SECURE
Cyber Resilience for SMEs

Quadro metodologico per la valutazione della conformità al CRA

20/10/2025

Funded by the European Union

Dichiarazione sui finanziamenti dell'UE: Finanziato dall'Unione europea nell'ambito del GA n. 101190325. I punti di vista e le opinioni espressi sono tuttavia esclusivamente quelli degli autori e non riflettono necessariamente quelle dell'Unione europea o del Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca.
Né l'Unione europea né l'autorità che eroga il finanziamento possono essere ritenute responsabili per tali opinioni.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Dichiarazione di non responsabilità dell'ECCC: Il progetto è sostenuto dal Centro europeo di competenza per la cibersicurezza e dai suoi membri

DICHIARAZIONE DI NON RESPONSABILITÀ

Questa versione è una traduzione del documento originale in lingua inglese; in caso di discrepanze o ambiguità interpretative, prevale la versione originale in inglese.

Indice

Elenco delle tabelle e delle figure

Abbreviazioni

AES – Standard di crittografia avanzato

API – Interfaccia di programmazione dell'applicazione

CI/CD – Integrazione continua e distribuzione/implementazione continua

CIS – Centro per la sicurezza di Internet

CRA – Regolamento sulla ciberresilienza

CSIRT – Computer Security Incident Response Team

CVD – Divulgazione coordinata delle vulnerabilità

CVE – Vulnerabilità ed esposizioni comuni

CVSS – Sistema comune di valutazione delle vulnerabilità

CWE – Enumerazione comune delle vulnerabilità

DDoS – Attacco distribuito di tipo "Denial of Service"

DMS – Sistema di gestione dei documenti

DPIA – Valutazione d'impatto sulla protezione dei dati

ECDSA – Algoritmo di firma digitale a curva ellittica

ENISA – Agenzia dell'Unione europea per la cibersicurezza

ETSI – Istituto europeo di normazione tecnica

UE – Unione europea

DoC UE – Dichiarazione di conformità dell'Unione europea

EUCS – Sicurezza del cloud nell'UE

FTP – Protocollo di trasferimento file

GDPR – Regolamento generale sulla protezione dei dati

IDS – Sistema di rilevamento delle intrusioni

IEC – Commissione Elettrotecnica Internazionale

IoT – Internet delle cose

IPS – Sistema di prevenzione delle intrusioni

ISO – Organizzazione internazionale per la normazione

MFA – Autenticazione a più fattori

NB – Organismo notificato

NIST – Istituto Nazionale di Standard e Tecnologia (Stati Uniti)

NIST NVD – Banca dati nazionale delle vulnerabilità del NIST

OCTAVE – Valutazione operativa delle minacce, delle risorse e delle vulnerabilità critiche

OTA – Over The Air

OWASP – Progetto aperto mondiale sulla sicurezza delle applicazioni

OWASP ESAPI – API di sicurezza aziendale OWASP

OWASP SAMM – Modello di maturità per la garanzia del software OWASP

OWASP ZAP – Proxy di attacco OWASP Zed

PASTA – Processo per la simulazione di attacchi e l'analisi delle minacce

PDE – Prodotto con elementi digitali

PSIRT – Team di risposta agli incidenti di sicurezza del prodotto

RBAC – Controllo degli accessi basato sui ruoli

SBOM – Distinta base del software

SDLC – Ciclo di vita dello sviluppo sicuro

SIEM – Gestione delle informazioni e degli eventi di sicurezza

PMI – Piccole e medie imprese

SNMP – Protocollo semplice di gestione della rete

SPDX – Scambio di dati sui pacchetti di sistema

SQL – Linguaggio di interrogazione strutturato

SSL – Secure Sockets Layer

STRIDE – Spoofing, Manomissione, Ripudio, Divulgazione di informazioni, Denial of Service, Elevazione dei privilegi

TLS – Sicurezza del livello di trasporto

UPnP – Universal Plug and Play

VPN – Rete privata virtuale

XSS – Cross-site Scripting

Introduzione

Il Cyber Resilience Act (CRA) dell'Unione europea, Regolamento (UE) 2024/2847, istituisce un quadro normativo completo volto a garantire che i prodotti con elementi digitali (PDE) siano sicuri durante l'intero ciclo di vita, dalla progettazione fino al termine della vita utile. Per **aiutare le piccole e medie imprese (PMI) a valutare e migliorare il proprio stato di conformità al CRA**, il presente documento fornisce un quadro metodologico per l'autovalutazione della conformità. Esso fa parte del materiale fornito dal **progetto SECURE**[1] , volto a sostenere le PMI nell'attuazione del CRA.

Il quadro approfondisce in modo estremamente dettagliato **cinque criteri chiave**: (1) Conformità ai requisiti essenziali di cibersicurezza, (2) Certificazione dei prodotti con elementi digitali, (3) Classificazione dei prodotti in Classe I o Classe II e azioni corrispondenti, (4) Completezza della documentazione tecnica e (5) Procedure generali di valutazione della conformità.

Ogni sezione è arricchita da indicazioni approfondite, esempi pratici, casi di studio, liste di controllo, riferimenti a modelli, strumenti e standard, garantendo che le PMI possano orientarsi efficacemente tra gli obblighi del CRA con strategie su misura, in linea con i propri vincoli di budget.

Le indicazioni riportate hanno esclusivamente **carattere orientativo,** benché basate su approcci e best practice riconosciuti. I riferimenti a strumenti e quadri metodologici esistenti sono forniti esclusivamente a titolo illustrativo.

La presente linea guida sarà aggiornata in funzione dell'evoluzione del quadro normativo del CRA.

[1] Il progetto "Rafforzamento della resilienza informatica delle PMI dell'UE" (SECURE) offre sostegno finanziario e orientamento alle PMI per conformarsi al CRA.

Quadro metodologico per la valutazione della conformità al CRA

1. Conformità ai requisiti essenziali di cibersicurezza

La **conformità ai requisiti essenziali di cibersicurezza** costituisce il pilastro dell'adeguamento al CRA, garantendo che i prodotti con elementi digitali soddisfino rigorosi standard di cibersicurezza per poter essere immessi sul mercato dell'UE. L'Allegato I del CRA specifica 13 **requisiti di cibersicurezza dei prodotti** e 8 **requisiti di gestione delle vulnerabilità**, per un totale di **21 requisiti essenziali**. Questa sezione fornisce una metodologia esaustiva che consente alle PMI di valutare la conformità, raccogliere le evidenze, identificare le lacune e sviluppare piani di correzione. Include spiegazioni dettagliate, strumenti pratici, casi di studio, modelli e indicazioni passo dopo passo per garantire una valutazione e una conformità approfondite.

1.1. Requisiti di cibersicurezza dei prodotti

I requisiti di cibersicurezza dei prodotti impongono che i prodotti siano progettati e sviluppati ponendo la sicurezza come principio fondamentale ("sicuri fin dalla progettazione e per impostazione predefinita"). Tali requisiti garantiscono che i prodotti siano privi di vulnerabilità sfruttabili note, dispongano di configurazioni predefinite sicure, supportino aggiornamenti di sicurezza tempestivi e proteggano la riservatezza, l'integrità e la disponibilità dei dati. Di seguito è riportata un'analisi completa dei requisiti[2] , con indicazioni dettagliate, esempi, strumenti e metodologie.

1.1.1. Assenza di vulnerabilità sfruttabili note

I fabbricanti devono garantire che i prodotti siano privi di vulnerabilità sfruttabili note al momento dell'immissione sul mercato, il che richiede rigorosi test pre-rilascio, tra cui scansioni delle vulnerabilità, test di penetrazione e revisioni del codice. Le PMI, spesso con risorse limitate, possono avvalersi di strumenti di test e scansione della sicurezza convenienti (ad esempio, uno scanner dinamico per applicazioni web, uno scanner di vulnerabilità di rete, uno strumento di test statico della sicurezza delle applicazioni e uno scanner di immagini dei container) per identificare i problemi.

[2] Alcuni requisiti dell'Allegato I del CRA, parzialmente in sovrapposizione, sono stati raggruppati nella presente linea guida, dando luogo a un elenco di otto ambiti operativi.

Ad esempio, un fabbricante di serrature intelligenti dovrebbe verificare la presenza di vulnerabilità Bluetooth, quali protocolli di accoppiamento deboli o attacchi di replay, e documentare le misure correttive in un registro di gestione delle vulnerabilità. I test dovrebbero allinearsi a standard quali **OWASP Top 10** o **CWE/SANS Top 25** per coprire le vulnerabilità più comuni.

