UNI/PdR 186-6:2026	Requisiti per l'identificazione e la valutazione del livello di rischio basso per il rilascio del Report certificativo secondo l'art. 3 del d.lgs. 103/2024 – Parte 6: ambito tutela della fede pubblica
Sommario	La presente prassi di riferimento tratta i requisiti per l'identificazione e la valutazione del livello di rischio per l'ambito omogeneo tutela della fede pubblica secondo l'art. 3 del d.lgs. 103/2024.
Data	2026-xx-xx

Avvertenza

Il presente documento è un progetto di Prassi di Rifermento (UNI/PdR) sottoposta alla fase di consultazione, da utilizzare solo ed esclusivamente per fini informativi e per la formulazione di commenti.

Il processo di elaborazione delle Prassi di Riferimento prevede che i progetti vengano sottoposti alla consultazione sul sito web UNI per raccogliere i commenti del mercato: la UNI/PdR definitiva potrebbe quindi presentare differenze rispetto al documento messo in consultazione.

Questo documento perde qualsiasi valore al termine della consultazione, cioè il: 3 settembre 2026

UNI non è responsabile delle conseguenze che possono derivare dall'uso improprio del testo dei progetti di Prassi di Riferimento in consultazione.

UNI
UN MONDO FATTO BENE

PREMESSA

La presente prassi di riferimento UNI/PdR 186-6:2026 non è una norma nazionale, ma è un documento pubblicato da UNI, come previsto dal Regolamento UE n.1025/2012, che raccoglie prescrizioni relative a prassi condivise all'interno del seguente soggetto firmatario di un accordo di collaborazione con UNI:

Governo Italiano

Ministero delle Imprese e del Made in Italy

Decreto legislativo 12 luglio 2024, n.103

La presente prassi di riferimento è stata elaborata dal Tavolo “Definizione del livello di rischio basso ai sensi del d.lgs. 103/2024” condotto da UNI, costituito dai seguenti esperti:

XXX

La presente prassi di riferimento è stata ratificata dal Presidente dell’UNI il xx xxxx 2026.

Le prassi di riferimento, adottate esclusivamente in ambito nazionale, rientrano fra i “prodotti della normazione europea”, come previsti dal Regolamento UE n.1025/2012, e sono documenti che introducono prescrizioni tecniche, elaborati sulla base di un rapido processo ristretto ai soli autori, sotto la conduzione operativa di UNI.

Le prassi di riferimento sono disponibili per un periodo non superiore a 5 anni, tempo massimo dalla loro pubblicazione entro il quale possono essere trasformate in un documento normativo (UNI, UNI/TS, UNI/TR) oppure devono essere ritirate.

Chiunque ritenesse, a seguito dell’applicazione della presente prassi di riferimento, di poter fornire suggerimenti per un suo miglioramento è pregato di inviare i propri contributi all’UNI, Ente Italiano di Normazione, che li terrà in considerazione.

SOMMARIO

1 SCOPO E CAMPO DI APPLICAZIONE

La presente prassi di riferimento ha come scopo l'identificazione dei parametri di definizione del livello di rischio basso per rilascio da parte di enti di certificazione accreditati di un Report certificativo, ai sensi del Decreto Legislativo 12 luglio 2024, n. 103 Semplificazione dei controlli sulle attività economiche, in attuazione della delega al Governo di cui all'articolo 27, comma 1, della legge 5 agosto 2022, n. 118 (d.lgs. 103/2024).

Le imprese che ricadono nel campo di applicazione del d.lgs. 105/2015 sono da considerare escluse dall'applicazione della prassi in oggetto.

La presente parte della prassi di riferimento definisce i requisiti per l'identificazione e la valutazione del livello di rischio basso per il rilascio del Report certificativo secondo l'art. 3 del d.lgs. 103/2024 per l'ambito omogeneo d) tutela della fede pubblica. Il presente documento si intende applicato come specificato nel punto 5.

2 RIFERIMENTI NORMATIVI E LEGISLATIVI

La presente parte di prassi di riferimento rimanda, mediante riferimenti datati e non, a disposizioni contenute in altre pubblicazioni. Tali riferimenti normativi e legislativi sono citati nei punti appropriati del testo e sono di seguito elencati. Per quanto riguarda i riferimenti datati, successive modifiche o revisioni apportate a dette pubblicazioni valgono unicamente se introdotte nella presente parte di documento come aggiornamento o revisione. Per i riferimenti non datati vale l'ultima edizione della pubblicazione alla quale si fa riferimento.

