessità e delle dimensioni della supply chain, la conformità agli standard TAPA può essere ottenuta attraverso un singolo LSP/Richiedente o più LSP/Richiedenti e subappaltatori qualificati.

Il presente documento di certificazione può essere applicato a:

a) Alcuni o tutti i luoghi di stoccaggio all'interno della supply chain, a seconda del rischio e/o dei requisiti del Cliente (Buyer) o dell'LSP/Richiedente;
b) Strutture di proprietà o in gestione all'LSP/Richiedente;
c) Strutture di proprietà o gestite del Cliente (Buyer).

Gli utilizzatori a cui si rivolge questo documento di certificazione sono:

a) Clienti (Buyers)/produttori/distributori
b) LSP/Richiedenti
c) IAB
d) Forze dell'Ordine o altre organizzazioni governative
e) Organizzazioni professionali di logistica
f) Assicuratori

4. Requisiti TAPA per la Certificazione e gli Audit

I siti sono classificati con uno dei tre livelli di sicurezza, in base al livello di protezione necessaria:

a) Livello A = Elevata protezione di sicurezza
b) Livello B = Moderata protezione di sicurezza
c) Livello C = Protezione di sicurezza standard

Gli LSP/Richiedenti o i Clienti (Buyers) possono ottenere inizialmente la Certificazione di livello C, per poi passare al livello B o A, a seguito dei miglioramenti fatti. Inoltre, come definito tra Cliente (Buyer) e LSP/richiedente, le strutture situate in paesi ad alto rischio possono essere classificate al livello A, mentre tutti gli altri paesi sono classificati con livello B o C. In tutti i casi, è responsabilità del Cliente (Buyer) definire il livello di sicurezza direttamente con l'LSP/richiedente, a seconda della natura della merce e dei rischi specifici.

L'organizzazione può scegliere le tre opzioni seguenti (Tabella 1) per dimostrare la conformità ed essere certificata secondo gli standard di sicurezza TAPA.

L'LSP/Richiedente deve assicurarsi che venga impiegato un IAB o un AA, per completare il processo di audit e certificazione.

Prima che l'audit di certificazione sia programmato/iniziato, gli LSP/Richiedenti devono informare lo IAB o l'AA sul livello di sicurezza che vogliono certificare nel loro processo.

Tabella 1

Tipo	Opzione	Livello	Tipo di Auditor
IAB Audit	Certificazione di un singolo sito	A, B o C	TAPA IAB AA
	Certificazione multi-sito (di più siti)	A, B o C	TAPA IAB AA
Self-Audit	Auto-Certificazione.	C	LSP/Richiedente AA o IAB AA

4.1 Certificazione di un singolo sito

L'ambito della certificazione di un singolo sito deve essere chiaramente definito e lo IAB eseguirà un audit basato su questo ambito. In questo caso, le certificazioni TAPA IAB sono specifiche per singolo sito/struttura. Se i requisiti degli standard di security TAPA, durante l'audit, sono tutti soddisfatti, si considera che l'LSP/Richiedente abbia superato l'audit e lo IAB rilascerà un certificato che indica che il sito specifico dell'LSP/Richiedente è ora certificato secondo lo standard di security TAPA e il livello (A, B o C) applicabile. Lo IAB fornirà a TAPA i risultati dell'audit sotto forma di copie dei certificati emessi o di notifica nel caso di audit non superati.

4.2 Certificazione multi-sito

La Certificazione multi-sito richiede che l'LSP/Richiedente metta in atto un sistema di gestione della security unico volto a garantire che tutti i siti inclusi nel sistema di gestione soddisfino i requisiti dello Standard applicabile. Gli elementi richiesti sono:

- Una funzione centrale identificata.
- Tutti i siti identificati ed elencati nella Certificazione.
- Tutti i siti soggetti a sorveglianza continua e audit interni.

4.2.1 La Funzione Centrale

La funzione centrale può, ma non deve necessariamente, essere la sede centrale dell'LSP/Richiedente. Tuttavia, deve;

- Essere direttamente responsabile del sistema di gestione unico.
- Avere la responsabilità di garantire che tutti i suoi siti all'interno del sistema di gestione siano conformi ai requisiti dello standard FSR.
- Avere l'autorità per erogare azioni correttive e preventive quando necessario in qualsiasi sito.
- Avere un accordo o una politicy documentati che specifichino i ruoli e le responsabilità della funzione centrale e dei siti.