Linee guida dettagliate:

- **Scansione delle vulnerabilità**: utilizzare OpenVAS o Nessus per individuare i CVE, programmando scansioni bisettimanali durante la fase di sviluppo. Le PMI possono accedere a livelli gratuiti di strumenti come Trivy per le applicazioni basate su container.
- **Test di penetrazione**: eseguire test manuali o automatizzati utilizzando strumenti come Metasploit oppure avvalersi di fornitori terzi per valutazioni trimestrali. Concentrarsi su aree ad alto rischio come l'autenticazione o le interfacce di rete.
- **Revisioni del codice**: utilizzare SonarQube per individuare vulnerabilità a livello di codice, quali SQL injection o cross-site scripting (XSS). Implementare revisioni tra pari per i componenti critici.
- **Documentazione**: tenere un registro di gestione delle vulnerabilità con colonne dedicate all'ID CVE, al punteggio CVSS, al componente interessato, all'azione correttiva e allo stato. Utilizzare strumenti come Jira o Trello per il monitoraggio.
- **Piano di correzione**: per le vulnerabilità senza patch, stabilire le priorità in base ai punteggi CVSS (ad es. >7,0 come critico) e fissare tempistiche di correzione (ad es. 30 giorni per i problemi critici).

Caso studio: Una PMI che sviluppa un termostato intelligente esegue una scansione delle vulnerabilità utilizzando Nessus, identificando un protocollo di crittografia debole (TLS 1.1). La PMI esegue l'aggiornamento a TLS 1.3, testa la correzione con OWASP ZAP e documenta il processo in un registro, includendo i punteggi CVSS e i rapporti di test. L'autovalutazione conferma che non permangono vulnerabilità note, come rilevato da un rapporto di test di penetrazione fornito da un fornitore terzo.

Tabella1 : Modello di registro di gestione delle vulnerabilità

ID CVE	Punteggio CVSS	Componente	Descrizione	Azione correttiva	Stato	Data di risoluzione

CVE-2025-1234	8.5	TLS 1.1	Crittografia debole	Aggiornamento a TLS 1.3	Risolto	15/06/2025

1.1.2. Configurazioni predefinite sicure

I prodotti devono essere forniti con impostazioni predefinite rafforzate per ridurre al minimo i rischi, ad esempio disabilitando i servizi non necessari, utilizzando password complesse e chiudendo le porte aperte. Le PMI dovrebbero allinearsi alla norma **ETSI EN 303 645**, che fornisce linee guida specifiche per l'IoT, o **ai benchmark CIS** per tecnologie specifiche (ad esempio, Linux, Docker). Ad esempio, una telecamera per la casa intelligente dovrebbe disabilitare l'accesso remoto per impostazione predefinita, richiedere password univoche e chiudere le porte inutilizzate come Telnet.

Linee guida dettagliate:

- **Revisione della configurazione**: sviluppare una checklist basata sulla norma ETSI EN 303 645, verificando impostazioni quali la disattivazione delle modalità di debug, l'assenza di credenziali predefinite e la chiusura delle porte. Utilizzare strumenti che effettuino controlli di rafforzamento della sicurezza del sistema.
- **Scansione delle porte**: utilizzare **Nmap** per identificare le porte e i servizi aperti, assicurandosi che siano attivi solo quelli necessari. Ad esempio, disabilitare l'FTP se non richiesto.
- **Politiche relative alle password**: implementare password predefinite complesse o obbligare gli utilizzatori a impostarle durante la configurazione. Utilizzare strumenti di verifica della complessità delle password.
- **Documentazione**: includere le impostazioni di configurazione nella documentazione tecnica, facendo riferimento a standard quali i CIS Benchmarks. Documentare eventuali deviazioni e le relative giustificazioni.
- **Linee guida per gli utilizzatori**: fornire istruzioni di configurazione nei manuali d'uso, spiegando come mantenere configurazioni sicure (ad esempio, disabilitando il Wi-Fi per gli ospiti).

Funded by the European Union

Caso studio: una PMI fabbricante di router Wi-Fi garantisce che le impostazioni predefinite disabilitino UPnP e Telnet, utilizzando Nmap per verificare le porte chiuse. La checklist di autovalutazione conferma la conformità alla norma ETSI EN 303 645, clausola 5.1, corredata da un rapporto di configurazione e dalle istruzioni del manuale d'uso.

Tabella 2 : Modello di lista di controllo per la configurazione

Impostazione	Requisito	Stato	Prova	Note
UPnP	Disabilitato	Conforme	Rapporto di scansione Nmap	Verificato 10/06/2025

1.1.3. Aggiornamenti di sicurezza tempestivi

I prodotti devono supportare gli aggiornamenti di sicurezza automatici con opzioni di disattivazione da parte dell'utilizzatore. Le PMI possono utilizzare meccanismi di aggiornamento **over-the-air (OTA)** tramite piattaforme come **Mender.io, AWS IoT Device Management** o **Balena**. Gli aggiornamenti devono essere firmati e verificati utilizzando strumenti come **OpenSSL** per impedire manomissioni. Ad esempio, un fabbricante di dispositivi indossabili dovrebbe garantire che gli aggiornamenti del firmware risolvano le vulnerabilità entro 30 giorni dalla loro scoperta, con chiare notifiche agli utilizzatori.

Linee guida dettagliate:

- **Infrastruttura di aggiornamento**: configurare un server di aggiornamento OTA o utilizzare soluzioni basate sul cloud. Assicurarsi che gli aggiornamenti siano firmati con RSA-2048 o ECDSA.
- **Test degli aggiornamenti**: verificare che gli aggiornamenti vengano installati senza compromettere la funzionalità, utilizzando ambienti di test come **Docker**. Eseguire test di regressione per garantire la compatibilità.
- **Notifica agli utilizzatori**: utilizzare e-mail, notifiche in-app o indicatori LED per informare gli utilizzatori degli aggiornamenti. Fornire istruzioni per la disattivazione nei manuali d'uso.

- **Documentazione**: includere nella documentazione tecnica la frequenza degli aggiornamenti, i meccanismi di firma e le procedure di notifica agli utilizzatori. Registrare la cronologia degli aggiornamenti con timestamp e i CVE risolti.
- **Metriche di conformità**: monitorare i tempi di distribuzione degli aggiornamenti (ad es. <30 giorni per le patch critiche) e i tassi di adozione da parte degli utilizzatori.

Caso studio: una PMI fabbricante di altoparlanti intelligenti utilizza Mender.io per distribuire aggiornamenti del firmware firmati, risolvendo un CVE entro 25 giorni. L'autovalutazione documenta il processo OTA, la notifica agli utilizzatori tramite e-mail e i risultati dei test di regressione, garantendo la conformità ai requisiti CRA.

Tabella 3 : Modello di registro degli aggiornamenti

ID aggiornamento	CVE risolto	Data di rilascio	Tempo di implementazione	Notifica agli utilizzatori	Stato
V2.1.3	CVE 2025-5678	1 luglio 2025	25 giorni	E-mail inviata il 30/06/2025	Implementato

1.1.4. Protezione contro gli accessi non autorizzati

Meccanismi di autenticazione avanzati, come **l'autenticazione a più fattori (MFA)**, **OAuth 2.0** o **OpenID Connect**, sono essenziali per impedire accessi non autorizzati. Le PMI possono utilizzare **i JSON Web Token (JWT)** per la sicurezza delle API e **il controllo degli accessi basato sui ruoli (RBAC)** per limitare le autorizzazioni. Strumenti come **Burp Suite** o **Postman** possono simulare attacchi per testare i controlli di accesso. Ad esempio, un dispositivo IoT connesso al cloud dovrebbe richiedere l'autenticazione a più fattori (MFA) per gli account utente e utilizzare i JWT per gli endpoint delle API.

Linee guida dettagliate:

- **Implementare l'autenticazione**: utilizzare librerie MFA come **Auth0** o **Okta** per gli account utente. Implementare i JWT per le API, seguendo lo standard RFC 7519.

- **Testare i controlli di accesso**: eseguire test di penetrazione con Burp Suite per simulare attacchi di forza bruta o di dirottamento della sessione. Utilizzare strumenti come **Wireshark** per monitorare il traffico di rete.
- **Documentare le policy**: includere le policy di autenticazione e controllo degli accessi nella documentazione tecnica, specificando i protocolli (ad es. OAuth 2.0) e le configurazioni RBAC.
- **Monitorare gli accessi**: abilitare la registrazione dei tentativi di accesso utilizzando **Syslog** o **ELK Stack**, con avvisi in caso di attività sospette (ad es. accessi falliti ripetuti).
- **Audit periodici**: pianificare audit trimestrali dei controlli di accesso, utilizzando strumenti come **HashiCorp Vault** per la gestione delle credenziali.

