CyberSic

Manuale d'uso

Registro dei rischi ISO/IEC 27005, controlli e Dichiarazione di Applicabilità ISO/IEC 27001, checklist ISO/IEC 27002, piano di trattamento, sistema di gestione, revisioni e rivalutazione.

Edizione del 17/10/2026 · cybersic.data-set.it/manuale

Indice

Introduzione
- Il percorso verso la certificazione
- Versione di prova e con abbonamento
- I registri di esempio

Da dove cominciare
- 1 — Preparare
- 2 — Valutare il rischio
- 3 — Mettere in piedi il sistema
- 4 — Far funzionare il sistema
- 5 — Verso la certificazione
- Il ritmo, una volta avviato

Accesso e registri
- Accedere
- L'elenco dei registri e il cruscotto

La pagina del registro
- Il glossario
- Il salvataggio

Organizzazione e criteri

Ruoli e persone

Adempimenti
- Chi verifica e chi approva

Passo 1 — Asset
- Schede e griglia
- Gli asset in CSV
- Come classificare
- Archivi e classificazione

Passo 2 — Minacce e rischio
- Le minacce in CSV
- Le matrici dei collegamenti
- Come si calcola il rischio
- Perché vale il controllo più efficace

Passo 3 — Controlli e SoA
- La checklist di verifica
- La guida ISO/IEC 27002 ai controlli
- I controlli in CSV

Passo 4 — Trattamento
- Da dove vengono i trattamenti

Revisioni e rivalutazione

Sistema di gestione: i registri
- Gli indicatori
- La checklist di audit
- La copertura del programma di audit
- Il fascicolo per il riesame
- I registri in CSV
- Allegare file

Conformità e miglioramento
- L'analisi del contesto (facoltativa)
- Analisi del contesto: scenario, esempio, passi successivi

Impostazioni: estensioni e campi codificati
- Gli elenchi che si regolano

Riepilogo
- La mappa della norma ISO/IEC 27001

Documenti da stampare

Importare ed esportare

Domande frequenti e avvertenze

Appendice — I modelli delle finestre

Appendice — Revisioni del manuale

Introduzione

CyberSic accompagna un'organizzazione nel percorso di certificazione ISO/IEC 27001: dalla valutazione del rischio all'applicazione dei controlli, ai trattamenti, fino alla rivalutazione periodica. Ogni organizzazione (o ogni sede, o ogni ambito del sistema di gestione) ha il suo **registro dei rischi**, che contiene tutto: asset, minacce, controlli con la Dichiarazione di Applicabilità, risposte alla checklist, piano di trattamento, revisioni.

Il metodo di calcolo è quello del foglio «Registro dei rischi ISO/IEC 27005» da cui il programma nasce: un registro fatto con quel foglio si importa in CyberSic e dà gli stessi numeri.

Il percorso verso la certificazione

Sezione	Che cosa si fa	Requisito ISO/IEC 27001
Organizzazione	Dati dell'organizzazione, campo di applicazione, criteri di valutazione del rischio	4.3, 6.1.2 a
Passo 1 — Asset	Censimento delle informazioni e valori di riservatezza, integrità, disponibilità	6.1.2 c
Passo 2 — Minacce	Identificazione delle minacce, verosimiglianza, conseguenze, rischio	6.1.2 c, d, e
Passo 3 — Controlli	Applicabilità dei controlli (SoA), verifica con la checklist, valutazione	6.1.3 b, c, d
Passo 4 — Trattamento	Opzione, azioni, responsabili, scadenze, rischio residuo e sua accettazione	6.1.3 e, f; 8.3
Revisioni	Consolidamento del registro approvato e rivalutazione nel tempo	8.2, 9.3
Ruoli e persone	Ruoli e responsabilità, personale, competenze, prese visione, organigramma, mansionari	5.2, 5.3, 7.2, 7.3
Adempimenti	Attività periodiche assegnate ai ruoli, con scadenze, avvisi ed esecuzioni	8.1, 9.1
Sistema	Documenti, procedure, audit con la checklist e la copertura del programma, incidenti, inventario, obiettivi, indicatori, formazione, riesami con il fascicolo	6.2, 7.5, 9.1, 9.2, 9.3
Conformità	Analisi del contesto (facoltativa), non conformità e azioni correttive, fornitori, requisiti legali e contrattuali, cambiamenti, rischi e opportunità del sistema, comunicazione, contatti, continuità operativa	4.1, 4.2, 6.1.1, 6.3, 7.4, 8.1, 10.2; controlli 5.5, 5.6, 5.19–5.23, 5.29–5.34

L'analisi del contesto (4.1, 4.2: fattori interni ed esterni, parti interessate e loro esigenze) si può fare in due modi: registrare nella Documentazione di sistema quella che c'è già, fatta per un altro sistema di gestione, oppure farla qui, con la pagina facoltativa Analisi del contesto, che ne genera il documento. Gli obblighi di legge e di contratto che ne derivano hanno il loro registro (Conformità).

Versione di prova e con abbonamento

La **versione di prova** si apre dal pulsante «Prova» della pagina iniziale, senza registrazione. Il registro è uno solo ed è legato all'indirizzo da cui ci si collega: chi usa la stessa rete vede lo stesso registro, e se l'indirizzo cambia non lo si ritrova più. **Non inserire dati reali o riservati** nella versione di prova; per conservare quello che si è fatto, esportarlo in XML. Il registro di prova che nessuno usa per **sette giorni** viene cancellato: ogni volta che lo si riapre i sette giorni ripartono.

Con l'abbonamento ogni utente ha la sua area riservata, non raggiungibile dal web, con più registri separati. Gli allegati ci sono solo con un'utenza.

I registri di esempio

Nella pagina iniziale, sotto i pulsanti del manuale, ci sono tre registri già compilati, di organizzazioni inventate, da aprire mentre si legge questo manuale:

- **Studio tecnico: il percorso completo** — uno studio di progettazione con asset, minacce, controlli valutati con la checklist e trattamenti; ha una **revisione 1.0 già consolidata** e i miglioramenti fatti dopo, così nella sezione Revisioni si può provare subito la rivalutazione (il rischio ransomware scende da Alto a Medio).
- **Poliambulatorio: dati sanitari e SoA** — asset con i campi privacy compilati e una Dichiarazione di Applicabilità con esclusioni motivate.
- **Software in cloud: sviluppo e controlli cloud** — controlli ISO/IEC 27017 e 27018, criteri di valutazione più severi (Medio da 16, Alto oltre 32) e un'azione scaduta.

Tutti e tre hanno anche qualche riga in ciascuno dei registri del sistema di gestione, legata al resto: l'audit che ha trovato la non conformità, la procedura rivista per trattare quel rischio, l'incidente collegato all'asset e alla minaccia, gli obiettivi collegati ai trattamenti, gli indicatori con le loro misurazioni (in obiettivo, da migliorare, fuori soglia), il riesame della direzione che li riassume. Alcune date sono volutamente passate (una revisione da fare, una garanzia scaduta), per vedere come vengono segnalate.

Nella versione di prova l'esempio **prende il posto** del registro che c'è (la pagina lo chiede prima); per chi è entrato con la propria utenza diventa un registro nuovo in elenco, che si può archiviare quando non serve più.

Da dove cominciare: dal registro vuoto alla certificazione

Un percorso consigliato per chi parte da zero. L'ordine non è obbligatorio — il programma accetta i dati in qualunque ordine — ma conviene: ogni passo prepara il successivo (i ruoli scritti all'inizio, per esempio, vengono poi proposti in tutti i campi dei responsabili). Per ogni passo: che cosa fare, dove, e il punto della norma a cui risponde. In qualunque momento la mappa della norma (Riepilogo) dice che cosa c'è e che cosa manca.

Fase 1 — Preparare (una giornata)

1. **Guardare un esempio.** Aprire lo «Studio tecnico» dalla pagina iniziale (I registri di esempio) e scorrere le sezioni: si vede in mezz'ora come appare un registro compilato.
2. **Creare il registro** dell'organizzazione dall'elenco dei registri (L'elenco dei registri). Un registro per ogni organizzazione o per ogni campo di applicazione separato.
3. **Organizzazione** (Organizzazione e criteri): dati dell'organizzazione, **campo di applicazione**, **confini e interfacce**; i criteri di valutazione si lasciano ai valori predefiniti, salvo ragioni precise. *4.3, 6.1.2.*
4. **Ruoli** (Ruoli e persone): la direzione, chi è responsabile della sicurezza delle informazioni, chi gestisce i sistemi (anche un consulente esterno), il referente privacy o il DPO, le funzioni che trattano dati importanti. Per ciascuno compiti, competenze richieste e «Riporta a». *5.3.*
5. **Personale**: le persone con email, i ruoli che ricoprono, se ricevono gli avvisi, le competenze che hanno. L'organigramma si compone da solo. *5.3, 7.2.*
6. **Impostazioni** (Impostazioni), solo se servono: le unità organizzative, la scala di classificazione dell'organizzazione se è diversa da quella proposta, le estensioni cloud o privacy dei controlli se l'organizzazione ne ha bisogno.

Fase 2 — Valutare il rischio (alcune settimane)

7. **Asset** (Passo 1): le informazioni e ciò che le contiene, **per insiemi** («progetti in corso», «portatili dei tecnici», «gestionale in cloud»), non bene per bene; per ciascuno categoria, referente, classificazione, valori di riservatezza, integrità e disponibilità. Un elenco già fatto in un foglio di calcolo si carica in CSV (Gli asset in CSV). *6.1.2 c.*
8. **Minacce** (Passo 2): «Dal catalogo ISO/IEC 27005…» si spuntano quelle pertinenti e si aggiungono in blocco; per ciascuna gli asset colpiti e la verosimiglianza. La matrice minacce × asset fa vedere che cosa manca. Il rischio lo calcola il programma. *6.1.2 c, d, e.*
9. **Controlli e SoA** (Passo 3): tema per tema, per ogni controllo applicabile o escluso, con la **giustificazione**; per gli applicabili lo stato di attuazione, la checklist di verifica, la valutazione, il responsabile e come è attuato; poi i controlli si collegano alle minacce che riducono. La guida ISO/IEC 27002 spiega ogni controllo. *6.1.3 b, c, d.*
10. **Trattamento** (Passo 4): per i rischi medi e alti l'opzione, le azioni, il responsabile, la scadenza, il proprietario del rischio e l'accettazione del rischio residuo. Dalle azioni si creano gli **obiettivi** con «Crea un obiettivo da questo trattamento». *6.1.3 e, f; 6.2.*
11. **Prima revisione** (Revisioni): quando la direzione approva valutazione, SoA e piano, si consolida la revisione 1.0 e si stampano registro, SoA e piano (Documenti da stampare). *6.1.2, 6.1.3, 8.2.*

Fase 3 — Mettere in piedi il sistema

12. **Politica e documenti** (Sistema › Documentazione di sistema): la politica per la sicurezza (tipo «Politica», approvata, in vigore) e le **prese visione** del personale dalla sua finestra; le procedure, con le loro revisioni. *5.2, 7.3, 7.5*.
13. **Analisi del contesto** (L'analisi del contesto): se c'è già, fatta altrove, la si registra nella Documentazione di sistema con «4.1, 4.2» nel riferimento; altrimenti la si fa qui — fattori interni ed esterni, parti interessate, metodo, cambiamento climatico, conclusioni — e «Genera il documento» la registra da sola. Conviene farla prima o insieme ai requisiti e ai rischi del sistema, che ne derivano; meglio ancora abbozzarla già durante la Fase 2, perché ne vengono anche minacce da valutare e il perimetro del campo di applicazione (vedi lo scenario di lavoro e i passi successivi). *4.1, 4.2*.
14. **Conformità** (Conformità e miglioramento): i **requisiti** di legge e di contratto, i **fornitori** che trattano dati o gestiscono sistemi, i **contatti** per le emergenze, i processi della **continuità operativa**, il **piano di comunicazione**, i **rischi e le opportunità del sistema**. *4.2, 6.1.1, 7.4, 8.1; controlli 5.5, 5.6, 5.19–5.23, 5.29–5.34*.
15. **Adempimenti** (Adempimenti): le attività periodiche che i controlli richiedono — verifica delle utenze, controllo dei log, prove di ripristino, revisione dei documenti, valutazione dei fornitori, prove dei piani di continuità — ciascuna con il suo ruolo, la ripetizione e gli avvisi. *8.1*.
16. **Indicatori** (Gli indicatori): poche misure dell'efficacia di controlli e trattamenti, con obiettivo e soglia, collegate agli obiettivi. *6.2, 9.1*.
17. **Formazione** (Sistema › Formazione): la sensibilizzazione per tutti e la formazione per i ruoli, con i partecipanti scelti dal personale e la verifica dell'efficacia. *7.2, 7.3*.
18. **Inventario** (Sistema › Inventario): i beni uno per uno, collegati agli asset e assegnati alle persone, così alla cessazione si sa che cosa farsi restituire. *Controlli 5.9, 5.11*.