UNI EN ISO 9000 Sistemi di gestione per la qualità - Fondamenti e vocabolario

UNI EN ISO 9001 Sistemi di gestione per la qualità - Requisiti

UNI EN ISO 14001 Sistemi di gestione ambientale - Requisiti e guida per l'uso

UNI CEI EN ISO/IEC 17000 Valutazione della conformità - Vocabolario e principi generali

UNI EN ISO 22301 Sicurezza e resilienza - Sistemi di gestione per la continuità operativa – Requisiti

UNI CEI EN ISO/IEC 27001 Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni - Requisiti

UNI CEI EN ISO/IEC 27701 Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione delle informazioni sulla privacy - Requisiti e linee guida

UNI ISO 14298 Tecnologia grafica - Gestione dei processi di stampa di sicurezza

UNI ISO 28000 Sicurezza e resilienza - Sistemi di gestione della sicurezza - Requisiti

UNI ISO 37001 Sistemi di gestione per la prevenzione della corruzione - Requisiti e guida all'utilizzo

UNI ISO 37301 Sistemi di gestione per la compliance - Requisiti con guida per l'utilizzo

UNI/PdR 186-1 Requisiti per l'identificazione e la valutazione del livello di rischio basso per il rilascio del Report certificativo secondo l'art. 3 del d.lgs. 103/2024 – Parte 1: aspetti generali

Decreto Legislativo 12 luglio 2024, n. 103 Semplificazione dei controlli sulle attività economiche, in attuazione della delega al Governo di cui all'articolo 27, comma 1, della legge 5 agosto 2022, n. 118

3 TERMINI E DEFINIZIONI

Ai fini del presente documento valgono i termini e le definizioni della UNI EN ISO 9000 e della UNI CEI EN ISO/IEC 17000.

4 PRINCIPIO

La presente prassi di riferimento ha come scopo l'interpretazione dell'art. 3 "Sistema di identificazione e valutazione del livello di rischio "basso"" del d.lgs. 103/2024, il quale identifica cinque ambiti omogenei come base per un sistema di identificazione e gestione del rischio su base volontaria:

a) protezione ambientale;

b) igiene e salute pubblica;

c) sicurezza pubblica;

d) tutela della fede pubblica;

e) sicurezza dei lavoratori.

La presente parte della prassi di riferimento definisce i requisiti della valutazione del rischio basso per le organizzazioni nell'ambito omogeneo d) tutela della fede pubblica.

5 AMBITO OMOGENEO D) TUTELA DELLA FEDE PUBBLICA

L'ambito omogeneo tutela della fede pubblica riguarda l'insieme delle misure, delle procedure e delle condizioni organizzative finalizzate a prevenire e contrastare fenomeni di falsificazione, contraffazione, alterazione, frode e uso indebito di segni, documenti, titoli, certificazioni e informazioni aventi rilievo pubblico, nonché a garantire l'autenticità, l'integrità, la tracciabilità e l'affidabilità delle attestazioni e delle dichiarazioni rese nell'ambito dell'attività economica.

La tutela della fede pubblica, quindi, costituisce un insieme di principi, leggi e misure organizzative e di controllo, poste dall'ordinamento giuridico, volte a garantire la veridicità, completezza, integrità, tracciabilità e legittimità delle informazioni e dei documenti prodotti o utilizzati dalle imprese. Essa si fonda sulla presunzione di affidabilità di tali informazioni e mira a prevenire frodi e alterazioni idonee a generare danni economico-sociali, salvaguardando l'affidamento della collettività e la certezza dei rapporti giuridici.

La presente parte della prassi di riferimento deve essere applicata in congiunzione con la UNI/PdR 186-1, la quale definisce gli aspetti generali ritenuti validi per tutti gli ambiti omogenei e pertanto contiene dei requisiti e delle informazioni integrative per l'applicazione della presente prassi di riferimento.

6 IDENTIFICAZIONE E VALUTAZIONE DEL LIVELLO DI RISCHIO NELL'AMBITO TUTELA DELLA FEDE PUBBLICA

6.1 Generale

A fronte della fascia di classificazione per dimensione e del tipo di impatto dell'attività effettiva dell'impresa sulla tutela della fede pubblica, viene definita per l'ambito omogeneo tutela della fede pubblica la lista di certificazioni ed evidenze (o procedura equivalente) applicabili per l'assegnazione del livello di rischio basso.