Caso studio: una PMI che sviluppa un campanello intelligente implementa l'autenticazione a più fattori (MFA) utilizzando Auth0 e la testa con Burp Suite, individuando e risolvendo una vulnerabilità nella gestione delle sessioni. L'autovalutazione include le policy di autenticazione, i rapporti di test e le configurazioni dei log.

Tabella 4 : Modello di politica di controllo degli accessi

Componente	Autenticazione	Controllo degli accessi	Metodo di verifica	Prove	Stato
Accesso utilizzatore	MFA (Auth0)	RBAC (Amministratore/Utilizzatore)	Burp Suite	Rapporto di test 20/06/2025	Conforme

1.1.5. Riservatezza, integrità e disponibilità dei dati

La crittografia è fondamentale per la protezione dei dati. Le PMI dovrebbero implementare **AES-256** per i dati a riposo e **TLS 1.3** per i dati in transito, in linea con **lo standard NIST SP 800-52**. La convalida degli input dovrebbe impedire attacchi di tipo "injection", utilizzando librerie come **OWASP ESAPI**. Ad esempio, un dispositivo di monitoraggio sanitario deve crittografare i dati dei pazienti per conformarsi al GDPR e al CRA, garantendo riservatezza e integrità.

Linee guida dettagliate:

- **Selezionare gli standard di crittografia**: utilizzare AES-256 per l'archiviazione e TLS 1.3 per la comunicazione. Implementare la gestione delle chiavi con **AWS KMS** o **HashiCorp Vault**.
- **Testare la crittografia**: eseguire test di penetrazione con Metasploit per verificare la protezione dei dati. Utilizzare strumenti come **SSL Labs** per valutare le configurazioni TLS.
- **Convalida degli input**: implementare la convalida degli input utilizzando ESAPI o librerie simili per prevenire attacchi di tipo SQL injection o XSS.
- **Documentare la crittografia**: includere i protocolli di crittografia, le politiche di gestione delle chiavi e i risultati dei test nella documentazione tecnica.
- **Monitorare la disponibilità**: utilizzare strumenti di monitoraggio come **Nagios** per garantire il tempo di attività del sistema e la resilienza contro gli attacchi DDoS.

Caso studio: una PMI fabbricante di dispositivi medici crittografa i dati dei pazienti con AES-256 e TLS 1.3, esegue test con Metasploit e documenta la conformità nella documentazione tecnica. La convalida degli input impedisce attacchi di tipo SQL injection, come verificato dalle scansioni OWASP ZAP.

Tabella 5 : Modello di conformità alla crittografia

Tipo di dati	Crittografia	Gestione delle chiavi	Metodo di prova	Prove	Stato
Dati dei pazienti	AES-256	AWS KMS	Metasploit	Rapporto di prova 25/06/2025	Conforme

1.1.6. Riduzione al minimo dei dati e della superficie di attacco

I prodotti dovrebbero raccogliere solo i dati necessari e ridurre al minimo le interfacce aperte. Le PMI possono utilizzare **Nmap** per eseguire la scansione delle porte aperte e **OWASP Dependency-Check** per identificare le dipendenze inutilizzate. Una **valutazione d'impatto sulla protezione dei dati (DPIA)**, in linea con il GDPR, dovrebbe giustificare la raccolta dei dati. Ad esempio, un fitness tracker dovrebbe limitare i dati alla frequenza cardiaca e ai passi, disabilitando i servizi Bluetooth inutilizzati.

Linee guida dettagliate:

- **Mappare i flussi di dati**: condurre una DPIA per documentare la raccolta, il trattamento e l'archiviazione dei dati. Utilizzare strumenti come **OneTrust** per l'automazione della DPIA.
- **Ridurre al minimo le interfacce**: utilizzare Nmap per identificare e chiudere porte o API non necessarie. Disattivare i protocolli inutilizzati come SNMP o FTP.
- **Rimuovere le dipendenze**: utilizzare Dependency-Check per identificare e rimuovere le librerie inutilizzate.
- **Documentazione della riduzione**: includere i risultati della DPIA e le configurazioni delle interfacce nella documentazione tecnica.
- **Revisioni periodiche**: pianificare aggiornamenti trimestrali della DPIA per riflettere le modifiche apportate al prodotto.

Caso studio: una PMI fabbricante di fitness tracker effettua una DPIA, limita la raccolta dei dati alle metriche essenziali e disabilita i servizi Bluetooth inutilizzati. Le scansioni con Nmap confermano una superficie di attacco minima, documentata nell'autovalutazione.

Tabella 6 : Modello di sintesi della DPIA

Tipo di dati	Finalità	Necessità	Misure di minimizzazione	Prove	Stato
Frequenza cardiaca	Monitoraggio dello stato di salute	Essenziale	Tracciamento della posizione disabilitato	Rapporto DPIA 30/06/2025	Conforme

1.1.7. Mitigazione degli incidenti e registrazione

I prodotti devono includere meccanismi per limitare i danni derivanti da incidenti, quali la limitazione della frequenza o il rilevamento delle intrusioni, e consentire una registrazione sicura. Le PMI possono utilizzare strumenti per la registrazione, garantendo un'archiviazione a prova di manomissione. Ad esempio, un router di rete dovrebbe registrare i tentativi di accesso non autorizzati e implementare la limitazione della frequenza per prevenire attacchi di forza bruta.

Linee guida dettagliate:

- **Implementare la mitigazione**: utilizzare la limitazione della velocità (ad es. tramite **NGINX**) e sistemi di rilevamento delle intrusioni come Snort.
- **Abilitare la registrazione**: configurare Syslog o ELK Stack per una registrazione sicura e crittografata. Impostare criteri di conservazione (ad es. 6 mesi).
- **Verifica delle misure di mitigazione**: simulare attacchi con strumenti come **hping3** per verificare l'efficacia della limitazione della velocità e dell'IDS.
- **Documentare i log**: includere i formati dei log, le politiche di conservazione e i risultati dei test nella documentazione tecnica.
- **Esaminare i log**: pianificare revisioni mensili dei log per identificare anomalie, utilizzando strumenti come **Splunk** per l'analisi.

Caso studio: un'azienda di medie dimensioni specializzata in router implementa la limitazione della velocità con NGINX e registra i tentativi di accesso con ELK Stack. I test di penetrazione con hping3 confermano l'efficacia delle misure di mitigazione, documentate nell'autovalutazione.

Tabella 7 : Modello di configurazione dei log

Tipo di evento	Formato del log	Archiviazione	Conservazione	Metodo di prova	Prove	Stato
Tentativi di accesso	Syslog	Crittografato	6 mesi	hping3	Rapporto di test 01/07/2025	Conforme

1.1.8. Cancellazione dei dati dell'utilizzatore

I prodotti devono consentire agli utilizzatori di rimuovere in modo sicuro e permanente i propri dati e le proprie impostazioni. A seconda della natura del prodotto e del supporto di memorizzazione, possono essere utilizzate tecniche quali la sovrascrittura sicura, la cancellazione crittografica o il ripristino protetto delle impostazioni di fabbrica. Ad esempio, un altoparlante intelligente dovrebbe offrire una **funzione di ripristino delle impostazioni di fabbrica** che renda irrecuperabili i dati dell'utilizzatore. Le PMI dovrebbero verificare l'efficacia della procedura mediante prove tecniche adeguate.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Linee guida dettagliate:

- **Implementazione della cancellazione**: fornire un'opzione di ripristino delle impostazioni di fabbrica sicura, utilizzando, ove appropriato, meccanismi di cancellazione crittografica (ad es. OpenSSL s_random) o strumenti di cancellazione sicura adeguati al supporto interessato.
- **Verifica della cancellazione**: utilizzare strumenti forensi per verificare che i dati siano irrecuperabili.
- **Documentare la procedura**: includere le istruzioni di cancellazione e i risultati dei test nella documentazione tecnica.
- **Linee guida per gli utilizzatori**: fornire istruzioni chiare nei manuali d'uso, con assistenza online per la risoluzione dei problemi.
- **Test periodici**: programmare test annuali per garantire che i meccanismi di cancellazione rimangano efficaci.

Caso studio: una PMI fabbricante di altoparlanti intelligenti implementa un ripristino delle impostazioni di fabbrica con cancellazione crittografica, testato con Autopsy. L'autovalutazione include le istruzioni del manuale d'uso e i rapporti di prova.