Fase 4 — Far funzionare il sistema (qualche mese)

19. **Registrare quello che succede**: gli adempimenti eseguiti («Fatto» dal cruscotto), le misurazioni degli indicatori, gli **incidenti**, le **non conformità** con le azioni correttive, i **cambiamenti** prima di farli. *6.3, 8.1, 9.1, 10.2*.
20. **Audit interno** (La checklist di audit): un audit pianificato nel registro degli audit, condotto con la checklist; dalle domande con esito NC o RACC si aprono le non conformità. La copertura dice che cosa resta da verificare negli audit successivi. *9.2*.
21. **Riesame della direzione** (Il fascicolo per il riesame): «Proponi i testi nei campi vuoti» raccoglie gli elementi in ingresso dai registri; la direzione scrive decisioni e azioni. Poi si aggiorna la valutazione del rischio e si consolida una nuova revisione. *9.3, 8.2, 10.1*.

Fase 5 — Prepararsi alla certificazione

22. **Mappa della norma** (La mappa della norma): portare ogni punto a «completo», scrivere per ognuno **chi ne risponde** e, nella nota, dove stanno le evidenze che non sono nel portale. Il giorno dell'audit la mappa porta in un clic alle registrazioni di ogni punto.
23. **Le stampe** da avere pronte: registro dei rischi, SoA, piano di trattamento, mappa della norma, rapporti su obiettivi e indicatori, ultimo audit con la checklist, fascicolo e verbale del riesame, organigramma e mansionari.

Il ritmo, una volta avviato

Quando	Che cosa
Ogni settimana	Il cruscotto degli adempimenti: eseguire quelli in scadenza, registrare l'esecuzione. Gli avvisi per email ricordano a chi tocca.
Quando succede	Un incidente, una non conformità, una segnalazione, un cambiamento, un fornitore nuovo, una persona che entra o esce (ruoli, beni, accessi, prese visione).
Ogni tre mesi	Le misurazioni degli indicatori; uno sguardo alla mappa della norma e alle non conformità aperte nel Riepilogo.
Ogni anno	Audit interno, riesame della direzione, rivalutazione del rischio con una nuova revisione, sensibilizzazione, revisione della politica e dei documenti in scadenza, valutazione dei fornitori, prova dei piani di continuità.

Accesso e registri

Accedere

Dalla pagina iniziale, «Login»: si entra con l'indirizzo e-mail e la password. Se per l'utenza è attiva la verifica in due passaggi, arriva per posta un codice da inserire. Chi ha dimenticato la password la recupera dalla stessa finestra: arriva per posta un link per sceglierne una nuova, che vale un'ora e una volta sola (finché non lo si usa, la password attuale resta valida). Una password provvisoria data dall'amministratore va cambiata al primo accesso.

Dopo cinque tentativi falliti sullo stesso indirizzo, o venti dalla stessa rete, l'accesso resta fermo per un quarto d'ora.

Con la stessa utenza si lavora da **una postazione per volta**: un nuovo accesso, da un altro computer o da un altro browser, chiude la sessione di prima. Chi la stava usando, alla prima operazione, viene riportato alla pagina iniziale, dove legge che cosa è successo e a che ora è stato fatto l'altro accesso; se non è stato lui, conviene cambiare subito la password. Lo stesso succede se l'utenza viene sospesa o cancellata, se la password viene cambiata o dopo un'ora senza operazioni. Le modifiche già salvate restano; quelle non ancora confermate con Salva si perdono. Uscire con il comando di uscita chiude la sessione anche sul server; chiudere la finestra del browser no.

L'elenco dei registri e il cruscotto

Dopo l'accesso si arriva all'elenco dei registri. In alto il **cruscotto** riassume tutti i registri: quanti sono, quanti hanno una revisione consolidata, i rischi alti e medi, quelli medi o alti ancora senza una decisione di trattamento, le azioni aperte e quelle scadute. Nella tabella, per ogni registro, gli stessi numeri e l'ultima revisione.

- **Nuovo registro**: codice, organizzazione (o descrizione), riferimento (sede, ambito, commessa) e data. Memorizzando, il registro si crea e si apre subito; l'organizzazione diventa l'intestazione del registro.
- Un clic su una riga apre la scheda, con il pulsante **Apri il registro**.
- **Archivia** toglie il registro dall'elenco. Il file non viene cancellato: resta conservato fra gli archiviati.
- L'elenco si esporta in CSV o XML, con i numeri del cruscotto.

La pagina del registro

Nella barra viola in alto, a sinistra: il logo (torna all'elenco), **importa** e **esporta** il registro in XML, il menu delle **stampe** e il manuale; a destra il registro aperto e lo stato del salvataggio. Subito sotto, nella **barra bianca delle sezioni**, le funzioni principali nell'ordine in cui si lavora: Organizzazione, Ruoli e persone, Asset, Minacce, Controlli, Trattamento, Adempimenti, Revisioni, Sistema, Conformità, Riepilogo, e l'ingranaggio delle Impostazioni. La sezione aperta è piena di colore; su uno schermo stretto la barra scorre di lato.

Vai a… Al centro della barra viola c'è una casella di ricerca delle funzioni: si scrive una parte del nome di quello che si cerca (per esempio «fattori», «obiettivi», «SoA», «organigramma», «matrice») e compare l'elenco delle sezioni, dei registri, delle pagine e delle stampe che corrispondono, ciascuno con la sezione in cui sta. Con le frecce e Invio, o con un clic, si va lì come se si fosse passati dai menu: non serve ricordare dove sta un registro. Ctrl+K porta alla casella da qualunque punto della pagina; Esc la chiude. Sugli schermi stretti la casella non c'è.

Il glossario

La norma usa i termini con un significato preciso, e usarli allo stesso modo in documenti, registri e risposte all'audit evita equivoci. L'icona **Glossario** della barra viola (accanto al manuale) apre a destra i **termini e le definizioni** della ISO/IEC 27002:2022 (punto 3: controllo, asset, minaccia, vulnerabilità, incidente, politica specifica, RPO e RTO…), con note, esempi e la norma da cui ciascuno viene, e in fondo le **abbreviazioni** (ABAC, BIA, SIEM, SSO…). La casella in alto cerca nei termini, nelle definizioni e nelle sigle; i rimandi fra i termini («asset (3.1.2)») sono collegamenti. Il pannello resta aperto accanto alla scheda o alla finestra che si sta compilando. Anche «Vai a…» trova ogni termine e ogni sigla.

Asset, minacce, controlli e trattamenti sono **schede**: un clic sulla testata le apre o le chiude; la scheda aperta è evidenziata. La testata riporta già l'essenziale (per una minaccia, la fascia e il valore del rischio attuale). I pulsanti **Apri tutte** e **Chiudi** aprono o chiudono insieme le schede elencate, e la barra dei filtri resta in alto mentre si scorre la pagina. L'avviso della versione di prova si può chiudere.

Il salvataggio

Le modifiche **si confermano**. Un campo cambiato diventa giallo e resta **da salvare**: la scheda lo dice anche da chiusa («da salvare» accanto al titolo) e in fondo alla scheda compare la barra con **Salva** e **Annulla modifiche**. In basso al centro della pagina si legge quante modifiche sono in sospeso in tutto il registro, con **Salva tutto** e **Annulla**; anche **Ctrl+S** salva tutto. Rimettere in un campo il valore di prima toglie la modifica.

Le modifiche in sospeso non si perdono cambiando sezione, filtrando o chiudendo una scheda; si perdono chiudendo la pagina (il browser chiede conferma) o importando un registro (il programma avvisa).

Salva scrive le modifiche **tutte insieme o nessuna**: se un valore non è accettato (una data impossibile, una soglia incoerente) compare il motivo, il campo diventa rosso e non si salva niente, nemmeno le altre modifiche; si corregge e si preme di nuovo Salva. I numeri del rischio si aggiornano dopo il salvataggio: li calcola il programma sul server, gli stessi che finiscono nelle stampe e nelle revisioni.

Organizzazione e criteri

I dati dell'organizzazione (denominazione, indirizzo, P.IVA, recapiti, DPO, chi redige, versione e data del documento) compaiono nell'intestazione di tutte le stampe. Il **campo di applicazione** descrive l'ambito del sistema di gestione; sotto, i **confini, le interfacce e le dipendenze** (4.3 c): che cosa resta fuori (una sede, un servizio affidato all'esterno) e dove il sistema tocca quello di altri (il consulente informatico, il fornitore del servizio in cloud). Si stampano nel registro dei rischi e viaggiano con l'esportazione.

I **criteri di valutazione** sono le due soglie che dividono il rischio in fasce. Con i valori predefiniti — gli stessi del foglio di calcolo originale — il rischio è **Basso sotto 20**, **Medio fino a 40**, **Alto oltre 40**. Si possono cambiare per registro; cambiano le fasce, non i valori.

Ruoli e persone

Le responsabilità su asset, controlli, trattamenti e su ogni riga dei registri si assegnano a **ruoli**; le **persone** ricoprono uno o più ruoli. Così, quando una persona cambia, si cambia chi ricopre il ruolo e tutto quello che è assegnato al ruolo resta al suo posto. La sezione **Ruoli e persone** ha tre registri e due pagine.