L'ambito omogeneo tutela della fede pubblica interessa imprese che operano in settori e contesti diversi, nei quali l'attività economica può incidere sulla fiducia del pubblico e delle istituzioni nella conformità di prodotti, documenti, attestazioni e informazioni. Rientrano, a titolo esemplificativo, le organizzazioni coinvolte in processi di produzione e distribuzione con requisiti di tracciabilità, nell'emissione e gestione di documentazione con valore probatorio o amministrativo, nella gestione di dati e identità digitali, nonché nelle filiere esposte a rischio di frode e contraffazione.

I principali soggetti che possono effettuare controlli o svolgere funzioni di vigilanza rilevanti per la tutela della fede pubblica presso le imprese o in via telematica (in relazione alla specifica attività svolta) includono, a titolo non esaustivo: Camere di Commercio; Agenzia delle Entrate; autorità e amministrazioni competenti al rilascio/gestione di titoli abilitativi, certificazioni e autorizzazioni; Agenzia delle Dogane e dei Monopoli per gli ambiti di competenza; autorità di vigilanza e controllo su prodotti e mercati (per esempio in materia di etichettatura, tracciabilità, marchi e indicazioni); nonché le autorità di pubblica sicurezza e giudiziarie nei casi di accertamento di reati di falsità, frode e contraffazione.

Diversamente dagli ambiti omogenei a) protezione ambientale, b) igiene e salute pubblica ed e) sicurezza dei lavoratori, nei quali sono previsti sistemi strutturati di vigilanza tecnica periodica, nell'ambito omogeneo tutela della fede pubblica i controlli sono spesso connessi alla correttezza documentale e dichiarativa, alla conformità dei processi di tracciabilità e rintracciabilità, alla prevenzione delle frodi, alla gestione delle identità e degli accessi (anche digitali) e alla correttezza delle informazioni rese al pubblico e alle autorità competenti. In funzione del settore, possono inoltre intervenire controlli mirati su filiere e prodotti a rischio, anche a seguito di segnalazioni, ispezioni documentali e verifiche di conformità.

6.2 Soggetti interessati e coinvolti

La procedura si applica a tutte le imprese di qualsiasi settore e dimensione secondo lo scopo e campo di applicazione di cui al punto 1.

6.3 Impatto sulla tutela della fede pubblica dei soggetti interessati e coinvolti

6.3.1 Generale

Le imprese di cui al punto 6.2 sono di seguito classificate in base all'impatto sulla tutela della fede pubblica determinato dall'ambito di attività e dai rischi di falsità, frode e contraffazione mitigati nel settore di attività.

Differentemente dagli ambiti trattati dalla UNI/PdR 186-2, UNI/PdR 186-3 e UNI/PdR 186-4, le imprese non sono classificate in base alla criticità del settore, ed è svolta una valutazione del fattore

di rischio basata sull'attività effettiva dell'impresa che, a prescindere dal settore, può avere un maggiore o minore impatto sugli aspetti di tutela della fede pubblica.

L'impatto identificato sulla fede pubblica non rientra in maniera esplicita come parametro all'interno del prospetto 3 degli elementi minimi per la determinazione del rischio basso in quanto è considerato e coperto dalla parte specialistica o, ove applicabile, dalla procedura equivalente.

6.3.2 Norme di sistema di gestione

La seguente lista riporta le norme di sistema di gestione che, pur avendo carattere trasversale, risultano funzionalmente collegate all'ambito omogeneo della tutela della fede pubblica, in quanto idonee a presidiare assetti organizzativi, processi e misure che concorrono alla prevenzione e alla mitigazione dei relativi rischi.

- UNI EN ISO 9001 Sistemi di gestione per la qualità - Requisiti
- UNI CEI EN ISO/IEC 27001 Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni - Requisiti
- UNI ISO 37001 Sistemi di gestione per la prevenzione della corruzione - Requisiti e guida all'utilizzo
- UNI ISO 37301 Sistemi di gestione per la compliance - Requisiti con guida per l'utilizzo

6.3.3 Impatti sulla tutela della fede pubblica

Il prospetto 1 identifica a titolo esemplificativo i principali contesti di rilevanza per l'ambito omogeneo della tutela della fede pubblica e il tipo di impatto che essi hanno. A ciascun contesto è applicata una norma di sistema di gestione di cui al punto 6.3.2 che ha lo scopo di mitigare i rischi identificati.