Tabella 8 : Modello di verifica della cancellazione dei dati

Componente	Metodo di cancellazione	Strumento di test	Prove	Stato
Dati utilizzatore	Cancellazione crittografica	Autopsy	Rapporto di prova 05/07/2025	Conforme

1.2. Requisiti per la gestione delle vulnerabilità

Gli 8 requisiti per la gestione delle vulnerabilità garantiscono una gestione continua della sicurezza dopo il rilascio, richiedendo processi per l'identificazione, la correzione e la divulgazione delle vulnerabilità. Di seguito è riportata un'analisi dettagliata dei requisiti[3] .

1.2.1. Distinta base del software (SBOM)

I fabbricanti devono mantenere una SBOM leggibile meccanicamente in formati comunemente utilizzati quali **CycloneDX** o **SPDX**. Strumenti come **Snyk**, **Dependabot** o **Trivy** possono automatizzare la generazione della SBOM. Ad esempio, un'azienda specializzata in applicazioni web utilizza Dependabot per monitorare le dipendenze e generare una SBOM, garantendo la trasparenza dei componenti di terze parti.

Linee guida dettagliate:

- **Generare la SBOM**: utilizzare Snyk o Trivy per creare un SBOM, includendo i numeri di versione e le licenze.
- **Aggiornare la SBOM**: pianificare aggiornamenti mensili per includere nuovi componenti o patch.
- **Verifica dei componenti**: verificare la presenza di vulnerabilità utilizzando l'NVD del NIST o il database di Snyk.
- **Documentare la SBOM**: includere la SBOM nella documentazione tecnica, con un registro delle modifiche per gli aggiornamenti.
- **Integrazione con CI/CD**: utilizzare strumenti come **GitHub Actions** per automatizzare la generazione della SBOM nelle pipeline di sviluppo.

Caso studio: una PMI che offre servizi cloud genera una SBOM con CycloneDX, individuando una libreria vulnerabile (Log4j). La PMI applica la patch alla libreria, aggiorna la SBOM e documenta il processo nell'autovalutazione.

[3] Per evitare sovrapposizioni, alcuni degli otto requisiti di gestione delle vulnerabilità dell'Allegato I sono stati raggruppati nella presente linea guida in sei ambiti operativi.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Tabella 9 : Modello di riepilogo SBOM

Componente	Versione	Licenza	Vulnerabilità	Azione	Stato
Log4j	2.16.0	Apache 2.0	CVE-2021-44228	Corretto alla versione 2.17.1	Risolto

1.2.2. Risoluzione tempestiva delle vulnerabilità

Le vulnerabilità devono essere risolte senza indebiti ritardi, dando priorità ai problemi critici in base **ai punteggi CVSS**. Le PMI dovrebbero rilasciare le patch entro 30 giorni per le vulnerabilità critiche ed entro 60 giorni per le altre. Ad esempio, una PMI fabbricante di telecamere intelligenti corregge una vulnerabilità CVE entro 25 giorni, informando gli utilizzatori tramite e-mail.

Linee guida dettagliate:

- **Monitoraggio delle vulnerabilità**: utilizzare Snyk, l'NVD del NIST o **VulnDB** per tenere traccia dei CVE.
- **Stabilire le priorità delle patch**: utilizzare i punteggi CVSS per stabilire le priorità (ad esempio, >7,0 come critico, 4,0-6,9 come medio).
- **Testare le patch**: eseguire test di regressione in un ambiente sandbox per garantire la stabilità.
- **Notifica agli utilizzatori**: utilizzare e-mail, notifiche in-app o avvisi sul sito web per informare gli utilizzatori.
- **Documentare le misure correttive**: includere le tempistiche delle patch, i risultati dei test e le notifiche agli utilizzatori nella documentazione tecnica.

Caso studio: una PMI fabbricante di serrature intelligenti individua una vulnerabilità CVE critica (CVSS 8,8) e rilascia una patch entro 20 giorni, documentando il processo e la notifica agli utilizzatori nell'autovalutazione.

Tabella 10 : Modello di registro di risoluzione delle vulnerabilità

ID CVE	Punteggio CVSS	Componente	Data della patch	Metodo di notifica	Stato
CVE-2025-5678	8.8	Firmware	01/07/2025	E-mail	Risolto

1.2.3. Test di sicurezza regolari

Sono necessari test periodici, inclusi test di penetrazione, scansioni delle vulnerabilità e revisioni del codice. Le PMI possono utilizzare **OpenVAS**, **Nessus** o fornitori di terze parti per audit convenienti, programmando scansioni trimestrali e test di penetrazione annuali.

Linee guida dettagliate:

- **Pianificazione dei test**: pianificare scansioni delle vulnerabilità trimestrali e test di penetrazione annuali, in conformità con **l'Allegato A.12.6.1 della norma ISO 27001**.
- **Utilizzo degli strumenti**: impiegare OpenVAS per le scansioni, Burp Suite per le applicazioni web o Metasploit per i test di penetrazione.
- **Documentare i risultati**: includere nella documentazione tecnica i rapporti di test, i risultati e i piani di correzione.
- **Gestire le criticità rilevate**: dare priorità ai problemi in base alla gravità e stabilire tempistiche di risoluzione.
- **Automatizzare i test**: integrare strumenti come **Snyk** nelle pipeline CI/CD per eseguire scansioni continue.

Caso studio: una PMI fabbricante di dispositivi per la casa intelligente effettua scansioni trimestrali con OpenVAS e un test di penetrazione annuale con un fornitore terzo, documentando i risultati e i piani di correzione nell'autovalutazione.

Tabella 11 : Modello di programma per i test di sicurezza

Tipo di test	Frequenza	Strumento	Ultima esecuzione	Risultati	Stato della correzione

Scansione delle vulnerabilità	Trimestrale	OpenVAS	30/06/2025	2 CVE	Risolti

1.2.4. Trasparenza nella divulgazione delle vulnerabilità

I fabbricanti dovrebbero rendere pubbliche, dopo la disponibilità di un aggiornamento o di una misura correttiva, informazioni sulle vulnerabilità corrette che consentano agli utilizzatori di comprendere la natura della vulnerabilità, i prodotti interessati e le misure da adottare. Le PMI dovrebbero pubblicare avvisi di sicurezza sul proprio sito web specificando la gravità, l'impatto, le versioni interessate, le misure di mitigazione/soluzioni alternative e le tempistiche, in linea con gli standard riconosciuti di divulgazione delle vulnerabilità e le best practice (ad esempio, ISO/IEC 29147 e ISO/IEC 30111, le linee guida CVD dell'ENISA, le linee guida di coordinamento multipartitico di FIRST o una politica interna equivalente e coerente con tali riferimenti).

Linee guida dettagliate:

- **Creare un modello di divulgazione**: sviluppare un formato standard per gli avvisi, che includa l'ID CVE, il punteggio CVSS, l'impatto e i dettagli della patch.
- **Pubblicare gli avvisi**: pubblicarli sul sito web aziendale, sul blog o sul portale dedicato alla sicurezza.
- **Notificare gli utilizzatori**: utilizzare e-mail, notifiche in-app o social media per informare gli utilizzatori.
- **Documentare le divulgazioni**: includere un link o il percorso DMS all'archivio pubblico delle notifiche di sicurezza, il registro interno delle modifiche al testo della notifica e la prova delle notifiche agli utilizzatori (elenchi, timestamp e canali).
- **Coinvolgere** i coordinatori: ove opportuno, condividere gli avvisi con i CSIRT/PSIRT nazionali competenti o con le comunità e gli archivi di coordinamento delle vulnerabilità per favorire un'ampia sensibilizzazione (utilizzare canali neutri; non è richiesto alcun marchio specifico).
- **Indicare la base** di riferimento**:** nella politica pubblica, specificare la linea guida a cui ci si allinea (ad es. ISO/IEC 29147 e ISO/IEC 30111 o le best practice CVD dell'ENISA) e precisare che sono accettati processi funzionalmente equivalenti. Indicare la versione e la data della politica e rivederla annualmente.

Funded by the European Union

Caso studio: una PMI fabbricante di smart TV pubblica un avviso di sicurezza relativo a un CVE, descrivendo in dettaglio la patch e l'impatto. L'autovalutazione include l'avviso e i registri delle notifiche agli utilizzatori.