- **Ruoli**: nome, sigla, tipo (direzione, funzione aziendale, sicurezza delle informazioni, protezione dei dati, comitato, esterno), **a chi riporta**, scopo, **compiti e responsabilità** (uno per riga: sono il mansionario), autorità e deleghe, competenze richieste. Nella finestra del ruolo si spuntano le persone che lo ricoprono. Un ruolo non può riportare a se stesso né a un ruolo che gli riporta.
- **Personale**: cognome e nome, email, telefono, funzione, rapporto (dipendente, collaboratore, consulente, fornitore), stato (in servizio, assente, cessato), i **ruoli ricoperti** (si spuntano), se **riceve gli avvisi degli adempimenti** per email, e le **competenze possedute** con le loro evidenze (titoli, attestati, esperienza).
- **Prese visione**: chi ha ricevuto e letto un documento del sistema — la politica, una procedura, le regole d'uso — in quale versione, quando e come. Il modo più rapido è dalla finestra del documento (sezione Sistema, «Documentazione di sistema»): il riquadro **Prese visione** elenca il personale in servizio, con la spunta verde per chi ha già letto la versione in vigore; si spuntano gli altri, si sceglie come (firma, email, portale…) e **Registra la presa visione di oggi**. Le prese visione si scrivono subito, senza passare da Salva. Quando il documento cambia versione, l'elenco riparte: chi aveva letto quella di prima è segnato «versione precedente».

Le evidenze della persona (7.2, 7.3). Nel registro della **formazione** i partecipanti si scelgono anche dal personale (le caselle «Partecipanti scelti dal personale»), e nell'**inventario** un bene si assegna a una persona del personale. Il mansionario della persona mette così insieme le **competenze richieste** dai suoi ruoli e quelle che ha, la **formazione** a cui ha partecipato, i **documenti** di cui ha preso visione — e, in rosso, le politiche in vigore che non ha ancora letto — e i **beni** che ha in consegna.

Alla cessazione (controlli 5.11, 5.18, 6.5). Quando una persona passa a «Cessato», la sua finestra e il suo mansionario dicono che cosa resta da chiudere: i beni dell'inventario ancora «In uso» da farsi restituire, i ruoli che ricopriva e che vanno passati ad altri, gli accessi da revocare.

I responsabili. I campi che nominano un responsabile — il referente di un asset, il responsabile di un controllo, il responsabile e il proprietario di un trattamento, il responsabile di un documento, di un incidente, di un obiettivo, di un indicatore, chi approva — propongono i ruoli del registro mentre si scrive: si sceglie il ruolo, o si scrive altro. Un campo che porta il nome (o la sigla) di un ruolo conta fra le responsabilità di quel ruolo. Se il ruolo cambia nome, quei campi lo seguono da soli. Gli adempimenti invece si assegnano al ruolo scegliendolo da un menu.

Organigramma. Ricavato dai ruoli («Riporta a») e dal personale: in cima i ruoli che non riportano a nessuno, sotto quelli che riportano a loro, in ogni casella il ruolo, la sigla e le persone che lo ricoprono («da assegnare» se nessuno). I ruoli esterni hanno la cornice tratteggiata. Si stampa dalla pagina o dal menu delle stampe.

Mansionari. Per ruolo: scopo, compiti, autorità, competenze, chi lo ricopre, e **tutto quello che nel registro è assegnato al ruolo** — asset di cui è referente, controlli di cui è responsabile, trattamenti, adempimenti con la ripetizione e la prossima scadenza, righe dei registri (documenti, incidenti, obiettivi, indicatori…). Per persona: i suoi ruoli, ciascuno con compiti e responsabilità, e quello che la nomina per nome (anche con il titolo davanti, «Arch. Paolo Verdi»). Si sceglie un ruolo o una persona, o tutti; la stampa ne mette uno per pagina, su foglio verticale. Nel mansionario di una persona ogni ruolo sta in un riquadro con la sua fascia di titolo, e così «Assegnato per nome» e le evidenze (competenze, formazione, prese visione, beni): si vede subito dove finisce un ruolo e comincia l'altro. I titoli non restano soli in fondo a una pagina e gli elenchi brevi non si spezzano.

Ruoli e persone viaggiano con l'esportazione in XML ed entrano nelle revisioni, come gli altri registri; si esportano e si importano anche in CSV (i ruoli di una persona separati da « | »).

Adempimenti

Un **adempimento** è un'attività da svolgere a scadenza, quasi sempre ripetuta: la verifica delle utenze attive, il controllo dei log del firewall e dei server, la prova di ripristino dei salvataggi, il riesame dei diritti privilegiati. Si assegna a un **ruolo**, e le persone che lo ricoprono ricevono gli **avvisi per email**.

- **Prima scadenza**, **Ripeti ogni** N **giorni, settimane, mesi o anni**, e se serve **Fino al** (termine). Senza ripetizione l'adempimento ha una scadenza sola. I mesi si contano dalla prima scadenza: dal 31 gennaio, ogni mese, si va al 28 febbraio, al 31 marzo, al 30 aprile.
- **Avvisi**: i giorni rispetto alla scadenza, separati da spazi. Negativi **prima**, zero il giorno stesso, positivi **dopo** (un sollecito se non è stato fatto): `-30 -7 0 +3` vuol dire un mese prima, una settimana prima, il giorno stesso e tre giorni dopo.
- I **controlli collegati** (per codice, come negli indicatori), il riferimento (norma, legge, procedura), dove si registra l'esito, lo stato (attivo, sospeso, concluso: sospesi e conclusi non danno scadenze né avvisi).

Le esecuzioni. Ogni volta che l'adempimento si fa se ne registra l'esecuzione: a quale scadenza si riferisce, quando è stato fatto, da chi, l'esito (eseguito, eseguito con rilievi, non eseguito), le evidenze e le note. Una scadenza con un'esecuzione «eseguito» o «eseguito con rilievi» è chiusa, e i suoi avvisi si fermano. Il modo più rapido è il pulsante **Fatto** accanto alla scadenza (nel cruscotto o nella finestra dell'adempimento): crea l'esecuzione con la data di oggi, e si completano esito ed evidenze prima di Salva. La **prossima scadenza** è la prima non ancora fatta: se è passata, l'adempimento è **scaduto** (le scadenze passate senza esecuzione si contano come arretrate); se è vicina — entro il primo avviso, o una settimana — è **in scadenza**; altrimenti è regolare.

Il cruscotto (la prima pagina della sezione): quanti adempimenti sono scaduti, in scadenza, regolari, e quanti si sono eseguiti negli ultimi 30 giorni; l'elenco di quelli **da fare**, con il pulsante Fatto; il **calendario** del mese, con ogni scadenza colorata (verde fatta, rossa scaduta e non fatta, arancio in scadenza, azzurra da fare) e le frecce per gli altri mesi; la **timeline**, un adempimento per riga da un mese prima a tre mesi dopo, con la linea di oggi; e gli **avvisi per email di oggi**, con i destinatari e se sono già partiti. Un clic su una scadenza apre l'adempimento.

Gli avvisi per email partono una volta al giorno, per tutti i registri. Per ogni adempimento attivo, per la sua prossima scadenza, parte l'ultimo avviso il cui giorno è arrivato (chi riapre il programma dopo una settimana non riceve tutti gli avvisi persi, ma uno), e ogni avviso parte una volta sola. Lo ricevono le persone che ricoprono il ruolo dell'adempimento, in servizio, con «riceve gli avvisi» attivo e un indirizzo valido. Nella versione di prova non partono (non c'è un destinatario). Lo **scadenzario** si stampa dal cruscotto o dal menu delle stampe: gli adempimenti dal più urgente, con ruolo e persone, ripetizione, prossima scadenza, arretrate, ultima esecuzione e avvisi, e le scadenze dei prossimi 90 giorni.

Chi verifica e chi approva

Per gli adempimenti di maggiore rilevanza si possono indicare, oltre al ruolo responsabile, **chi verifica** e **chi approva** (due ruoli, nella finestra dell'adempimento, sulla stessa riga del ruolo responsabile e dei controlli collegati, in quest'ordine). Sono **facoltativi**: se restano vuoti l'adempimento funziona come prima; se si compilano, ogni esecuzione attende la verifica, l'approvazione o tutte e due, in quest'ordine.

- Nella tabella delle esecuzioni compaiono le colonne **Verifica** e **Approvazione**: si sceglie l'esito («Verificato», «Verificato con osservazioni», «Da rifare»; «Approvato», «Non approvato») e si scrive chi l'ha dato. La data la mette il programma, se manca; nella finestra dell'esecuzione ci sono anche le date e le note della verifica e dell'approvazione.

- Il controllo è **morbido**: un'esecuzione fatta chiude comunque la sua scadenza, anche se la verifica o l'approvazione mancano. Restano solo segnalate come **da verificare** o **da approvare**: accanto allo stato dell'adempimento, nella sua finestra e nel riquadro **Da verificare e da approvare** del cruscotto.
- Soltanto due esiti riaprono la scadenza, perché dicono che l'attività non va bene così: una verifica **«Da rifare»** e un'approvazione **«Non approvato»**. Dopo una verifica «Da rifare» non si chiede l'approvazione.
- Le persone del ruolo che verifica o approva ricevono un **avviso per email**, una volta sola per esecuzione, quando tocca a loro (con le stesse regole degli altri avvisi). Nel loro mansionario l'adempimento compare con l'indicazione «verifica» o «approva».
- Nello **scadenzario** (la stampa) una colonna dice chi verifica e chi approva ogni adempimento e quante esecuzioni aspettano; sotto, l'elenco delle **esecuzioni da verificare e da approvare**, dalla più vecchia, con chi le ha eseguite e che cosa attendono. Se nessun adempimento ha chi verifica o chi approva, la colonna e l'elenco non compaiono.
- Anche nelle **stampe dei registri** degli adempimenti e delle esecuzioni c'è la colonna **Verifica e approvazione**: per l'adempimento chi verifica, chi approva e quante esecuzioni aspettano; per l'esecuzione l'esito della verifica e dell'approvazione con chi e quando (in rosso «Da rifare» e «Non approvato») e che cosa attende. In testa, quante esecuzioni sono da verificare e da approvare. Anche qui, senza ruoli la colonna non compare.

Passo 1 — Asset

Ogni scheda è un'informazione o un asset trattato dall'organizzazione (un archivio, un servizio, un sistema, un insieme di documenti). Per ciascuno si indicano unità organizzativa, trattamento e finalità, ruolo dell'organizzazione (titolare, contitolare, responsabile) e soprattutto i tre **valori**:

- **Riservatezza**, **Integrità**, **Disponibilità**: da 1 (Basso) a 4 (Critico). Sono il danno che l'organizzazione subirebbe se l'informazione fosse divulgata, alterata o non disponibile.

Nelle note si scrive perché si sono dati quei valori: è la prima cosa che un auditor chiede. Seguono MTPD (tempo massimo di indisponibilità tollerabile), archivi, classificazione, referente, e i campi facoltativi per la privacy (interessati, tipi di dati, base giuridica, fornitori, destinatari, trasferimenti extra SEE, tempi di conservazione).

Categoria, classificazione, unità organizzativa, ruolo e base giuridica sono **campi codificati**: si scelgono da un elenco, che ogni registro regola nelle Impostazioni. Che cosa scrivere in archivi e classificazione è spiegato in Archivi e classificazione.

Ogni asset ha una **categoria**; le sei proposte sono quelle con cui di norma si classificano: **Informativi**, **Software**, **Hardware**, **Infrastrutture**, **Human**, **Intangibili**. Le schede sono raggruppate per categoria, e si filtrano per categoria e per testo. La categoria non entra nel calcolo: serve a ragionare su asset che hanno minacce e controlli simili, e dice come arrivare al valore (vedi Come classificare).