4.2.2 I Siti

Tutti i siti inclusi nel sistema di gestione della security devono avere tra loro un rapporto, che può essere legale o contrattuale, con la funzione centrale dell'organizzazione. Il rapporto non può essere esteso a siti o strutture subappaltatrici incluse nel Sistema di Certificazione multi-sito della funzione centrale.

4.2.3 Verificare la Funzione Centrale

- L'audit del sistema di certificazione della funzione centrale richiede;
- La selezione e l'utilizzo di un IAB approvato da TAPA per l'audit del sistema di gestione della security
- Che lo IAB svolga audit annuali nei confronti della funzione centrale dell'LSP/Richiedente e verifichi la conformità al sistema di gestione della security che comprende, a titolo esemplificativo ma non esaustivo:
    - Le registrazioni, procedure e linee di condotta del sistema di gestione della security delle funzioni centrali sono campionate.
    - Registrazioni disponibili per i siti che fanno parte del sistema di gestione della security che includano i risultati delle verifiche su carta e/o su supporto digitale e la gestione delle non conformità.
- Che lo IAB rilasci all'LSP/Richiedente un certificato TAPA FSR multi-sito che soddisfi tutti i requisiti di conformità.
- Che il certificato multi-sito contenga le date di inizio/fine della certificazione in corso di validità, il numero di siti registrati con i livelli di sicurezza del sistema di gestione della security al momento dell'audit e le eventuali deroghe concesse.

- Il certificato sarà valido per 3 anni. Gli audit svolti nel secondo e terzo anno non richiedono il rilascio di un nuovo certificato, a meno che il sistema di gestione della security non sia cambiato in modo significativo.
- Il certificato multi-sito elenca tutti i siti che fanno parte del sistema di gestione e i relativi livelli di sicurezza.
- Non è consentito avere siti che operano con versioni diverse di FSR. Tutti i siti elencati nel certificato saranno conformi alla versione FSR specificata sul certificato ufficiale multi-sito.
- Se un LSP/Richiedente vuole passare all'ultima versione di FSR prima della scadenza del suo certificato in corso di validità, dovrà essere richiesto un nuovo audit di certificazione.

4.2.4 Verificare i Siti

Le verifiche dei siti prescelti richiederanno:

- Che tutti i siti registrati nel sistema di gestione della security della funzione centrale siano disponibili per l'audit quando selezionati. Nota: qualsiasi sito selezionato per l'audit in un ciclo di 3 anni della certificazione non sarà sottoposto ad un nuovo audit.
- I siti saranno fisicamente sottoposti ad audit a campione (Tabella 2).
- La verifica a campione sarà basata su una selezione casuale del 10% dei siti registrati all'anno.

Tabella 2

	Primo anno	Secondo anno	Terzo anno
Dimensioni del campione	10 % + CF*	10 % + CF*	10 % + CF*

CF – Funzione centrale che svolge il ruolo centrale di gestione del sistema di gestione della security.

4.2.5 Inserimento di Nuovi Siti

L'LSP/Richiedente può richiedere allo IAB l'inserimento di nuovi siti o di un nuovo gruppo di siti all'interno di un'organizzazione già certificata multi-sito, in occasione o prima del ciclo annuale di verifiche del sito tramite IAB. Lo IAB includerà questi siti aggiuntivi nel totale dei siti quando andrà a selezionare il campione da sottoporre ad audit.

L'LSP/Richiedente deve assicurarsi che tutti i nuovi siti siano stati verificati internamente e che soddisfino il livello di sicurezza richiesto prima di chiedere la loro aggiunta al sistema di gestione. Questo processo deve essere documentato e reso disponibile allo IAB su richiesta.

Se l'audit dello IAB viene completato con successo, lo IAB riemette i certificati alla funzione centrale con i nuovi siti inclusi.

4.2.6 Rimozione di Siti

L'LSP/Richiedente può rimuovere alcuni siti dal sistema di gestione della security cancellandoli dall'elenco dei siti e informando formalmente lo IAB. Lo IAB revocherà le certificazioni dei singoli siti e adeguerà e riemetterà il Certificato multi-sito. Lo IAB prenderà nota della rimozione dei siti nel totale per la selezione al momento dell'audit a campione.

4.2.7 Cambio di Livello in Siti esistenti

L'LSP/Richiedente può modificare il livello di certificazione dei siti inclusi nel sistema di gestione della security. Una richiesta di modifica del livello deve essere formalmente inviata allo IAB. I siti che vengono declassati saranno automaticamente accettati al livello di certificazione inferiore. I siti che devono avere livelli di certificazione maggiori saranno inclusi negli audit a campione di quell'anno o, nel caso in cui gli audit a campione siano già stati effettuati o non possano essere completati entro 60 giorni, verrà richiesto un nuovo audit da parte dello IAB.