Tabella 12 : Modello di avviso di sicurezza

ID CVE	Punteggio CVSS	Impatto	Dettagli della patch	Data di pubblicazione	Metodo di notifica
CVE-2025-1234	7,5	Violazione dei dati	Firmware v2.1.3	01/07/2025	Sito web, e-mail

È possibile aggiungere altre colonne, quali: Versioni/Build interessate; Misure di mitigazione/Soluzioni alternative (se la patch non è ancora disponibile); Cronologia della divulgazione (segnalazione ricevuta - presa in carico - corretta - pubblicata); Ringraziamenti (ricercatore/CSIRT, se applicabile).

1.2.5. Politica di divulgazione coordinata delle vulnerabilità (CVD)

Le PMI devono fornire un canale chiaro per la segnalazione delle vulnerabilità, come un indirizzo e-mail dedicato o un portale web. Piattaforme come HackerOne o Bugcrowd possono facilitare la CVD attraverso programmi di bug bounty, incoraggiando gli hacker etici a segnalare i problemi.

Linee guida dettagliate:

- **Definire la politica CVD**: creare una policy con un indirizzo e-mail dedicato (ad es. security@company.com) o un portale, seguendo le linee guida **ISO 29147**.
- **Promuovere la segnalazione**: pubblicizzare la policy sul sito web aziendale e sui forum degli sviluppatori.
- **Rispondere tempestivamente**: confermare la ricezione delle segnalazioni entro 7 giorni e fornire aggiornamenti entro 30 giorni.
- **Documentare la policy**: includere la politica CVD, i parametri di risposta e le vulnerabilità segnalate nella documentazione tecnica.

- **Premiare chi segnala**: valutare l'introduzione di programmi di bug bounty per incentivare le segnalazioni, utilizzando piattaforme come HackerOne.

Caso studio: una PMI crea un portale CVD su HackerOne, ricevendo e risolvendo una vulnerabilità segnalata entro 25 giorni. L'autovalutazione documenta la politica e gli indicatori di risposta.

Tabella 13 : Modello di politica CVD

Canale	Tempo di risposta	Vulnerabilità segnalate	Prove	Stato
security@company.com	7 giorni	3 CVE	Segnalazione su HackerOne	Risolto

1.2.6. Aggiornamenti di sicurezza gratuiti

Gli aggiornamenti devono essere forniti gratuitamente per un periodo di assistenza definito (ad esempio, almeno 5 anni per i dispositivi IoT o per tutta la durata di vita del prodotto). Le PMI dovrebbero garantire che gli aggiornamenti siano facili da installare, preferibilmente in modo automatico, utilizzando meccanismi OTA.

Linee guida dettagliate:

- **Definire il periodo di assistenza (CRA art. 13(8)):** stabilire un periodo di assistenza che rifletta la durata prevista di utilizzo del prodotto; tale periodo non può essere inferiore a 5 anni, a meno che non si preveda ragionevolmente che il prodotto venga utilizzato per meno di 5 anni, nel qual caso il periodo di assistenza corrisponde a tale durata inferiore. Se si prevede che il prodotto venga utilizzato per più di 5 anni, stabilire un periodo di assistenza più lungo**.**
- **Automatizzare gli aggiornamenti**: utilizzare piattaforme OTA come Mender.io o Balena per aggiornamenti senza interruzioni.
- **Testare gli aggiornamenti**: verificare l'installazione e la funzionalità degli aggiornamenti in un ambiente di test.

- **Documentare l'assistenza**: includere le policy sull'assistenza, i registri degli aggiornamenti e le istruzioni per l'utilizzatore nella documentazione tecnica.
- **Monitorare la conformità**: tenere traccia della distribuzione degli aggiornamenti e dei tassi di adozione da parte degli utilizzatori, assicurandosi che non vengano imposti costi.

In base ai requisiti del CRA, il fabbricante deve garantire che ogni aggiornamento di sicurezza rimanga a disposizione degli utilizzatori per un periodo di almeno 10 anni dalla sua emissione o per la durata residua del periodo di assistenza, a seconda di quale dei due sia più lungo. In pratica, le PMI dovrebbero mantenere un archivio delle patch di sicurezza (ad esempio sul sito web o sul server di aggiornamento) accessibile ai clienti anche dopo la fine dell'assistenza ufficiale. Inoltre, se il prodotto subisce evoluzioni attraverso versioni software principali, il fabbricante deve offrire agli utilizzatori le nuove versioni gratuitamente e senza imporre costi aggiuntivi per hardware o software per poter beneficiare delle correzioni di sicurezza (ai sensi dell'art. 13, comma 10, del CRA). Tutti questi aspetti saranno documentati nella documentazione tecnica, compresa la motivazione del periodo di assistenza (minimo 5 anni) e le modalità con cui gli utilizzatori vengono informati della fine del periodo di assistenza o della disponibilità di aggiornamenti di sicurezza a lungo termine.

Caso studio: una PMI fabbricante di termostati intelligenti si impegna a fornire 5 anni di aggiornamenti gratuiti tramite Mender.io, documentando la politica e il meccanismo OTA nell'autovalutazione.

Tabella 14 : Modello di politica di assistenza

Prodotto	Periodo di assistenza	Meccanismo di aggiornamento	Ultimo aggiornamento	Prove	Stato
Termostato	5 anni	OTA (Mender.io)	01/07/2025	Registro degli aggiornamenti	Conforme

1.3. Checklist raccomandata per l'autovalutazione

Per adempiere agli obblighi previsti dal CRA in materia di documentazione tecnica e valutazione della conformità, la gestione di una checklist strutturata per l'autovalutazione può fornire un valido supporto. Si raccomanda l'utilizzo di un'unica checklist che copra tutti i 21 requisiti dell'Allegato I per

monitorare lo stato, le prove e l'approvazione durante l'intero ciclo di vita del prodotto. Le colonne di tale checklist di autovalutazione possono essere:

- **Riferimento all'Allegato I / ID del requisito (ad es. 1.1.9 Avvio sicuro)**
- **Prodotto / Versione (inclusa la build del firmware/software)**
- **Dichiarazione di conformità UE (Sì / Parziale / No)**
- **Prove oggettive (link/percorso) (rapporto di prova, politica, configurazione, SBOM, avviso)**
- **Data del test/della revisione**
- **Ruolo responsabile / Titolare**
- **Scostamenti e controlli compensativi (se presenti)**
- **Rischio residuo e motivazione**
- **Azione successiva / Data di scadenza**
- **Approvazione / Firma (nome, data)**
- **Riferimento alla documentazione tecnica (dove si trova nell'indice della documentazione tecnica)**

Le PMI possono utilizzare una dashboard di conformità in strumenti come **Confluence**, **Notion** o **Excel** per visualizzare i progressi, collegarsi alla documentazione di supporto e monitorare le azioni correttive.

Questa checklist è uno strumento di controllo interno destinato a supportare la conformità alle norme CRA (documentazione tecnica, valutazione della conformità e monitoraggio post-commercializzazione). Di per sé, non sostituisce alcun obbligo previsto dalle norme CRA, ma organizza piuttosto la documentazione che è necessario produrre e conservare.

1.4. Caso studio

Una PMI che sviluppa un campanello intelligente effettua un'autovalutazione:

- **Requisiti di prodotto**: utilizza OWASP ZAP per verificare l'assenza di vulnerabilità, implementa TLS 1.3 e disabilita le porte inutilizzate. I test di penetrazione confermano la conformità.

- **Gestione delle vulnerabilità**: genera una SBOM con CycloneDX, esegue scansioni trimestrali con OpenVAS e pubblica una politica CVD su HackerOne.
- **Risultato**: raggiunge la piena conformità a 18 requisiti, identifica lacune negli aggiornamenti automatici e pianifica le misure correttive entro 3 mesi, documentandole in una dashboard.

1.5. Strumenti e risorse

Gli esempi e le funzionalità elencati in questo documento sono indipendenti dallo strumento utilizzato. Descrivono ciò che uno strumento deve fare, non quale marchio utilizzare. I team possono utilizzare qualsiasi soluzione equivalente che assicuri le funzionalità indicate e produca la relativa documentazione di supporto.

- **Scansione delle vulnerabilità**: OpenVAS, Nessus, Trivy.
- **Test di penetrazione**: Metasploit, Burp Suite.
- **Analisi del codice**: SonarQube, OWASP Dependency-Check.
- **Registrazione dei log**: Syslog, ELK Stack, Graylog.
- **Generazione di SBOM**: Snyk, CycloneDX, SPDX.
- **Standard/Norma**: ETSI EN 303 645, NIST SP 800-53, ISO 27001.

Questa sezione fornisce alle PMI una metodologia solida e dettagliata per raggiungere e documentare la conformità a tutti i requisiti essenziali, corredata da strumenti pratici, modelli e casi studio.