Ogni asset ha anche uno **stato**: **ONLINE** (in esercizio), **OFFLINE** (fuori esercizio ma ancora dell'organizzazione: spento, in magazzino, sospeso — i dati che contiene vanno ancora protetti) o **ELIMINATO** (dismesso o ceduto). Un asset nuovo nasce ONLINE. Lo stato compare sulla scheda, in griglia, nelle matrici e nella stampa del registro, e si può filtrare.

Un asset **ELIMINATO resta nel registro**, con la sua storia e i suoi collegamenti, ma **non conta più nel calcolo**: le conseguenze delle minacce a cui è collegato si ricavano dagli altri asset collegati, e una minaccia a cui restano collegati solo asset eliminati usa il valore delle conseguenze indicato a mano, come se non avesse asset. Nelle schede delle minacce l'asset compare barrato, nelle matrici ha un punto al posto del valore. Rimettendolo ONLINE o OFFLINE torna a contare. Un asset **OFFLINE conta come uno ONLINE**: è fuori esercizio, ma i dati che contiene vanno ancora protetti.

> **Cambiare lo stato cambia i rischi**
>
> Mettere un asset a ELIMINATO può abbassare il rischio di alcune minacce. Le revisioni già consolidate non cambiano: conservano i numeri di allora. Conviene consolidare una revisione prima di eliminare asset importanti, per poter confrontare il prima e il dopo.

Schede e griglia

Asset, minacce, controlli e trattamenti si guardano in due modi, con i pulsanti in alto a sinistra (la scelta resta memorizzata nel browser, sezione per sezione):

- **Schede**: una scheda per voce, da aprire con un clic sulla testata.
- **Griglia**: la tabella classica, una riga per voce. Un clic su un'intestazione ordina (per esempio gli asset per valore, le minacce per rischio attuale); un clic su una riga apre la stessa scheda in una **finestra**. Valgono le stesse regole: i campi cambiati restano da salvare finché non si preme Salva nella finestra; chiudendola senza salvare restano in sospeso e la riga lo segnala («da salvare»).

Nella sezione Asset il pulsante **Stampa** apre l'elenco degli asset pronto per la stampa o per il salvataggio in PDF: riporta gli asset che la pagina sta mostrando, quindi con la categoria, lo stato e il testo scelti nei filtri. La stampa riporta i dati salvati: se ci sono modifiche in sospeso, la pagina lo ricorda prima di aprirla. Lo stesso pulsante c'è nelle sezioni **Minacce** e **Controlli**, per l'elenco delle minacce e l'elenco dei controlli mostrati.

Gli asset in CSV: esportare e importare

Nella sezione Asset, il menu **CSV** serve a lavorare l'elenco in un foglio di calcolo e a riportarlo nel registro — per esempio per classificare venti asset in un colpo, o per **riprendere gli asset di un altro registro** già fatto per un'organizzazione simile.

- **Esporta gli asset mostrati (CSV)** scarica un file che il foglio di calcolo apre in colonne: una riga per asset, una colonna per campo (nome, categoria, stato, unità, referente, classificazione, archivi, trattamento, valori R, I, D, note, MTPD e i campi dei dati personali). Valgono i filtri in uso, come per la stampa.
- **Importa asset da un file CSV…** legge un file così fatto e **aggiunge** gli asset nuovi, **aggiorna** quelli che ritrova, e **non elimina niente**: un asset che nel file non c'è resta com'è. Per eliminare un asset si usa il cestino, nella pagina.

Come una riga ritrova il suo asset:

- La prima colonna, **«Rif (non modificare)»**, lega la riga all'asset da cui è stata esportata, **solo dentro lo stesso registro**: riportando il file nel registro da cui è uscito, ogni riga aggiorna il suo asset anche se gli è stato cambiato il nome.
- Una riga senza «Rif», o esportata da un altro registro, è un **asset nuovo** — a meno che nel registro ce ne sia già uno con lo stesso nome. In quel caso si sceglie all'importazione: **lasciarlo com'è** (la scelta proposta: non tocca le valutazioni già fatte) o **aggiornarlo** con i dati del file.
- Gli asset nuovi arrivano in fondo all'elenco, in esercizio (ONLINE), e **non collegati** a nessuna minaccia: i collegamenti non viaggiano nel file.

Che cosa controlla l'importazione: i valori R, I, D vanno da 1 a 4; categoria, classificazione, stato, ruolo, base giuridica (e l'unità organizzativa, se il suo elenco è compilato) devono usare le voci del registro in cui si importa. **Se anche una sola riga non va, non si importa niente**, e la finestra elenca che cosa correggere, con il numero della riga nel file. Una cella vuota svuota il campo dell'asset che si aggiorna (tranne i valori R, I, D, che restano); una colonna tolta dal file lascia quel campo com'è; una colonna con un titolo che il programma non conosce viene ignorata, e l'esito lo dice.

> **Nel foglio di calcolo**
>
> Per salvare, «Salva con nome» e il formato
> **CSV UTF-8 (delimitato dal separatore di elenco)**
> : così le lettere accentate restano giuste. Il programma legge comunque anche il CSV semplice, e i file separati da virgola o da tabulazione. Per preparare un file a mano basta la prima riga con i titoli delle colonne — almeno «Informazioni / asset» — nell'ordine che si vuole.

Come classificare: la guida accanto ai campi

Sotto i menu dei valori (riservatezza, integrità, disponibilità, verosimiglianza, conseguenze a mano) e della categoria compare **che cosa vuol dire il valore scelto**, e cambia cambiando il valore. Il **?** accanto all'etichetta apre a destra la **guida completa**, che resta aperta mentre si compila: le scale con gli esempi, da che cosa ricavare i livelli, le sei

categorie, i fattori della verosimiglianza. Le scale sono quelle del calcolo e non cambiano; i criteri sono un punto di partenza, da adattare alla propria organizzazione e da scrivere nella propria metodologia.

Livello	Riservatezza	Integrità	Disponibilità
1 Basso	Informazione pubblica o a uso interno, senza danni	Errore irrilevante, correggibile subito	Fermo tollerabile oltre 3 giorni lavorativi
2 Medio	Dati aziendali interni, danno limitato	Errore con correzione semplice, nessun effetto sul cliente	Fermo tollerabile fino a 1 giorno lavorativo
3 Alto	Codice sorgente, dati contrattuali, credenziali, dati personali comuni	Errore che altera il funzionamento di un servizio o i dati dei clienti	Fermo di poche ore con effetti sui clienti
4 Critico	Dati particolari o giudiziari, chiavi crittografiche, segreti di produzione	Alterazione che può causare decisioni sbagliate con danno grave	Fermo anche breve che blocca l'attività dei clienti

Categoria	Che cosa comprende	Come si arriva al valore
Informativi	Dati e documenti in qualsiasi formato: archivi, codice sorgente, contratti, registri, credenziali	Direttamente: per contenuto e requisiti di legge. È la categoria da cui parte tutto
Software	Applicativi e strumenti, sviluppati o acquistati	Integrità e disponibilità, e i dati che trattano
Hardware	Dispositivi fisici: server, computer, telefoni, supporti, apparati di rete	Per ereditarietà: il valore più alto fra le informazioni contenute o trattate
Infrastrutture	Ambienti e servizi che ospitano l'attività: cloud, rete, sede, alimentazione, fornitori	Pesa la disponibilità; eredita dai dati ospitati
Human	Persone e competenze, interne ed esterne	Per criticità del ruolo: privilegi, competenze uniche, accesso a dati sensibili
Intangibili	Proprietà intellettuale, marchio, reputazione, certificazioni, licenze	Per impatto sul business

Verosimiglianza	Definizione (su 12 mesi, senza contare i controlli collegati)
1 Bassa	Improbabile: richiede condizioni rare o capacità elevate, non è comune nel settore
2 Media	Plausibile: accade in organizzazioni simili, o almeno una volta in 1-3 anni
3 Alta	Attesa: frequente nel settore, attacco automatizzato, o attività quotidiana in cui l'errore è facile

> **Senza contare i controlli**
>
> Il rischio attuale si ottiene moltiplicando per il fattore del controllo collegato più efficace. La verosimiglianza si dà quindi come se i controlli collegati non ci fossero: tenerne conto qui vorrebbe dire contarli due volte.

Archivi e classificazione: che cosa scrivere

Sono i due campi dell'asset che dicono **dove sta** l'informazione e **come va trattata**. Non entrano nel calcolo del rischio, ma sono quelli che un auditor confronta con la realtà: l'armadio è chiuso davvero? il documento «riservato»

gira per posta in chiaro? Accanto a ciascuno, nella scheda, il **?** apre la stessa spiegazione.

ARCHIVI: DOVE STA L'INFORMAZIONE

Un'informazione non sta «in azienda»: sta in un **contenitore** — un sistema, un supporto, un luogo. Nel campo si scrive il contenitore principale e, se ci sono, le copie: «dove sta, e dove sta la copia». Serve a sapere che cosa proteggere (le minacce colpiscono il contenitore), a dare al contenitore il valore dell'informazione più importante che ospita, e a rispondere a chi chiede dove sono i dati (registro dei trattamenti, richieste degli interessati, incidenti).

Il campo ha un elenco di **proposte** (server in sede, NAS in sede, servizio in cloud, postazioni e portatili, archivio cartaceo, supporti rimovibili, presso un fornitore…): se ne sceglie una e la si completa, oppure si scrive altro.

Informazione / asset	Che cosa scrivere in Archivi
Contabilità e fatturazione	Server in sede (base di dati del gestionale); copia notturna su NAS e copia settimanale fuori sede
Fascicoli del personale	Archivio cartaceo in sede (armadio chiuso, ufficio personale); scansioni in una cartella di rete ad accesso ristretto
Posta elettronica	Servizio in cloud (SaaS); copie locali sulle postazioni
Codice sorgente	Deposito del codice in cloud; copie di lavoro sui portatili degli sviluppatori
Contratti firmati	Archivio cartaceo in sede (originali); gestione documentale in cloud (copie)
Dati dei clienti del servizio	Cloud pubblico (IaaS/PaaS), regione UE; copie di sicurezza nello stesso fornitore, altra zona
Registrazioni della videosorveglianza	Registratore in sede (locale tecnico), sovrascrittura dopo 7 giorni
Paghe	Presso un fornitore (studio paghe); cedolini nella posta dei dipendenti

Che cosa se ne ricava: ogni contenitore nominato qui dovrebbe essere una riga dell'inventario o un asset delle categorie Hardware o Infrastrutture; «cartaceo» porta ai controlli fisici (tema 7), «cloud» al 5.23, «fornitore» ai 5.19-5.22, «supporti rimovibili» al 7.10, le copie all'8.13; un contenitore fuori dallo Spazio economico europeo va detto nel campo del trasferimento extra SEE.