Prospetto 1 – Associazione tra contesti di impatto sulla tutela della fede pubblica e norme di sistema di gestione

Contesto	**Tipo di impatto sulla tutela della fede pubblica**	**Norma**	**Rischi mitigati**	**Settori tipici di applicazione**
Sicurezza delle informazioni	Alto	**UNI CEI EN ISO/IEC 27001**	Alterazioni/indisponibilità di dati, manipolazione registri, accessi indebiti	Servizi digitali, gestori dati, filiere con sistemi di tracciabilità
Gestione anticorruzione	Medio	**UNI ISO 37001**	Frode, collusione, alterazioni di esiti e attestazioni	Trasversale; filiere regolamentate

Gestione della compliance	Medio	**UNI ISO 37301**	Inadempienze, dichiarazioni non corrette, gestione inadeguata requisiti cogenti	Trasversale (settori con obblighi dichiarativi/certificativi)
Gestione per la qualità	Indiretto	**UNI EN ISO 9001**	Non conformità di processo, errori documentali, prodotti e servizi difettosi	Trasversale (produzione e servizi)

6.3.4 Norme specialistiche

La seguente lista riporta le norme specialistiche che risultano direttamente collegate all'ambito omogeneo della tutela delle fede pubblica, con riferimento a tracciabilità, antifrode, sicurezza della supply chain, gestione della sicurezza nella stampa e protezione dei dati.

- UNI EN ISO 22301 Sicurezza e resilienza - Sistemi di gestione per la continuità operativa - Requisiti
- UNI CEI EN ISO/IEC 27001 Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni - Requisiti
- UNI CEI EN ISO/IEC 27701 Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione delle informazioni sulla privacy - Requisiti e linee guida
- UNI ISO 28000 Sicurezza e resilienza - Sistemi di gestione della sicurezza - Requisiti
- UNI ISO 14298 Tecnologia grafica - Gestione dei processi di stampa di sicurezza
- UNI ISO 37001 Sistemi di gestione per la prevenzione della corruzione - Requisiti e guida all'utilizzo
- UNI ISO 37301 Sistemi di gestione per la compliance - Requisiti con guida per l'utilizzo

NOTA — Le norme elencate nel presente punto fanno riferimento a schemi di certificazione il cui stato di accreditamento può variare nel tempo. Alla data di pubblicazione della presente prassi, alcune norme risultano oggetto di accreditamento da parte degli organismi competenti, mentre per altre tale stato è in fase di sviluppo.

Ai fini dell'applicazione della presente prassi, sono ritenute valide esclusivamente le certificazioni rilasciate sotto accreditamento come specificato nella UNI/PdR 186-1. Pertanto, è responsabilità dell'organizzazione e dell'ente di certificazione verificare l'effettivo stato di accreditamento dello schema alla data di valutazione.

6.3.5 Impatti sulla tutela della fede pubblica

Il prospetto 2 identifica a titolo esemplificativo i contesti specifici di rilevanza per l'ambito omogeneo della tutela della fede pubblica e il tipo di impatto che essi hanno. A ciascun contesto è applicata una norma specialistica di cui al punto 6.3.4 che ha lo scopo di mitigare i rischi identificati.

Prospetto 2 – Associazione tra contesti di impatto sulla tutela della fede pubblica e norme specialistiche

Contesto	Tipo di impatto sulla tutela della fede pubblica	Norma	Rischi mitigati	Settori tipici di applicazione
Gestione della sicurezza nella stampa	Molto alto	**UNI ISO 14298**	Falsificazione di documenti/materiali sensibili, accessi non autorizzati, sottrazione supporti di sicurezza	Stampa di sicurezza, documenti e moduli controllati
Sicurezza della catena di approvvigionamento	Alto	**UNI ISO 28000**	Manomissioni, sostituzioni, ingresso merci contraffatte, alterazione catena di custodia	Logistica, import/export, filiere ad alto valore
Sicurezza delle informazioni	Alto	**UNI CEI EN ISO/IEC 27001**	Manipolazione dati, alterazione log, frodi digitali, compromissione di evidenze e audit trail	Piattaforme, servizi digitali, registri, conservazione digitale
Continuità operativa	Medio	**UNI ISO 22301**	Interruzione dei controlli, perdita tracciabilità, indisponibilità di registri/attestazioni	Servizi essenziali, piattaforme, grandi filiere

6.4 Elementi minimi per la determinazione del livello di rischio basso ai fini del rilascio del Report certificativo

Il presente punto definisce le varie combinazioni possibili tra certificazioni rispetto a norme di sistema di gestione (o valutazione positiva secondo la procedura equivalente) e norme più direttamente legate alla tutela della fede pubblica che consentono all'impresa di ottenere un Report certificativo secondo la presente UNI/PdR.