2. Certificazione dei prodotti contenenti elementi digitali

Il criterio **relativo alla certificazione dei prodotti contenenti elementi digitali** si avvale dei sistemi di certificazione europei in materia di cibersicurezza per dimostrare la conformità al CRA, in linea con il **Regolamento sulla cibersicurezza (UE) 2019/881**. I sistemi di certificazione dell'UE in materia di cibersicurezza sono previsti dalla legge sulla cibersicurezza (ad esempio, l'EUCC per i prodotti ICT), ma il loro ruolo ai fini della presunzione di conformità al CRA sarà specificato dagli atti delegati della Commissione ai sensi dell'art. 27, paragrafo 9.

Presunzione di conformità (CRA, art. 27, paragrafi 8 e 9): laddove la Commissione specifichi gli schemi europei di certificazione in materia di cibersicurezza applicabili mediante atto delegato ai sensi del CRA, si presume che i prodotti in possesso di una Dichiarazione di conformità UE o di un

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

certificato rilasciato nell'ambito di tale schema siano conformi solo ai requisiti dell'allegato I coperti da tale certificato. La presente sezione fornisce una metodologia esaustiva che consente alle PMI di valutare l'applicabilità della certificazione, di mappare i requisiti del CRA alle norme e di integrare le certificazioni nell'autovalutazione, con orientamenti dettagliati, casi studio e modelli.

2.1. Schemi di certificazione e norme

Il CRA incoraggia certificazioni **quali i Criteri Comuni (ISO/IEC 15408)**, **EUCS (EU Cloud Security), ETSI EN 303 645** (per l'IoT) e **IEC 62443** (per i sistemi industriali). Le PMI dovrebbero valutare se la categoria del proprio prodotto sia coperta da uno schema di certificazione esistente, utilizzando risorse quali **gli elenchi dei candidati alla certificazione dell'ENISA.**

Standard chiave:

- **ETSI EN 303 645**: riguarda la sicurezza dell'IoT, comprese le configurazioni sicure, la protezione dei dati e la divulgazione delle vulnerabilità.
- **Criteri comuni**: fornisce livelli di garanzia (EAL1-EAL7) per i prodotti IT, adatti a sistemi critici come i firewall.
- **ISO 27001**: si concentra sui processi di sicurezza organizzativa, rilevanti per la gestione delle vulnerabilità.
- **IEC 62443**: riguarda l'IoT industriale, coprendo lo sviluppo e il funzionamento sicuri.
- **NIST SP 800-53**: fornisce controlli tecnici di sicurezza, in linea con i requisiti CRA.

2.2. Metodologia di autovalutazione

L'autovalutazione dovrebbe includere una checklist dettagliata:

1. **Certificazioni esistenti**: il prodotto è in possesso di una certificazione di cibersicurezza? Ad esempio, un dispositivo per la casa intelligente certificato secondo la norma ETSI EN 303 645 soddisfa molti requisiti CRA.
2. **Applicabilità**: il prodotto è idoneo a un sistema di certificazione europeo? Consultare gli elenchi dell'ENISA o gli organismi notificati.
3. **Allineamento alle norme**: mappare i requisiti del CRA rispetto alle norme e agli standard pertinenti, individuando le eventuali sovrapposizioni. Ad esempio, i controlli della ISO/IEC

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

27001 relativi alla gestione delle vulnerabilità tecniche possono contribuire a documentare i processi adottati dal fabbricante.

4. **Pianificazione della certificazione**: valutare la fattibilità del percorso di certificazione, tenendo conto dei costi, delle tempistiche e dei benefici.
5. **Conformità parziale**: documentare l'adesione agli standard, anche in assenza di una certificazione completa, per dimostrare la dovuta diligenza.

Tabella 15 : Esempio di mappatura

Requisito CRA	Standard	Clausola	Prova
Configurazioni predefinite sicure	ETSI EN 303 645	Clausola 5.1	Rapporto di configurazione
Divulgazione delle vulnerabilità	ISO 27001	A.12.6.1	Politica CVD

2.3. Misure pratiche per le PMI

1. **Identificare gli standard pertinenti**: utilizzare il sito web dell'ENISA o consultare gli organismi notificati per individuare gli standard applicabili. Ad esempio, una PMI che si occupa di contatori intelligenti dovrebbe prendere in esame la norma IEC 62443.
2. **Documentare la conformità**: conservare la documentazione relativa al rispetto delle norme, come i rapporti di audit ISO 27001 o i risultati dei test ETSI EN 303 645.
3. **Coinvolgere gli organismi di certificazione**: contattare gli organismi accreditati elencati dall'ENISA per le procedure di certificazione.
4. **Sfruttare la conformità parziale**: documentare la conformità parziale alle norme per ridurre l'ambito di valutazione del CRA.
5. **Sviluppare una tabella di marcia per la certificazione**: pianificare tempistiche, budget e risorse per la certificazione. Ad esempio, la certificazione Common Criteria può richiedere dai 6 ai 12 mesi e costare tra i 50.000 e i 100.000 euro.

2.4. Caso studio

Una PMI che sviluppa una piattaforma IoT basata sul cloud persegue la certificazione EUCS:

- **Valutazione**: mette in relazione i requisiti del CRA con quelli dell'EUCS, individuando le sovrapposizioni in materia di protezione dei dati, crittografia e gestione delle vulnerabilità.
- **Azione**: si avvale di un organismo notificato (NB), presenta i rapporti di prova (ad es. test di penetrazione, SBOM) e documenta la conformità alle clausole dell'EUCS.
- **Risultato**: ottiene la certificazione entro 9 mesi, semplificando la conformità al CRA e rafforzando la fiducia del mercato. L'autovalutazione include una tabella di mappatura e un rapporto di certificazione.

2.5. Modello di roadmap per la certificazione

Tabella 16 : Modello di roadmap di certificazione

Certificazione	Tempistica	Stima dei costi	Responsabile	Documentazione	Stato
EUCS	9 mesi (dal 01/03/2025 al 01/12/2025)	75.000 €	Team di sicurezza	Rapporti di prova	In corso

2.6. Strumenti e risorse

- **ENISA**: Elenchi dei candidati alla certificazione e repertori degli organismi notificati.
- **Standard/Norma**: ETSI EN 303 645, ISO 27001, IEC 62443, Common Criteria.
- **Strumenti**: Confluence per la documentazione, Snyk per la generazione di SBOM, OWASP ZAP per i test.

Questa sezione garantisce che le PMI possano avvalersi delle certificazioni per semplificare la conformità al CRA, grazie a linee guida dettagliate, modelli e casi studio.

3. Classificazione dei prodotti: percorsi di conformità

Il criterio **della classificazione dei prodotti** determina il percorso di conformità appropriato sulla base della classificazione dei prodotti effettuata dal CRA in funzione del rischio nelle categorie Predefinito, Importante — Classe I (Allegato III), Importante — Classe II (Allegato III) e Critico

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

(Allegato IV). Questa sezione fornisce una metodologia esaustiva che consente alle PMI di classificare i prodotti, comprendere gli obblighi di conformità e integrare la classificazione nell'autovalutazione, con linee guida dettagliate, metodologie di valutazione del rischio e casi studio.

3.1. Comprendere la classificazione dei prodotti

Il CRA classifica i prodotti in base al loro potenziale rischio per la cibersicurezza, come definito nell'Allegato III e nell'Allegato IV:

- **Predefinito — Non elencato nell'Allegato III/IV.**
- **Importante — Classe I (Allegato III) —** ad es., sistemi operativi, browser, VPN, SIEM, router/modem.
- **Importante — Classe II (Allegato III) —** ad es., hypervisor, runtime per container, firewall, IDS/IPS.
- **Critico (Allegato IV) —** ad esempio, dispositivi hardware con moduli di sicurezza, gateway per contatori intelligenti, smart card/elementi di sicurezza.

La classificazione si basa sul caso d'uso del prodotto, sulla sensibilità dei dati e sul potenziale impatto sulle infrastrutture critiche o sulla sicurezza degli utilizzatori.

3.2. Metodologia di autovalutazione

L'autovalutazione dovrebbe includere un albero decisionale dettagliato:

1. **Verifica degli allegati CRA**: consultare gli allegati III e IV per le categorie di prodotti. Ad esempio, le telecamere per la casa intelligente rientrano nella Classe I, mentre il software VPN nella Classe II.
2. **Valutare l'impatto del rischio**: condurre una valutazione del rischio utilizzando **la norma ISO 27005**, **lo standard NIST SP 800-30** o **OCTAVE Allegro** per valutare l'impatto di un attacco informatico.
3. **Classificazione della documentazione**: registrare la classificazione, i risultati della valutazione del rischio e la motivazione nella documentazione tecnica.
4. **Verificare il percorso di conformità**: assicurarsi che venga seguito il modulo di valutazione corretto (controllo interno, esame UE di tipo) in base alla classificazione.