CLASSIFICAZIONE: COME VA TRATTATA

È l'**etichetta** che la politica di classificazione dell'organizzazione dà all'informazione (controlli 5.12 e 5.13). Non è il valore di riservatezza: quello è un numero che serve al calcolo; la classificazione dice a chi usa l'informazione, ogni giorno, **che cosa può farne**. È un campo codificato: si sceglie fra i livelli dell'elenco. I quattro proposti:

Livello	Che cosa ci sta	Regole di trattamento	Riservatezza, di norma
Pubblico	Sito, listini pubblicati, materiale promozionale, bilanci depositati	Nessuna cautela; conta solo che sia corretto	1

Livello	Che cosa ci sta	Regole di trattamento	Riservatezza, di norma
Interno	Procedure, organigramma, rubrica, verbali, comunicazioni al personale	Non si diffonde fuori dall'organizzazione; nessuna misura particolare	1-2
Riservato	Contratti e offerte, dati personali comuni di clienti e dipendenti, codice sorgente, dati contabili	Accesso per ruolo; invio solo con canali protetti; accordo di riservatezza con i terzi; scrivania e schermo puliti	3
Strettamente riservato	Dati particolari (salute) o giudiziari, credenziali e chiavi, piani strategici, segreti industriali	Accesso a persone individuate per nome; cifratura in archivio e in transito; niente supporti rimovibili; accessi registrati; distruzione sicura	4

Casi concreti: l'**anagrafica dei clienti** del gestionale è *Riservato*; le **cartelle sanitarie** e i certificati medici del personale sono *Strettamente riservato*; le **buste paga** sono *Riservato* (*Strettamente riservato* se riportano dati sulla salute o trattenute sindacali); il **manuale della qualità** e le procedure sono *Interno*; l'**archivio delle password** degli amministratori è *Strettamente riservato*; il **catalogo** pubblicato è *Pubblico*; le **copie di backup** prendono la classificazione più alta fra le informazioni che contengono.

> **Classificazione e riservatezza devono andare d'accordo**
>
> Un asset «Strettamente riservato» con riservatezza 2 è la prima incoerenza che un auditor nota: o è sbagliata l'etichetta, o il valore. I nomi dei livelli contano meno delle regole di trattamento, che vanno scritte nella politica di classificazione; tre o quattro livelli bastano.

Passo 2 — Minacce e rischio

Le minacce si aggiungono dal **catalogo ISO/IEC 27005** (42 minacce raggruppate per categoria, con l'origine D · A · E — Deliberata, Accidentale, Ambientale — e valori proposti) oppure si creano personalizzate.

Il pulsante **Dal catalogo ISO/IEC 27005…** apre l'elenco completo, per gruppo, con una casella accanto a ogni minaccia: si spuntano quelle che servono — una, un gruppo intero con la casella del gruppo, o tutte con «Seleziona tutte» — e «Aggiungi» le inserisce **in blocco**, in cima all'elenco e nell'ordine del catalogo. Chi comincia un registro può così aggiungerle tutte e poi eliminare quelle che non lo riguardano (un fenomeno vulcanico, per chi non ha vulcani vicino), oppure spuntare solo quelle che gli servono. La casella di ricerca restringe l'elenco, e «Seleziona tutte» vale allora per le voci trovate.

> **Niente doppioni**
>
> Le minacce che il registro ha già sono segnate «già nel registro» e non si possono spuntare: una minaccia del catalogo non entra due volte. Il confronto è sul nome, senza badare a maiuscole e spazi: una minaccia a cui è stato cambiato il nome non viene più riconosciuta come quella del catalogo, e si può aggiungere di nuovo.

Le minacce in CSV: esportare e importare

Anche la sezione Minacce ha il menu **CSV**, e funziona come quello degli asset: «Esporta le minacce mostrate (CSV)» scarica un file per il foglio di calcolo, «Importa minacce da un file CSV…» **aggiunge** le minacce nuove, **aggiorna** quelle che ritrova e **non elimina niente**. Valgono le stesse regole: la colonna «Rif» ritrova la minaccia dentro lo stesso registro anche se le è stato cambiato il nome; una riga senza «Rif» o di un altro registro è una minaccia nuova, salvo che ce ne sia già una con lo stesso nome (e allora si sceglie se lasciarla o aggiornarla); se una riga non va non si importa niente.

- Le colonne che si rileggono: nome, ambito, categoria (le voci del registro), verosimiglianza (1-3), parametri toccati (le lettere R, I, D), conseguenze a mano (1-4), note. Una minaccia nuova senza verosimiglianza nasce con 2.
- I **collegamenti viaggiano**: i controlli per codice (il catalogo è lo stesso in ogni registro), scritti fra parentesi quadre («[07.05] [08.24]») perché il foglio di calcolo non scambi un codice per una data; gli asset per nome, separati da « | ». All'importazione quelli scritti nel file vengono **aggiunti** a quelli che la minaccia ha già; **non se ne toglie nessuno**, nemmeno svuotando la cella. Un asset o un controllo che nel registro non c'è non ferma l'importazione: il collegamento non si fa, e l'esito dice quali.
- Le colonne dei **numeri calcolati** — conseguenze, rischio puro, inerente, attuale, fascia, residuo atteso — escono per chi vuole ordinare e filtrare nel foglio di calcolo, e all'importazione non contano: i numeri li calcola sempre il programma.

> **Portare un registro in un altro**
>
> Per riprendere il lavoro fatto per un'organizzazione simile: nel registro nuovo si importano **prima gli asset** e **poi le minacce**. Così le minacce ritrovano per nome gli asset a cui erano collegate, e arrivano già con i loro controlli. Applicabilità e valutazioni dei controlli si portano con il CSV dei controlli. I trattamenti e le risposte alla checklist non viaggiano nei CSV: per portare tutto il registro c'è l'esportazione in XML.

Per ogni minaccia:

- **Verosimiglianza**: 1 Bassa, 2 Media, 3 Alta.
- **Parametri coinvolti**: quali fra riservatezza, integrità e disponibilità la minaccia compromette.
- **Asset collegati**: gli asset esposti alla minaccia. Senza asset collegati, le conseguenze si indicano a mano (da 1 a 4).
- **Controlli collegati**: i controlli che proteggono da quella minaccia.

Sotto la scheda si leggono conseguenze, rischio puro, inerente e attuale. Anche le minacce si guardano a schede o in griglia, e accanto a verosimiglianza e conseguenze c'è la guida.

Le matrici dei collegamenti

Nella sezione Minacce, i pulsanti **Minacce × asset** e **Controlli × minacce** mostrano i collegamenti tutti insieme. Una casella piena è un collegamento; **un clic su una casella collega o scollega**, e il collegamento si salva subito, come nelle schede.

- Accanto al nome di ogni minaccia (o sotto, dove le minacce sono sulle colonne) stanno le sue **conseguenze** (C) e il **rischio attuale**: cambiano mentre si collega, e l'effetto di ogni casella si legge subito.
- **Minacce × asset**: le **minacce sulle righe**, con la descrizione per intero, e gli **asset sulle colonne**, nell'ordine delle categorie (sotto il nome i valori R·I·D e la categoria). Nella casella c'è il valore dell'asset per i parametri che la minaccia tocca; l'asset che determina le conseguenze ha il bordo marcato. L'ultima colonna conta quanti asset sono collegati alla minaccia; l'ultima riga a quante minacce è collegato ogni asset.
- **Controlli × minacce**: nella casella c'è la valutazione del controllo (da 1 a 4; «?» se non è valutato, e allora vale come il peggiore); il controllo più efficace, che determina il rischio attuale, ha il bordo marcato. Si sceglie il tema e quali controlli mostrare: applicabili o collegati, solo collegati, tutti quelli del tema.
- I filtri delle minacce (categoria, testo) scelgono quali minacce compaiono: le righe nella prima matrice, le colonne nella seconda. La prima riga e la prima colonna restano ferme scorrendo.

La terza matrice, **Controlli × asset**, **si legge soltanto**. Un controllo non si collega a un asset ma a una minaccia, e la minaccia agli asset: un controllo protegge quindi un asset **attraverso le minacce che hanno in comune**. Nella casella c'è quante sono, col colore della valutazione del controllo; un clic le elenca, con il loro rischio attuale, e da lì si apre la minaccia. Sotto il nome di ogni asset stanno i suoi valori R · I · D e il rischio attuale più alto fra le minacce a cui è esposto. Risponde a due domande che le altre matrici mostrano solo a pezzi: da quali controlli è protetto un asset (una colonna vuota o quasi è un asset scoperto), e quali asset dipendono da un controllo (la riga).

Come si calcola il rischio

Valore	Come si ottiene	Scala
Conseguenze	Il valore più alto fra gli asset collegati, guardando solo i parametri (R, I, D) che la minaccia tocca. Gli asset in stato ELIMINATO non contano. Senza asset che contano: il valore indicato a mano (1 se manca).	1–4
Rischio puro	Verosimiglianza × Conseguenze	1–12
Fattore di un controllo	5 − valutazione (Adeguato = 1, Inadeguato = 4). Un controllo non valutato vale 4.	1–4
Rischio inerente	Rischio puro × 4: come se non ci fosse nessun controllo	4–48
Rischio attuale	Rischio puro × il fattore più basso fra i controlli collegati, cioè quello del controllo più efficace. Senza controlli collegati, × 4.	1–48

> **Esempio**
>
> Incendio, verosimiglianza 2, tocca integrità e disponibilità; l'asset collegato ha R 4, I 1, D 3. Le conseguenze sono 3 (la riservatezza non conta: l'incendio non la tocca), il rischio puro 6, l'inerente 24 (Medio). Collegando il controllo 07.05 valutato «Quasi adeguato» (fattore 2) l'attuale scende a 12 (Basso).

Il metodo è volutamente semplificato: ogni minaccia è valutata rispetto ai soli controlli collegati, non all'insieme dei controlli. I valori servono a stabilire priorità di trattamento confrontabili fra loro.

PERCHÉ VALE IL CONTROLLO PIÙ EFFICACE

Quando a una minaccia sono collegati più controlli, il rischio attuale lo decide il **più efficace**: è il metodo del foglio di calcolo da cui il programma nasce, ripreso senza cambiarlo perché i registri fatti con il foglio diano gli stessi numeri. I controlli collegati a una minaccia si considerano **alternativi**: ognuno, da solo, è in grado di ridurre quel rischio, e il rischio scende fino a dove arriva il migliore. Nella scheda della minaccia e nelle matrici il controllo che decide è segnato col bordo marcato. Il metodo ha tre pregi:

- **è semplice e si spiega in audit**: «il rischio è 8 perché il controllo 8.7 è adeguato»;
- **non si gonfia**: aggiungere controlli deboli non abbassa il rischio, se ce n'è già uno forte;
- **non si azzera**: anche con un controllo adeguato il rischio attuale resta uguale al rischio puro (fattore 1).

E un limite: **non premia la difesa in profondità**. Tre controlli «Quasi adeguati» danno lo stesso rischio di uno solo, anche se insieme proteggono di più. C'è poi un effetto pratico da tenere presente: un controllo forte collegato a una minaccia che copre solo in parte **fa crollare il rischio**. Se all'incendio di una sala server si collegano anche il backup e la ridondanza dei server, valutati «Adeguato», il rischio risulta basso; ma il backup non evita l'incendio, ne limita soltanto il danno ai dati. Collegando solo la protezione fisica della sala, valutata «Parzialmente adeguato», il rischio torna medio, che è la misura giusta.

> **La regola pratica per chi compila**
>
> Collegare a una minaccia solo i controlli che la riducono davvero e in modo diretto, non quelli che la toccano di lato.

Passo 3 — Controlli e SoA

La sezione elenca i **93 controlli dell'Appendice A** della ISO/IEC 27001:2022 (organizzativi 5, persone 6, fisici 7, tecnologici 8; alcuni sono divisi in sottovoci, quindi le righe sono 119). Sono quelli della Dichiarazione di Applicabilità e della certificazione.