4.2.8 Passaggio da Singolo sito a Multi-sito

Gli LSP/Richiedenti che desiderano includere qualunque certificazione di un singolo sito preesistente in un sistema di gestione della security multi-sito, devono assicurarsi che i siti siano pienamente conformi alla stessa versione FSR riportata nel certificato multi-sito. La certificazione multi-sito non può incorporare versioni diverse dello standard FSR.

4.3 Auto-Certificazione (solo livello C)

L'auto-certificazione è applicabile solo al livello C. L'auto-certificazione (Tabella 3) deve essere eseguita da un AA dell'LSP/Richiedente o da un AA dello IAB. Un AA dell'LSP/Richiedente può essere un dipendente interno/associato, formato rispetto alla versione attuale del TAPA FSR, registrato e autorizzato da TAPA come AA. Indipendentemente dal tipo di auditor utilizzato per condurre l'auto-certificazione, il modulo di audit compilato deve essere presentato a TAPA per ricevere la Certificazione di livello C.

Tabella 3

Opzione	Descrizione	Livello	Tipo di Auditor*
Auto-Certificato	Auto-Certificazione.	C	LSP/Richiedente IAB o AA

L'audit viene effettuato utilizzando l'attuale audit form di TAPA e fornendo informazioni ed evidenze sufficienti a garantire a TAPA la conformità ai requisiti dello Standard di security TAPA applicabile. L'autocertificazione è specifica per sito/struttura. Se i requisiti dell'audit TAPA sono tutti soddisfatti, si considera che l'LSP/Richiedente abbia superato l'audit e sarà certificato al livello C dello Standard di security applicabile per quella specifica struttura.

5. Ri-Certificazione

Tutte le certificazioni di security TAPA FSR sono valide per un periodo di tre (3) anni senza possibilità di estensione.
Per evitare che la certificazione decada, prima della data di scadenza del certificato in corso di validità deve essere effettuato un audit di ri-certificazione. Anche il completamento di eventuali SCAR deve avvenire entro il periodo di 60 giorni e prima della data di scadenza del certificato in corso di validità.

Pertanto, per garantire un'adeguata pianificazione e preparazione, si raccomanda che l'LSP/Richiedente pianifichi l'audit di ri-certificazione tre (3) mesi prima della data di scadenza del certificato. Se il certificato dello standard di Security TAPA viene rilasciato entro il suddetto periodo di tre mesi, la data riportata sul nuovo certificato sarà la data di scadenza dell'attuale certificazione. Se le azioni correttive non vengono chiuse prima della data di scadenza e non viene concessa alcuna deroga, la certificazione scadrà.

Un LSP/Richiedente o Cliente (Buyer) può richiedere una ri-certificazione se una delle parti ritiene che il livello di classificazione sia cambiato. I costi per la ri-certificazione TAPA sono a carico dell'LSP/Richiedente, a meno che non sia stato negoziato diversamente con il/i Cliente/i (Buyer/s).

6. Audit di Follow Up

L'LSP/Richiedente si assicurerà di disporre di un processo interno per monitorare la conformità, negli anni che intercorrono tra gli audit formali (vedi tabella 4) condotti da un IAB AA o da un LSP/Richiedente AA, a seconda dei casi.

6.1 Azione Correttiva / SCAR

Una sintesi informale dei rilievi dovrebbe essere condivisa con l'LSP/Richiedente durante il meeting di chiusura dell'audit. Lo IAB o l'AA informerà l'LSP/Richiedente dei risultati dell'audit entro dieci (10) giorni lavorativi dal completamento dello stesso. Eventuali ritardi nell'emissione dei risultati dell'audit devono essere comunicati tempestivamente all'LSP/Richiedente e concordati tra lo IAB o l'AA e l'LSP/Richiedente.

Se uno qualsiasi dei requisiti non è soddisfatto, come emerso durante l'audit, l'AA presenta un Security Corrective Action Requirement (SCAR) al relativo LSP/Richiedente. L'LSP/Richiedente deve rispondere allo IAB o all'AA entro dieci (10) giorni lavorativi, documentando l'azione da intraprendere e la data in cui l'azione sarà completata. Le date di completamento delle SCAR possono essere definite tra lo IAB o l'AA e l'LSP/Richiedente. Tuttavia, l'attuazione delle azioni correttive non deve superare i sessanta (60) giorni dalla notifica all'LSP/Richiedente, a meno che il Regional Tapa Waiver Committee non approvi una deroga. L'LSP/Richiedente non può cercare di escludere un sito con una SCAR aperta dall'elenco totale dei siti nel sistema di certificazione multi-sito.