Tabella 17 : Esempio di albero decisionale

Domanda	Risposta	Azione
Il prodotto è incluso nell'allegato III o IV?	Sì (Classe II)	Rivolgersi a un organismo notificato per l'esame UE del tipo
Il malfunzionamento potrebbe avere ripercussioni sulle infrastrutture critiche?	No	Classificare come predefinito o Classe I, utilizzare il controllo interno

3.3. Percorsi di conformità

- **Prodotti predefiniti** — Modulo A (Controllo interno della produzione). Il fabbricante valuta autonomamente la conformità a tutti i 21 requisiti dell'Allegato I e conserva la documentazione tecnica completa.
- **Importante — Classe I —** Modulo A solo se vengono applicate norme armonizzate/specifiche comuni o uno schema di certificazione UE in materia di cibersicurezza applicabile (garanzia ≥ «sostanziale»); in caso contrario, è richiesta una valutazione da parte di terzi (Moduli B + C o H) per i requisiti non coperti.
- **Importante — Classe II** — È obbligatoria la valutazione da parte di terzi (Moduli B + C o H) o uno schema di certificazione UE in materia di cibersicurezza applicabile (livello di garanzia ≥ «sostanziale»); il Modulo A non è consentito.
- **Critico (Allegato IV)** — Laddove designato da un atto delegato, la certificazione UE in materia di cibersicurezza è obbligatoria (livello di garanzia come specificato). Fino a tale designazione, si applica l'art. 32, paragrafo 3 (stesse opzioni di «Importante — Classe II»).

3.4. Misure pratiche per le PMI

1. **Checklist per la classificazione**: elaborare una checklist per verificare se il prodotto soddisfa i criteri della Classe I o II, includendo domande sulla sensibilità dei dati, sull'impatto sull'infrastruttura e sugli elenchi dell'Allegato.

2. **Valutazione dei rischi**: utilizzare OCTAVE Allegro o NIST SP 800-30 per valutare i rischi, concentrandosi sulla probabilità e sull'impatto. Ad esempio, valutare rischi quali violazioni dei dati o manomissione dei dispositivi.
3. **Pianificazione della conformità**: per la Classe II, identificare gli organismi notificati (ad es. tramite ENISA) e stanziare un budget per gli audit (da 50.000 a 150.000 euro). Per l'impostazione predefinita/Classe I, programmare audit interni.
4. **Documentazione**: includere nella documentazione tecnica i rapporti di classificazione, le valutazioni dei rischi e i piani di conformità.
5. **Revisioni periodiche**: rivalutare la classificazione ogni anno per tenere conto degli aggiornamenti del prodotto o delle nuove linee guida CRA.

Tabella 18 : Modello di valutazione dei rischi

Minaccia	Probabilità	Impatto	Livello di rischio	Misure di mitigazione	Prove
Accesso non autorizzato	Medio	Alto	Alto	MFA	Rapporto di prova 01/07/2025

3.5. Caso studio

Una PMI che sviluppa un gestore di password (Classe I) lo classifica in base all'Allegato III, effettua una valutazione dei rischi secondo lo standard NIST SP 800-30 (identificando rischi quali il furto delle credenziali) e incarica un organismo notificato di eseguire l'esame CE del tipo. L'autovalutazione documenta la classificazione, la valutazione dei rischi e la preparazione all'audit, garantendo la conformità ai requisiti del CRA.

3.6. Strumenti e risorse

- **Valutazione dei rischi**: OCTAVE Allegro, NIST SP 800-30, ISO 27005.
- **Documentazione**: Confluence, SharePoint.
- **Organismi notificati**: elenco ENISA.

Questa sezione suggerisce un flusso di lavoro pratico e indipendente dagli strumenti che le PMI possono utilizzare per classificare i prodotti e scegliere un percorso appropriato di valutazione della conformità CRA. Si tratta di uno dei possibili modus operandi a supporto della conformità; le

organizzazioni possono utilizzare un flusso di lavoro equivalente se produce le stesse decisioni e le stesse prove. I passaggi e gli artefatti sopra indicati sono raccomandazioni, non metodi obbligatori previsti dal CRA. Laddove il presente documento menzioni uno «strumento di valutazione del rischio», consideratelo come un termine generico per indicare qualsiasi metodo che produca i risultati funzionali elencati (ad esempio, una matrice di rischio qualitativa o una scheda di valutazione semplificata).

La presente guida sarà aggiornata in linea con le evoluzioni degli atti di esecuzione/delegati dell'UE e degli schemi di certificazione. Fino ad allora, considerare i flussi di lavoro sopra indicati come **opzioni illustrative** per strutturare la classificazione interna e la raccolta delle prove.

4. Documentazione tecnica e valutazione dei rischi

Il criterio **«Documentazione tecnica e valutazione dei rischi»** garantisce che le PMI producano una documentazione completa per dimostrare la conformità al CRA. Il CRA richiede di produrre una documentazione tecnica per ciascun prodotto, che includa descrizioni del prodotto, valutazioni dei rischi, misure di sicurezza, rapporti di prova e guide per l'utilizzatore. Questa sezione fornisce una metodologia esaustiva per la compilazione e la valutazione della documentazione, con indicazioni dettagliate, modelli e casi studio.

4.1. Requisiti di documentazione

La documentazione tecnica deve includere:

1. **Descrizione del prodotto**: specifiche dettagliate, funzionalità e destinazione d'uso.
2. **Valutazione dei rischi**: analisi completa delle minacce e delle misure di mitigazione, in linea con **la norma ISO 27005** o lo standard **NIST SP 800-30**.
3. **Conformità ai requisiti essenziali**: prova della conformità a tutti i 21 requisiti, inclusi rapporti di test e policy.
4. **Rapporti dei test**: risultati delle scansioni di vulnerabilità, dei test di penetrazione e delle revisioni del codice.
5. **Ciclo di vita dello sviluppo sicuro (SDLC)**: politiche per la codifica, il collaudo e la revisione sicuri, in linea con **OWASP SAMM** o **Microsoft SDL**.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

6. **Linee guida per gli utilizzatori**: manuali o sezioni di guida online che spiegano le funzionalità di cibersicurezza, quali l'installazione degli aggiornamenti e la segnalazione delle vulnerabilità.

4.2. Metodologia di autovalutazione

1. **Checklist della documentazione**: verificare la presenza di tutti i documenti richiesti, comprese le descrizioni dei prodotti, le valutazioni dei rischi e i rapporti di test.
2. **Processo di valutazione dei rischi**: utilizzare **STRIDE** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) o **PASTA** (Process for Attack Simulation and Threat Analysis) per identificare le minacce.
3. **Raccolta delle prove**: raccogliere i rapporti di test (ad es. Nessus, Metasploit), le SBOM e le policy relative al ciclo di vita dello sviluppo del software (SDLC).
4. **Organizzazione della documentazione tecnica**: utilizzare sistemi di gestione dei documenti come **Confluence**, **SharePoint** o **Notion** per garantire l'accessibilità e la preparazione agli audit.
5. **Aggiornamenti regolari**: pianificare revisioni trimestrali per aggiornare la documentazione, tenendo conto delle modifiche ai prodotti o delle nuove vulnerabilità.

Tabella 19 : Modello di checklist per la documentazione

Documento	Obbligatorio	Stato	Prove	Lacune	Azione
Descrizione del prodotto	Sì	Completa	Specifiche V1.2	Nessuna	N/A
Valutazione dei rischi	Sì	Parziale	Rapporto STRIDE	Mancano i dettagli sulle misure di mitigazione	Da completare entro il 01/08/2025

4.3. Misure pratiche per le PMI

1. **Sviluppare la descrizione del prodotto**: specificare hardware, software, connettività e casi d'uso. Ad esempio, la descrizione di un termostato intelligente include i protocolli Wi-Fi e l'elaborazione dei dati.
2. **Effettuare una valutazione dei rischi**: utilizzare STRIDE per identificare minacce quali l'accesso non autorizzato o la manomissione dei dati. Documentare le misure di mitigazione quali la crittografia o i controlli di accesso.
3. **Raccogliere le prove**: compilare i rapporti di test utilizzando strumenti come Nessus, OWASP ZAP o SonarQube. Includere gli SBOM e le politiche SDLC.
4. **Organizzare la documentazione**: utilizzare Confluence per creare una documentazione tecnica strutturata, con cartelle dedicate alle descrizioni, alle valutazioni e ai rapporti.
5. **Fornire indicazioni agli utilizzatori**: sviluppare manuali con chiare istruzioni sulla cibersicurezza, utilizzando i modelli della norma **ETSI EN 303 645**.