La valutazione per la determinazione del livello di rischio basso nell'ambito omogeneo tutela della fede pubblica deve tenere conto dei seguenti elementi minimi:

a) una certificazione di una norma di sistema di gestione tra quelle elencate nel punto 6.3.2;

b) l'attuazione della procedura equivalente di cui al punto 6.5;

c) una norma specialistica tra quelle elencate nel punto 6.3.4.

In particolare, per rilascio del Report certificativo secondo la presente parte di UNI/PdR, l'impresa deve essere in possesso di una delle seguenti combinazioni di elementi minimi:

- Combinazione a) + c): una certificazione di una norma di sistema di gestione tra quelle elencate nel punto 6.3.2, e di una norma specialistica tra quelle elencate nel punto 6.3.4. In questo caso, la norma di sistema e la norma specialistica devono essere differenti.

- Combinazione a) + b): una certificazione di una norma di sistema di gestione tra quelle elencate nel punto 6.3.2, e l'attuazione della procedura equivalente di cui al punto 6.5. In questo caso, si applicano solamente i punti della procedura equivalente che non sono già coperti dalla norma di sistema di gestione per cui l'impresa è certificata.

ESEMPIO: Se un'impresa è certificata secondo la UNI EN ISO 9001, non ha bisogno di applicare il punto 9 della procedura equivalente (prospetto 4) in quanto esso è già compreso tra i requisiti della UNI EN ISO 9001.

- Combinazione b) + c): l'attuazione della procedura equivalente di cui al punto 6.5, e la certificazione di una norma specialistica tra quelle elencate nel punto 6.3.4. In questo caso, si applicano solamente i punti della procedura equivalente che non sono già coperti dalla norma di sistema di gestione per cui l'impresa è certificata.

- Combinazione solo b): l'attuazione della procedura equivalente di cui al punto 6.5. Questa opzione può essere utilizzata solo dalle imprese che rientrano nelle fasce dimensionali 1 e 2, determinate secondo i criteri riportati nella UNI/PdR 186-1. Questa combinazione può essere applicata solo per attività che hanno impatto fino a medio per la fede pubblica secondo i punti 6.3.3 e 6.3.5.

Le combinazioni per l'ottenimento del Report certificativo per l'ambito omogeneo tutela delle fede pubblica sono sintetizzate nel prospetto 3 sottostante.

Prospetto 3 – Elementi minimi per la determinazione del livello di rischio basso

Ottenimento Report certificativo?			
Elementi per la certificazione	**a) norma di sistema**	**b) procedura equivalente**	**c) norma specialistica**
a) norma di sistema	-	Sì[1]	Sì[2]
b) procedura equivalente	Sì[1]	Solo per imprese di fascia dimensionale 1[3] e 2[3]	Sì[1]
c) norma specialistica	Sì[2]	Sì[1]	-
1) Si applicano solamente i punti della procedura equivalente che non sono già coperti dalla norma			

(di sistema di gestione o specialistica) per cui l'impresa è già certificata.

2) Applicabile a condizione che la certificazione della norma di sistema e la certificazione della norma specialistica siano diverse.

3) L'utilizzo della sola procedura equivalente per l'ottenimento del Report certificativo si applica solamente alle imprese di fascia dimensionale 1 e 2, e può essere applicata solo per attività che hanno impatto fino a medio per la fede pubblica.

6.5 Procedura equivalente per la classificazione di rischio basso

Esclusivamente nei casi previsti dal punto 6.4, il soggetto richiedente può attuare la procedura equivalente indicata nel prospetto 4 ai fini dell'ottenimento del Report certificativo per l'ambito tutela della fede pubblica.

Il prospetto 4 riporta l'elenco di informazioni documentate che l'organizzazione deve presentare, ove applicabili, e le evidenze a esse collegate, ovvero degli esempi dei documenti richiesti per la valutazione dell'ambito ovvero del possesso del requisito richiesto nell'opzione b) di cui al punto 6.4. L'ente di certificazione può richiedere ulteriori evidenze documentate nel caso in cui quelle già fornite non siano ritenute esaustive.