Le estensioni servono solo a chi le usa e di norma non si vedono: **cloud** (ISO/IEC 27017 e 27018, per chi fornisce servizi cloud) e **privacy** (ISO/IEC 27701, titolare e responsabile del trattamento). Si accendono nelle Impostazioni, scheda «Catalogo dei controlli», e da quel momento compaiono fra i temi, nella SoA e nelle stampe. Spegnerle non cancella niente: un controllo già valutato o collegato a una minaccia resta visibile. Le clausole del sistema di gestione (punti 4–10) non sono fra i controlli: quei requisiti li seguono la mappa della norma e i registri del sistema di gestione.

Si lavora **un tema alla volta**: in alto i pulsanti dei temi (5 Organizzativi, 6 Persone, 7 Fisici, 8 Tecnologici, poi le estensioni accese) mostrano quanti controlli di ciascuno sono valutati; «Tutti» li elenca insieme. La ricerca per codice o nome cerca in tutti i temi. Si filtra anche per stato (non valutati, collegati a minacce, applicabilità da decidere, applicabili, esclusi).

I punti di vista degli attributi. La ISO/IEC 27002 classifica ogni controllo con cinque tipi di attributo, e una seconda riga della barra ha un menu per ciascuno: **tipo di controllo** (#Preventive, #Detective, #Corrective), **proprietà di sicurezza** (#Confidentiality, #Integrity, #Availability), **concetti di cybersecurity** (#Identify, #Protect, #Detect, #Respond, #Recover), **capacità operative** (gestione degli asset, continuità, sicurezza fisica…) e **domini di sicurezza** (#Governance and Ecosystem, #Protection, #Defence, #Resilience). Scegliendo un valore si vedono i controlli che lo hanno, **in tutti i temi**: per esempio #Resilience mostra i controlli che servono a reggere un'interruzione, e aggiungendo #Corrective solo quelli che agiscono dopo. I menu si combinano fra loro e con lo stato; «Togli i filtri», o un clic su un tema, torna all'elenco per tema. La stampa dell'elenco e il CSV riportano i controlli scelti, e la stampa dice con quali attributi. I controlli delle estensioni (cloud, privacy) non hanno attributi e non compaiono quando un attributo è scelto.

Anche i controlli si guardano a **schede** o in griglia: la griglia è la Dichiarazione di Applicabilità come tabella (codice, controllo, applicabilità, stato, valutazione, attuazione secondo la checklist, minacce collegate, responsabile, ultima verifica), nell'ordine della norma finché non si ordina per una colonna. Un clic su una riga apre in una finestra la scheda del controllo, con la sua checklist.

Per ogni controllo:

- **Applicabile (SoA)**: sì o no, con la **giustificazione** dell'inclusione o dell'esclusione. È il contenuto della Dichiarazione di Applicabilità.
- **Stato di attuazione** (non attuato, pianificato, parzialmente attuato, attuato) e data dell'ultima verifica.
- **Valutazione**: da 1 Inadeguato a 4 Adeguato. È questa che entra nel calcolo del rischio delle minacce collegate.
- Come è attuato, carenze, documenti, requisiti cogenti e contrattuali, responsabile.

In cima alla scheda c'è sempre la guida ISO/IEC 27002 al controllo, che aiuta a valutarlo; sotto, i campi. La checklist di verifica sta in fondo, in un riquadro **Approfondisci** chiuso: si apre con un clic e resta aperta finché si lavora, e si apre da sola quando ha già delle risposte.

La checklist di verifica

Per i controlli dell'Annex A la scheda contiene la **checklist ISO/IEC 27002:2022** del controllo: una breve descrizione, uno spunto pratico e le domande di verifica. A ogni domanda si risponde con:

- **C** Conforme (2 punti), **P** Parziale (1 punto), **NC** Non conforme (0 punti), **N/A** Non applicabile (esclusa dal calcolo),

annotando evidenze e azioni correttive. Il programma calcola la percentuale di attuazione e **propone** una valutazione: dal 90% Adeguato, dal 60% Quasi adeguato, dal 30% Parzialmente adeguato, sotto Inadeguato. Il pulsante «Usa la valutazione proposta» la copia nel campo Valutazione (da confermare con Salva); resta una proposta, che chi valuta può cambiare. La proposta si calcola sulle risposte salvate: se ce ne sono in sospeso, il programma chiede di salvarle prima.

La checklist nelle revisioni. Le risposte fanno parte della valutazione e si conservano in ogni revisione consolidata. Quando c'è una revisione, la scheda riporta sopra le domande l'attuazione di allora («Revisione 1.0 del …: 5 risposte, attuazione 20%») e sotto ogni domanda la risposta data allora, con esito, evidenze e note; se è diversa da quella attuale è segnata con ≠. Il pulsante **Riprendi le risposte della revisione** le ricopia nei campi, come punto di partenza della rivalutazione: restano da confermare con Salva, e se un campo ha già una risposta diversa il programma chiede prima di sostituirla. Nella testata del controllo, accanto all'attuazione attuale, compare quella della revisione.

Alcuni controlli dell'Annex A sono divisi in sottovoci (per esempio 05.01.01 e 05.01.02) che rimandano alla stessa scheda della checklist: le risposte sono comuni.

La guida ISO/IEC 27002 ai controlli

Prima di valutare un controllo bisogna sapere che cosa chiede. Per questo la scheda di ogni controllo che viene dalla ISO/IEC 27002 si apre con un riquadro che riporta, dalla norma:

- **il controllo**, cioè l'enunciato: che cosa l'organizzazione dovrebbe fare;
- **lo scopo**: perché lo fa, quale rischio vuole ridurre. È la domanda a cui la valutazione risponde: il controllo, come è attuato, raggiunge questo scopo?
- **gli attributi**, le etichette con cui la norma classifica ogni controllo (#Preventive, #Protect, #Continuity…); passando sopra un'etichetta se ne legge il significato.

Il pulsante **Come si legge questo controllo** apre a destra la guida intera, che resta aperta accanto alla scheda mentre si compila: enunciato e scopo, gli attributi spiegati uno per uno, la **guida** della norma (che cosa considerare per attuarlo, con i suoi elenchi), le **altre informazioni** e **dove si documenta in CyberSic**. I rimandi fra i controlli («vedere 5.30») sono collegamenti: un clic apre la guida di quel controllo, e la freccia in alto torna a quella di prima. «Nel registro» elenca le voci del catalogo che corrispondono a quel controllo: alcuni controlli della norma sono divisi in più voci (05.15.01, 05.15.02…), che hanno la stessa guida. Da lì si apre anche la pagina «Che cosa vogliono dire tutti gli attributi», con i cinque tipi e tutti i loro valori.

Come usarla per compilare:

- la **giustificazione** dell'inclusione o dell'esclusione si scrive rispetto allo scopo: un controllo si esclude quando il rischio che lo scopo descrive, per questa organizzazione, non c'è o è trattato in altro modo;
- «**come è attuato**» e le **carenze** si confrontano con le voci della guida: quelle che servono e mancano sono le carenze;
- la guida usa «dovrebbe»: sono raccomandazioni, non obblighi. Si attua quello che serve a trattare i rischi del registro;
- la checklist di verifica traduce la guida in domande a cui rispondere con le evidenze.

Dove si documenta. La guida intera si chiude con l'indicazione di dove si tengono, in CyberSic, le evidenze del controllo: per esempio, per le copie di sicurezza (8.13), l'adempimento periodico con le sue esecuzioni e le prove di

ripristino, i tempi di ripristino nella Continuità operativa, un indicatore per le prove riuscite. Questa parte è scritta per CyberSic, non viene dalla norma.

Il riquadro e la guida intera si vedono sempre, nelle schede e nella finestra della griglia, anche nella versione di prova. I controlli delle estensioni (cloud, privacy) non vengono dalla 27002 e non hanno questo riquadro.

I controlli in CSV: esportare e importare

Anche la sezione Controlli ha il menu **CSV**. «Esporta i controlli mostrati (CSV)» scarica un file per il foglio di calcolo con una riga per controllo — quelli del tema e dei filtri in uso — e quello che il registro dice di ciascuno: applicabilità, giustificazione, stato di attuazione, valutazione, responsabile, data dell'ultima verifica, come è attuato, carenze, documenti, requisiti cogenti e contrattuali. «Importa controlli da un file CSV…» riporta nel registro questi valori: serve a compilare la Dichiarazione di Applicabilità in un foglio di calcolo, o a **riprendere quella già fatta per un'organizzazione simile**.

- I controlli sono quelli del catalogo, uguali in ogni registro: l'importazione **aggiorna**, non aggiunge e non toglie. Ogni riga si riconosce dal **codice** con cui comincia la colonna «Controllo» («08.13.01 Backup delle informazioni»): va lasciata com'è. Un file con solo alcune righe aggiorna solo quei controlli.
- **Celle vuote**: di norma **non toccano il campo** — resta quello che il registro ha già, e si scrivono solo i valori che il file porta. È la scelta prudente quando il file viene da un altro registro. In alternativa si può chiedere che le celle vuote **svuotino** il campo: allora il file vale per intero, e una valutazione vuota cancella quella che c'è.
- Applicabile si scrive «Sì» o «No»; la valutazione va da 1 a 4; lo stato deve essere una delle voci del registro; la data si può scrivere come la scrive il foglio di calcolo (15/09/2026). Se una riga non va — un valore fuori scala, un codice che non esiste, un controllo ripetuto — **non si importa niente** e la finestra dice che cosa correggere.
- Le colonne «Tema», «Checklist (%)» e «Minacce collegate» servono a chi lavora nel foglio di calcolo e non si rileggono. Le risposte alla checklist e i collegamenti alle minacce non viaggiano in questo file (i collegamenti viaggiano con le minacce).

> **La valutazione cambia il rischio**
>
> Importare le valutazioni dei controlli ricalcola il rischio attuale di tutte le minacce a cui sono collegati. Conviene consolidare una revisione prima, per poter confrontare il prima e il dopo.

Passo 4 — Trattamento

Le minacce compaiono in ordine di rischio attuale decrescente; di norma solo quelle a rischio Medio o Alto e quelle con un trattamento già impostato (la casella in alto mostra anche le altre). Come le altre sezioni, si guardano a **schede** o in **griglia** (Schede e griglia): la griglia è il piano di trattamento in una tabella, con rischio attuale e residuo atteso, opzione, stato, responsabile, scadenza (in rosso se passata e non completata), proprietario, accettazione e quanti obiettivi sono collegati; un clic su una riga apre la scheda del trattamento in una finestra. Per ciascuna:

- **Opzione** (ISO/IEC 27005): mitigare, accettare, trasferire, evitare.
- **Proprietario del rischio**, analisi, azioni, responsabile delle azioni, scadenza, stato (da avviare, pianificato, in corso, completato).
- **Simulazione**: scelto uno dei controlli collegati e il valore che si prevede di raggiungere, il programma calcola il **rischio residuo atteso**.
- **Accettazione del rischio residuo** da parte del proprietario, con la data.

Le azioni con una scadenza passata e non completate risultano «scadute» nel cruscotto.