In tutti i casi, l'LSP/Richiedente deve presentare allo IAB o all'AA aggiornamenti/rapporti sullo stato di avanzamento di tutte le SCAR in sospeso. Ogni SCAR non completata prima della data di scadenza sarà comunicata in escalation dal Rappresentante per la Security dell'LSP/Richiedente alla Direzione

dell'LSP/Richiedente. Il motivo o i motivi della mancata conformità devono essere documentati e comunicati allo IAB o all'AA.

Nota 1: Non è necessario che lo IAB o l'AA effettuino un nuovo audit del sito per chiudere una SCAR. La prova della chiusura di una SCAR (ossia il raggiungimento della conformità) può essere presentata allo IAB o all'AA sotto forma di corrispondenza scritta, riunioni web o teleconferenze, fotografie, ecc.

Nota 2: Per la certificazione del sistema di gestione della security multi-sito, qualsiasi SCAR non chiusa o soggetta a un'estensione approvata può comportare la sospensione o la revoca dello stato di certificazione multi-sito dell'LSP/Richiedente e quindi tutti i siti non saranno più considerati certificati.

6.2 Monitoraggio della conformità

I self-audit intermedi effettuati dall'LSP/Richiedente devono essere completati secondo la Tabella 4 “Programma di audit e monitoraggio della conformità”. Il requisito del self audit intermedio si applica a tutti i siti e a tutti i livelli di certificazione e deve essere documentato sul TAPA audit form ufficiale e presentato allo **IAB** o per l'auto-certificazione a TAPA entro 30 giorni dalla data di scadenza della certificazione in corso.

Il self-audit intermedio deve essere effettuato dall'AA dell'LSP/Richiedente. Tutti gli AA devono aver sostenuto e superato l'esame relativo allo standard TAPA di riferimento e nella versione con cui sono tenuti ad effettuare l'audit.

La mancata conformità comporterà la sospensione della certificazione originale fino al completamento del self-audit intermedio. Le criticità individuate devono essere documentate, deve essere assegnata una data di scadenza per il completamento delle azioni correttive e le stesse devono essere tracciate fino alla chiusura entro 60 giorni.

Tabella 4: Programma di audit e monitoraggio della conformità

Ref	Azione	Frequenza	A	B	C
Certificazione di un singolo sito:					
6.2.1	Audit di Certificazione di un singolo sito (Audit di Certificazione IAB/AA)	Ogni tre (3) anni	✔	✔	✔
6.2.2	Self-audit intermedi di un singolo sito (AA dell'LSP/Richiedente)	Annualmente al 1° e 2° anniversario	✔	✔	✔

Certificazione multi-sito:					
6.2.3	Audit di certificazione della funzione centrale multi-sito (Audit di Certificazione IAB/AA)	Ogni tre (3) anni	✔	✔	✔
6.2.4	Audit delle funzioni centrali multi-sito (IAB/AA)	Annualmente al 1° e 2° anniversario	✔	✔	✔
6.2.5	Self-audit intermedi multi-sito (AA dell'LSP/Richiedente per tutti i siti in una certificazione multi-sito)	Ogni anno	✔	✔	✔
6.2.6	Audit a campione multi-sito (IAB/AA per il 10% dei siti in una certificazione multi-sito)	Ogni anno	✔	✔	✔

Auto-Certificazione					
6.2.7	Audit di auto-certificazione dell'LSP/Richiedente	Ogni tre (3) anni			✔
6.2.8	Self-audit intermedi (AA dell'LSP/Richiedente solo per l'auto-certificazione)	Annualmente al 1° e 2° anniversario			✔

7. Deroghe

Panoramica

Una deroga è un'approvazione scritta concessa per esentare un LSP/Richiedente da uno specifico requisito TAPA o per accettare una soluzione alternativa di conformità. Una deroga può essere richiesta se un LSP/Richiedente non è in grado di soddisfare un requisito specifico dell'FSR e può fornire misure alternative per soddisfare il requisito dello Standard di security. Le deroghe sono valide per il periodo della certificazione. Consultare l'FSR corrente per il processo di richiesta di deroga.

Publishing and copyright information

Publication history

First published in January 2020

First (present) edition published in January 2020

This Publicly Available Specification comes into effect on 1st July 2020