Prospetto 4 – Checklist per la procedura equivalente nell'ambito tutela della fede pubblica

	INFORMAZIONE DOCUMENTATA	**EVIDENZA**
1	Mappatura dei processi e dei punti in cui si generano/gestiscono documenti, registrazioni, attestazioni o dichiarazioni rilevanti (cartacee e digitali) riferibili a stati soggettivi e a processi, servizi, prodotti	Elenco processi Flow chart Matrice documentale
2	Elenco autorizzazioni, riconoscimenti, registrazioni, licenze, iscrizioni e comunicazioni obbligatorie pertinenti e stato di validità	Registro scadenze Copie titoli Ricevute invii/PEC Protocolli
3	Procedura di gestione e controllo della documentazione (creazione, approvazione, distribuzione, modifica, archiviazione, conservazione)	Documento recante la procedura di gestione e controllo della documentazione Registri revisioni Log del sistema documentale

4	Criteri di identificazione univoca, tracciabilità e rintracciabilità (lotti, seriali, registri), controlli su fornitori e canali, gestione resi e segnalazioni per la tracciabilità e l'antifrode	Matrice tracciabilità Registri lotti/seriali Criteri campionamento controlli
5	Valutazione dei rischi di falsificazione/contraffazione/alterazione e piano di trattamento (misure fisiche, procedurali e digitali)	Risk assessment Registro rischi Piano controlli
6	Gestione delle identità e degli accessi (fisici e digitali) ai sistemi e agli archivi rilevanti, inclusa segregazione dei compiti	Profili/ruoli Log accessi Procedure autorizzative Audit trail
7	Piano di controlli interni e verifiche (campionamenti, controlli in accettazione, controlli su etichettatura e comunicazioni)	Piano controlli Report verifiche e relative registrazioni Azioni correttive
8	Gestione incidenti/segnalazioni, comunicazioni alle parti interessate e ritiro/richiamo se applicabile	Registro incidenti Evidenze investigazioni Comunicazioni Corrective and preventive action (CAPA)
9	Eventuali non conformità, sanzioni o contestazioni pertinenti e relativa gestione degli ultimi 3 anni	Evidenze chiusura non conformità (NC) Provvedimenti Azioni correttive
10	Rispetto dei requisiti cogenti e tecnici per i fornitori di servizi/prodotti critici pertinenti la fede pubblica (ove applicabile) (per esempio, verifica periodica dei registratori di cassa, strumenti di misura utilizzati per una funzione	Elenco dei fornitori critici per la fede pubblica e relative registrazioni

	di misura legale)	

BIBLIOGRAFIA

[1] UNI CEI EN ISO/IEC 17020:2012 Valutazione della conformità - Requisiti per il funzionamento di vari tipi di organismi che eseguono ispezioni.

[2] UNI CEI EN ISO/IEC 17021-1:2015 Valutazione della conformità - Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione

[3] UNI CEI EN ISO/IEC 17029:2019 Valutazione della conformità - Principi e requisiti generali per gli Organismi di Validazione e Verifica

[4] Decreto 17 settembre 2024, n. 159 Regolamento di attuazione dell'articolo 4, comma 6 del decreto legislativo 25 novembre 2016, n. 219, relativo alla formazione e gestione del fascicolo informatico d'impresa

[5] ISO 12931 Performance criteria for authentication solutions used to combat counterfeiting of material goods.

[6] ISO 22380 Product authentication and verification.

[7] ISO/IEC 24760-1 Identity management — Part 1: Terminology and concepts.

[8] ISO/IEC 30107-3 Information technology — Biometric presentation attack detection — Part 3: Testing and reporting.

[9] ISO 14298 Management of security printing processes.

[10] Decreto Legislativo 12 luglio 2024, n. 103 Semplificazione dei controlli sulle attività economiche (d.lgs. 103/2024).

[11] ISO 22383 Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for the selection and performance evaluation of authentication solutions for material goods

[12] ISO 22380 Sicurezza e resilienza - Autenticità, integrità e affidabilità di prodotti e documenti - Principi generali afferenti al rischio di frode sui prodotti e contromisure

[13] UNI CEI EN ISO/IEC 24760 (serie) Tecnologie informatiche - Tecniche di sicurezza - Un quadro di riferimento per la gestione delle identità