4.4. Caso studio

Una PMI che produce una telecamera intelligente predispone la documentazione tecnica:

- **Descrizione del prodotto**: specifica le caratteristiche tecniche della telecamera, la connettività Wi-Fi e l'archiviazione su cloud.
- **Valutazione dei rischi**: utilizza STRIDE per identificare minacce quali lo streaming non autorizzato, mitigate tramite TLS 1.3 e l'autenticazione a più fattori (MFA).
- **Rapporti di test**: include i risultati delle scansioni Nessus e i rapporti dei test di penetrazione.
- **SDLC**: Adotta OWASP SAMM, documentando le pratiche di codifica sicura.
- **Guida per l'utilizzatore**: fornisce un manuale con le istruzioni di aggiornamento e un'e-mail CVD.
- **Risultato**: l'autovalutazione verifica la completezza, identifica le lacune nella documentazione SDLC e pianifica le azioni correttive entro 6 mesi.

4.5. Strumenti e risorse

- **Valutazione dei rischi**: STRIDE, PASTA, NIST SP 800-30.
- **Test**: Nessus, OWASP ZAP, Metasploit.
- **Documentazione**: Confluence, SharePoint, Notion.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- **Standard**: OWASP SAMM, Microsoft SDL, ETSI EN 303 645.

Questa sezione garantisce che le PMI dispongano di una documentazione tecnica completa e pronta per l'audit, con metodologie e modelli dettagliati.

5. Processo di valutazione della conformità e Dichiarazione di conformità UE

Il criterio relativo **al processo di valutazione della conformità e alla Dichiarazione di conformità UE** completa la conformità al CRA, garantendo che le PMI seguano il modulo di valutazione appropriato ed emettano una Dichiarazione di conformità UE valida. Questa sezione fornisce una metodologia esaustiva per orientarsi in questo processo, affrontare gli obblighi successivi all'immissione sul mercato del prodotto e preparare la Dichiarazione di conformità UE.

5.1. Moduli di valutazione della conformità

Il CRA applica i seguenti moduli dell'Allegato VIII:

- **Modulo A** — Controllo interno della produzione. Il fabbricante autovaluta la conformità a tutti i 21 requisiti; conserva la documentazione tecnica e una Dichiarazione di conformità. (Utilizzato come opzione predefinita; per la Classe I solo alle condizioni di cui al punto 3.3.)
- **Modulo B** — Esame UE del tipo. Un organismo notificato valuta un «tipo» di prodotto rappresentativo rispetto ai requisiti applicabili.
- **Modulo C** — Conformità al tipo basata sul controllo interno della produzione. Il fabbricante garantisce che la produzione sia conforme al «tipo» approvato nel Modulo B.
- **Modulo H** — Garanzia di qualità totale. Un organismo notificato valuta e monitora il sistema di qualità totale del fabbricante (progettazione e produzione) in relazione ai requisiti applicabili.

Come sintetizzato al punto 3.3, quando applicato alle diverse classi di prodotti, ciò significa:

- Modulo **predefinito**: A.
- **Importante — Classe I**: Modulo A solo se vengono applicate norme armonizzate/specifiche comuni o uno schema di certificazione UE applicabile (≥ «sostanziale»); altrimenti B + C o H.
- **Importante — Classe II**: B + C o H, oppure uno schema di certificazione UE applicabile (≥ «sostanziale»); il Modulo A non è consentito.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- **Critico (Allegato IV):** certificazione UE obbligatoria se designata da un atto delegato; fino ad allora, attenersi all'art. 32, paragrafo 3 (come per «Importante — Classe II»).

5.2. Metodologia di autovalutazione

1. **Determinare il modulo**: identificare il modulo richiesto in base alla classificazione (predefinito, Classe I o Classe II).
2. **Effettuare valutazioni interne**: per i dispositivi predefiniti e di Classe I, verificare la conformità a tutti i requisiti utilizzando la checklist di autovalutazione.
3. **Coinvolgere gli organismi notificati**: per i dispositivi di Classe II, presentare la documentazione tecnica a un organismo notificato e dare seguito ai risultati dell'audit.
4. **Adempiere agli obblighi post-commercializzazione**: monitorare le vulnerabilità, rilasciare aggiornamenti e mantenere la documentazione per tutto il ciclo di vita del prodotto.
5. **Rilasciare la dichiarazione**: firmare la Dichiarazione di conformità UE, attestando la conformità ai requisiti CRA.

Tabella 20 : Modello di Dichiarazione di conformità UE

Dichiarazione di conformità UE
Prodotto: [Nome del prodotto] Fabbricante: [Nome dell'azienda, indirizzo] Con la presente dichiariamo che il prodotto sopra indicato è conforme al Regolamento (UE) 2024/2847 (Cyber Resilience Act). Requisiti essenziali: Piena conformità all'Allegato I. Valutazione di conformità: [Modulo, ad es. Controllo interno della produzione] Norme applicate: [ad es., ETSI EN 303 645, ISO 27001] Data: [AAAA-MM-GG] Firmato: [Nome, Titolo]

5.3. Passaggi pratici per le PMI

1. **Verifica della classificazione**: confermare la classe del prodotto per determinare il modulo di valutazione.
2. **Effettuare audit interni**: utilizzare la checklist di autovalutazione per verificare la conformità, corredata da rapporti di prova e documentazione.
3. **Coinvolgere gli organismi notificati**: per la Classe II, contattare gli organismi accreditati (ad esempio tramite l'ENISA), presentare la documentazione tecnica e prepararsi agli audit.
4. **Monitoraggio post-commercializzazione**: utilizzare strumenti come Snyk o l'NVD del NIST per monitorare le vulnerabilità, rilasciando patch se necessario.
5. **Rilasciare la dichiarazione**: redigere e firmare la Dichiarazione di conformità UE, includendola nella documentazione tecnica.

5.4. Caso studio

Una PMI che sviluppa un giocattolo intelligente di Classe I effettua un audit interno, verificando la conformità a tutti i 21 requisiti utilizzando i rapporti di Nessus e OWASP ZAP. L'autovalutazione conferma la completezza della documentazione, portando alla firma della Dichiarazione di conformità UE. Per un firewall di Classe II, la PMI coinvolge un organismo notificato, presenta i rapporti di prova e risolve i risultati dell'audit entro 3 mesi, documentando il processo.

5.5. Strumenti e risorse

- **Audit**: Confluence per il monitoraggio degli audit, Nessus per i test.
- **Organismi notificati**: elenco ENISA.
- **Standard/Norma**: ETSI EN 303 645, ISO 27001.

Questa sezione garantisce che le PMI completino il processo di valutazione della conformità e mantengano la conformità, con metodologie e modelli dettagliati.

Conclusione

Questo quadro metodologico per la valutazione della conformità fornisce **supporto alle PMI nell'attuazione del Cyber Resilience Act dell'UE**, attraverso indicazioni approfondite, esempi pratici, casi studio e strumenti relativi a **cinque criteri chiave** del CRA: (1) Conformità ai requisiti essenziali di cibersicurezza, (2) Certificazione dei prodotti con elementi digitali, (3) Classificazione dei prodotti in Classe I o Classe II e azioni corrispondenti, (4) Completezza della documentazione tecnica e (5) Procedure generali di valutazione della conformità. In linea con gli obiettivi del progetto SECURE, le linee guida mirano a rendere tangibili gli obblighi del CRA attraverso raccomandazioni basate su approcci riconosciuti e best practice nel settore della cibersicurezza; tuttavia, mantengono un carattere puramente indicativo.

In base ai futuri sviluppi del contesto giuridico del CRA, le linee guida potrebbero essere soggette a modifiche. Come passi successivi per le PMI, si raccomanda di consultare ulteriori linee guida presenti **nell'archivio SECURE**, quali **«I requisiti essenziali di cibersicurezza del CRA: Allegato I, Parte I»** per suggerimenti pratici e raccomandazioni relative a ciascuna delle disposizioni dell'Allegato I, nonché **«CRA 101: Comprendere gli obblighi del CRA»** per una panoramica sintetica degli obblighi legali previsti dal CRA.