Da dove vengono i trattamenti

I trattamenti **non si aggiungono e non si scelgono**: ce n'è uno per ogni minaccia, perché il trattamento è la risposta a quel rischio e non una riga a sé. Per questo nella sezione non c'è un pulsante «Nuovo».

- **Che cosa compare.** Una minaccia è nell'elenco se il suo rischio attuale è in fascia **Media o Alta** (le fasce vengono dalle due soglie dei criteri, nella sezione Organizzazione), oppure se ha **già un trattamento compilato**, anche quando nel frattempo il rischio è sceso a Basso. La casella «Mostra anche i rischi bassi senza trattamento» le mostra tutte.
- **L'elenco cambia da solo.** Quando una valutazione cambia — un asset più critico, un controllo valutato peggio — una minaccia che passa da Basso a Medio entra nell'elenco con la scritta «da decidere», e il cruscotto la conta fra i rischi senza decisione.
- **Perché è legato alla minaccia.** Il rischio residuo atteso si calcola simulando un valore migliore per uno dei controlli collegati a quella minaccia, e l'accettazione del residuo da parte del proprietario riguarda un rischio preciso. È anche quello che chiede la norma: il piano di trattamento (ISO/IEC 27001, 6.1.3) risponde ai rischi valutati.

Come si procede. Si parte dall'alto, dai rischi più alti: si sceglie l'opzione, si scrivono analisi e azioni con responsabile e scadenza, si simula il controllo su cui si interviene per vedere dove arriva il residuo, e si registra l'accettazione del proprietario. Se la simulazione non offre controlli, la minaccia non ne ha di collegati: si collegano nella sezione Minacce.

Un trattamento che non nasce da un rischio valutato

Per un'azione estemporanea — un adeguamento chiesto da un cliente, un miglioramento deciso nel riesame — basta

aggiungere a monte una minaccia

che dica di che cosa si tratta (sezione Minacce, pulsante «Minaccia personalizzata»), senza asset collegati e con verosimiglianza e conseguenze al minimo. Risulta un rischio Basso: nella sezione Trattamento si spunta «Mostra anche i rischi bassi senza trattamento», la si apre e si compilano opzione, azioni, responsabile e scadenza. Da quel momento ha un trattamento e

resta nell'elenco

anche senza la casella, compare nel piano di trattamento e nelle scadenze del cruscotto. La minaccia aggiunta fa parte del registro dei rischi a tutti gli effetti: conviene darle un nome che la faccia riconoscere.
In alternativa, un'attività che non si vuole nel registro dei rischi si scrive nel registro Obiettivi e attività, dove il collegamento a una minaccia è facoltativo.

Revisioni e rivalutazione

Si lavora sempre sulla **bozza**. Quando il registro è approvato — riesame della direzione, audit, fine di un ciclo di trattamento — lo si **consolida** in una revisione (numero proposto 1.0, 1.1…, autore, nota). La revisione conserva il registro intero com'era in quel momento, con i rischi calcolati, e non si modifica più. Se ne scarica l'istantanea in XML.

Rivaluta confronta una revisione con la bozza: per ogni minaccia il rischio di allora e quello di adesso, la variazione e il trattamento. Si vede così l'effetto delle azioni fatte, e quali rischi sono aumentati. Sotto, lo stesso confronto per la **checklist**: per ogni scheda con risposte, l'attuazione nella revisione e adesso, la variazione e quanti esiti sono cambiati.

> **Importazione e revisioni**
>
> Importare un registro sostituisce il contenuto della bozza e rinumera le minacce: le revisioni precedenti restano, ma il confronto con loro minaccia per minaccia non è più significativo.

Sistema di gestione: i registri

Accanto alla valutazione e al trattamento del rischio, un sistema di gestione ISO/IEC 27001 si regge su alcuni registri che un auditor chiede uno per uno. La sezione **Sistema** li tiene in quest'ordine: Documentazione di sistema, Procedure e revisioni, **Audit**, **Registri**, Obiettivi e attività, **Indicatori**. Tre pulsanti, con la freccia, sono **gruppi**: un clic apre la prima voce e sotto compare una seconda riga, più piccola, con le voci del gruppo:

- **Audit**: il registro degli audit interni ed esterni, la checklist di audit, le checklist personalizzate e la copertura degli audit;
- **Registri**: registro degli incidenti, inventario hardware e software, formazione, riesame della direzione;
- **Indicatori**: gli indicatori e, meno in evidenza, tutte le misurazioni insieme. Le misurazioni di un indicatore si scrivono nella sua finestra; l'elenco di tutte serve per le ricerche su tutti gli indicatori, per esempio per vedere chi ha rilevato che cosa e se qualche misurazione manca.

Il numero accanto al nome è quante righe ha il registro (per un gruppo, i suoi registri principali), e in rosso quante hanno una data passata.

Registro	Che cosa contiene	Riferimento
Documentazione di sistema	Politiche, manuali, procedure, moduli, registri, piani, documenti esterni: codice, versione, stato, responsabile, dove si trova, prossima revisione	7.5
Procedure e revisioni	Una riga per ogni revisione di una procedura: che cosa è cambiato, chi l'ha redatta, verificata e approvata; la revisione in vigore è una, le precedenti restano come «Superata»	7.5.2, 7.5.3
Audit interni ed esterni	Programma ed esiti: tipo (interno, di seconda o di terza parte, di sorveglianza), ambito, auditor, la checklist da usare, non conformità maggiori e minori, osservazioni, azioni correttive con responsabile e scadenza, verifica dell'efficacia	9.2
Checklist personalizzate	Le domande delle checklist scritte nel registro, una riga per domanda, raggruppate dal nome della checklist (Le checklist personalizzate)	9.2
Registro degli incidenti	Eventi, quasi incidenti, incidenti e violazioni di dati personali: gravità, cause, azioni immediate e correttive, notifica al Garante, che cosa si è imparato	controlli 5.24–5.28, 6.8
Inventario hardware e software	I beni uno per uno: tipo, codice, marca e modello, assegnatario, ubicazione, scadenza di garanzia o licenza, stato, dismissione	controllo 5.9
Obiettivi e attività	Obiettivi per la sicurezza e attività per raggiungerli: risorse, responsabile, scadenza, avanzamento, indicatore, valutazione dei risultati	6.2
Indicatori	Le misure dell'efficacia di controlli e trattamenti: che cosa si misura e come, obiettivo dell'azienda, soglia di allarme, riferimento statistico; con l'esito dell'ultima misurazione, la tabella e il grafico (Gli indicatori)	9.1; ISO/IEC 27004
Misurazioni	I valori rilevati per gli indicatori, una riga per misurazione: di solito si scrivono dalla finestra dell'indicatore, qui si vedono tutte insieme e si caricano in blocco col CSV	9.1
Formazione	Piano e registro di formazione e sensibilizzazione: argomento, destinatari, partecipanti, docente, verifica dell'efficacia, evidenze	7.2, 7.3

Registro	Che cosa contiene	Riferimento
Riesame della direzione	Un riesame per riga, con gli elementi in ingresso e in uscita che la norma elenca: compilato per intero, è il verbale; gli elementi in ingresso si raccolgono dai registri (Il fascicolo per il riesame)	9.3

Nel gruppo Audit ci sono anche due pagine che non sono registri: la checklist di audit e la copertura degli audit.

Ogni registro è una griglia: un clic su un'intestazione ordina, un clic su una riga apre la scheda in una finestra, e le modifiche si confermano con Salva come nel resto del programma. In alto si cerca nel registro, si filtra per stato, e — dove il registro ha una data da tenere d'occhio (prossima revisione, scadenza delle azioni, scadenza di una licenza) — si mostrano solo le righe con la **data passata**, che in griglia è in rosso finché la riga non è chiusa. **Stampa** apre il registro pronto per la stampa: le colonne della griglia e, sotto ogni riga, gli altri campi compilati; per gli indicatori, in più, esito, grafico e tabella delle misurazioni di ciascuno.

Collegamenti con il registro dei rischi. Sono facoltativi e non entrano nel calcolo:

- un **obiettivo** si può collegare al rischio che tratta. Nella scheda del trattamento (Passo 4) compaiono gli obiettivi collegati, e il pulsante **Crea un obiettivo da questo trattamento** ne prepara uno con le azioni, il responsabile e la scadenza decisi nel trattamento: da lì in poi lo si segue nel registro, con avanzamento e valutazione dei risultati;
- un bene dell'**inventario** si può collegare all'asset di cui fa parte (il registro dei rischi ragiona per insiemi, «portatili e postazioni»; l'inventario li elenca uno per uno);
- un **incidente** si può collegare all'asset colpito e alla minaccia che si è verificata;
- un **indicatore** si collega ai controlli di cui misura l'efficacia e al rischio di cui misura il trattamento: compare nelle loro schede, con l'esito dell'ultima misurazione (Gli indicatori).

Se l'asset o la minaccia viene eliminato, la riga del registro resta e il collegamento si svuota.

I registri fanno parte del registro dell'organizzazione: entrano nelle revisioni consolidate e nell'esportazione. Importando un file che non li contiene (per esempio dal foglio di calcolo) i registri già compilati restano, ma perdono i collegamenti ad asset e minacce, che l'importazione rinumera.

Gli indicatori

Un controllo valutato «Adeguato» e un trattamento «Completato» dicono che una misura è stata messa in campo, non che funziona. Gli **indicatori** servono a questo: raccolgono, a intervalli regolari, un numero che misura una situazione — le prove di ripristino riuscite, i clic sui messaggi di phishing simulati, le ore di fermo del servizio — e lo confrontano con quello che l'azienda si è data come obiettivo e con un dato statistico esterno. È quello che la ISO/IEC 27001 chiede al punto 9.1 (monitoraggio, misurazione, analisi e valutazione); la ISO/IEC 27004 ne è la guida.

La scheda dell'indicatore (registro «Indicatori», «Nuovo: indicatore»):

- **Che cosa misura e perché**, il **tipo** (efficacia di un controllo, attuazione, esito, processo del sistema di gestione), la **formula** o il metodo, l'**unità di misura** (%, n., ore…), la **frequenza**, da dove si prendono i dati e chi misura.
- L'**andamento desiderato**: «Più alto è meglio» (ripristini riusciti) o «Più basso è meglio» (clic sul phishing, ore di fermo). Decide come si legge ogni confronto; l'elenco non si può ridurre, perché il programma lo usa nei suoi conti.
- I tre valori di confronto: l'**obiettivo dell'azienda** (il valore atteso), la **soglia di allarme** (oltre la quale la situazione è da affrontare subito) e il **riferimento statistico**, con la sua fonte: un dato di settore, un rapporto pubblico, la media di un gruppo di aziende. Si scrivono con la virgola, come 99,5.

- I **controlli** di cui misura l'efficacia, per codice («8.13 5.24»: un controllo che il catalogo divide in parti, come 8.13, vale per tutte le sue parti), e il **rischio** di cui misura il trattamento. Lì l'indicatore compare, nella scheda del controllo e in quella del trattamento.
- La **prossima misurazione**: passata, la riga va in rosso come le altre scadenze.
- I **dati di base**, per gli indicatori che sono un rapporto: **che cosa si conta** (i portatili cifrati, le persone formate) e **su che cosa**, la base, che è un dato dell'azienda (i portatili in uso, le persone che trattano quei dati). I due nomi diventano i titoli delle colonne nella tabella delle misurazioni.

Conteggio e base: in una misurazione che li porta tutti e due il valore **lo calcola il programma**, al salvataggio: conteggio diviso base, per cento se l'unità dell'indicatore è «%» (2 portatili cifrati su 6 = 33,33%), altrimenti il rapporto e basta (30 ore di fermo su 4 fermi = 7,5 ore in media). In quella riga il valore non si scrive a mano. Una misurazione nuova riprende la base dell'ultima, perché un dato come il numero dei dipendenti cambia di rado: se è cambiato, si corregge. La base deve essere più di zero e il conteggio non può essere negativo. Chi non ha i dati di base scrive direttamente il valore, come prima. Se si cambia l'unità dell'indicatore (da «%» ad altro, o viceversa), i valori calcolati si rifanno.

Le misurazioni si scrivono nella finestra dell'indicatore: «Aggiungi una misurazione» apre una riga nella tabella con la data di oggi; si scrivono il periodo («3° trim. 2026»), il valore, chi l'ha rilevato e un commento, e si conferma con Salva insieme al resto della scheda. Se per un periodo l'obiettivo o il riferimento erano diversi (un obiettivo alzato dal riesame, il dato statistico dell'anno), si scrivono nella riga: valgono per quel periodo, e nel grafico la linea fa un gradino. Vuoti, valgono quelli dell'indicatore. Molte misurazioni insieme — una serie tenuta finora in un foglio di calcolo — si caricano dal registro «Misurazioni» con il menu CSV, scrivendo l'indicatore col suo nome o col suo codice.

L'esito si calcola sull'ultima misurazione che ha un valore:

Esito	Quando
In obiettivo	il valore raggiunge l'obiettivo, nel verso desiderato
Da migliorare	non lo raggiunge, ma non ha passato la soglia di allarme (o la soglia non c'è)
Fuori soglia	non raggiunge l'obiettivo e ha passato la soglia di allarme
Senza obiettivo	l'obiettivo non è stato scritto: l'indicatore si misura, ma non si giudica
Nessuna misurazione	non ci sono ancora valori

Accanto all'esito il programma dice se il valore è migliore o peggiore del **riferimento statistico** e se è in miglioramento o in peggioramento rispetto alla **misurazione precedente**. Il **grafico** mette in fila le misurazioni (sono periodi, a distanza uguale) con le linee dell'obiettivo, del riferimento e della soglia, ciascuna col suo tratto e la sua etichetta; passando sopra un punto se ne legge il valore. La **tabella** sotto il grafico è la stessa serie in numeri.

Dove si vedono: nella griglia del registro (ultimo valore, un piccolo grafico dell'andamento, l'esito), nella scheda dei controlli e dei trattamenti collegati, nel **Riepilogo** (quanti indicatori in obiettivo, da migliorare, fuori soglia, e quali), e nella **stampa** del registro, che dopo l'elenco riporta per ogni indicatore esito, grafico e tabella.

> **L'esito non cambia il rischio**
>
> Un indicatore fuori soglia non abbassa da solo la valutazione dei controlli collegati: il calcolo del rischio resta quello del metodo. È un'informazione per chi valuta — un buon motivo per rivedere la valutazione del controllo, o per riaprire il trattamento — e un elemento del riesame della direzione, che deve considerare i risultati di monitoraggio e misurazione (9.3.2).

> **Il riferimento statistico**
>
> Va scritta la fonte, con l'anno: un dato senza fonte non si può difendere davanti a un auditor. Nei registri di esempio i riferimenti sono valori d'esempio, e lo dicono.

Eliminando un indicatore si eliminano anche le sue misurazioni; il programma lo chiede prima.

I registri in CSV: esportare e importare

Tutti i registri hanno il menu **CSV**, come asset, minacce e controlli: un registro si compila più in fretta in un foglio di calcolo, e spesso esiste già — un elenco dei computer, l'elenco dei documenti, il registro della formazione tenuto finora in un foglio. Le regole sono le stesse per tutti; qui sono dette con l'esempio dell'inventario, e la tabella in fondo dice che cosa cambia da un registro all'altro.

- **Esporta le righe del registro (CSV)** scarica tutte le righe del registro aperto, una colonna per campo.
- **Importa righe da un file CSV… aggiunge** le righe nuove, **aggiorna** quelle che ritrova e **non elimina niente**: una riga che nel file non c'è resta com'è, con i suoi allegati.
- Un file esportato da questo registro ritrova le sue righe dalla colonna «Rif (non modificare)», anche se sono state cambiate.
- Una riga senza «Rif», o di un altro registro, è una riga nuova, a meno che nell'inventario ce ne sia già una **uguale**: stesso codice, stessa descrizione e stesso numero di serie. In quel caso si sceglie se lasciarla com'è (la scelta proposta) o aggiornarla. Le righe uguali fra loro **si contano**: otto portatili identici, senza codice né numero di serie, restano otto; e ricaricare due volte lo stesso file non li raddoppia.
- Per un file preparato a mano basta la colonna «Descrizione»; le altre sono facoltative, in qualunque ordine, con i titoli dei campi della scheda (Tipo, Codice / etichetta, Marca / produttore, Modello / versione, Quantità, Assegnato a, Ubicazione, Stato…). Una colonna con un titolo che il programma non conosce viene ignorata, e l'esito lo dice.
- Tipo e stato devono usare le voci del registro; le date si scrivono come 31/12/2026; «Dati cifrati» come «Sì» o «No». Se una riga non va, **non si importa niente** e la finestra dice che cosa correggere.
- L'**asset** del registro dei rischi di cui il bene fa parte si scrive con il suo **nome**: se nel registro non c'è, l'importazione prosegue, il collegamento non si fa e l'esito lo elenca. Gli allegati non viaggiano nel file.

Negli altri registri cambia solo che cosa vuol dire «una riga uguale», per i file che non portano il «Rif» o vengono da un altro registro, e quale colonna è indispensabile:

Registro	Una riga è già presente se ha uguali	Colonna indispensabile
Documentazione di sistema	Codice, Titolo, Versione	Titolo

Registro	Una riga è già presente se ha uguali	Colonna indispensabile
Procedure e revisioni	Codice, Procedura, Revisione (ogni revisione è una riga)	Procedura
Audit interni ed esterni	Codice / titolo, Data pianificata	Codice / titolo
Checklist personalizzate	Nome della checklist, N. d'ordine, Argomento	Argomento
Registro degli incidenti	Numero, Oggetto, Rilevato il	Oggetto
Inventario hardware e software	Codice / etichetta, Descrizione, N. di serie	Descrizione
Obiettivi e attività	Obiettivo	Obiettivo
Indicatori	Codice, Indicatore	Indicatore
Misurazioni	Indicatore (scritto col nome o col codice), Data della misura	Data della misura e Indicatore: una misurazione di un indicatore che nel registro non c'è ferma l'importazione
Formazione	Argomento, Data	Argomento
Riesame della direzione	Data del riesame	Data del riesame
Non conformità e azioni correttive	Numero, Oggetto	Oggetto
Fornitori	Fornitore	Fornitore
Requisiti legali e contrattuali	Requisito	Requisito
Cambiamenti	Cambiamento, Data prevista	Cambiamento
Rischi e opportunità del sistema	Tipo, Descrizione breve	Descrizione breve
Piano di comunicazione	Su che cosa, A chi	Su che cosa
Contatti con autorità e gruppi	Autorità, ente o gruppo	Autorità, ente o gruppo
Continuità operativa	Processo o servizio	Processo o servizio
Fattori del contesto	Interno o esterno, Fattore	Fattore
Parti interessate	Parte interessata	Parte interessata
Prese visione	Documento, Persona, Data (scritti col nome)	Documento e Persona, che devono esserci nel registro

Gli stessi campi sono ricordati nella finestra di importazione di ogni registro. I collegamenti viaggiano per nome anche qui: l'asset e la minaccia di un incidente, il rischio trattato da un obiettivo.

La checklist di audit

Nel gruppo **Audit** della sezione Sistema, la pagina **Checklist di audit** conduce un audit domanda per domanda. Si sceglie l'audit (fra quelli del registro degli audit) e la pagina propone le domande della **checklist dell'audit**, che si sceglie nella scheda dell'audit al campo **Checklist da usare**: la checklist di audit ISO/IEC 27001, descritta qui, oppure una checklist personalizzata. Un riquadro in testa alla pagina («Quale checklist, e come se ne fa una nuova») lo riassume.

La **checklist di audit ISO/IEC 27001** ha 139 domande, divise per capitolo: contesto, leadership, pianificazione, supporto, attività operative, valutazione delle prestazioni, miglioramento e controlli dell'Appendice A. Ogni domanda porta il **punto o il controllo della norma** che verifica (per esempio 6.1.3 d), A.5.15). Accanto alle domande sui controlli c'è lo stato del controllo nella SoA del registro.

I filtri scelgono il capitolo e l'esito (anche «da compilare») e cercano nel testo. Per ogni domanda si sceglie l'**esito** — **OK** conforme, **NC** non conformità, **RACC** raccomandazione od osservazione, **n.a.** non applicabile, **n.v.** non verificato — e si scrivono **evidenze** e note. Le risposte si salvano come gli altri campi (in sospeso fino a Salva), viaggiano con l'esportazione in XML ed entrano nelle revisioni. In testa, quante domande e quanti esiti di ogni tipo; nella finestra dell'audit, il conteggio delle risposte e dei rilievi, e i pulsanti per aprire la checklist e stampare i rilievi. Sotto una domanda con esito NC o RACC (salvato) compare **Registra la non conformità** (o l'osservazione): apre nel registro delle non conformità una riga già collegata all'audit e alla domanda, con requisito, evidenze e note; da quel momento sotto la domanda si legge la non conformità e il suo stato.

La **stampa** (pulsante della pagina, o menu delle stampe) mette tutte le domande con esito ed evidenze, oppure solo i **rilievi** (NC e RACC), con il riepilogo degli esiti per capitolo. Nelle domande i requisiti sono **parafrasati**, non riportati dal testo della norma, e vanno letti accanto alla norma stessa. La checklist ISO/IEC 27001 è comune a tutti i registri e **non si modifica** dal programma: per cambiarne le domande se ne fa una copia (qui sotto).

Le checklist personalizzate

Per un audit che non segue la checklist ISO/IEC 27001 — un audit a un fornitore, a un processo, una verifica mirata dopo un incidente — si scrive una checklist propria. Le domande stanno nel registro **Checklist personalizzate** (gruppo Audit), una riga per domanda: **nome della checklist** (le domande con lo stesso nome formano la checklist), numero d'ordine, capitolo o sezione, argomento, **che cosa verificare**, l'informazione documentata da vedere, note per chi fa l'audit, e — facoltativo — il **punto o controllo ISO/IEC 27001** che la domanda verifica.

Le checklist personalizzate possono essere **quante se ne vogliono**: ogni nome diverso è una checklist. In testa al registro, la barra **Checklist** le elenca con il numero delle loro domande; «Tutte» le mostra insieme, un clic su un nome mostra solo le sue domande, nel loro ordine.

- **Una checklist nuova**: **Nuova checklist…** chiede il nome e apre subito la prima domanda, già intestata. Le domande successive si aggiungono con «Nuovo: domanda» mentre la checklist è scelta nella barra: nascono in quella checklist, con il numero d'ordine che segue (di dieci in dieci). Si può anche scrivere la checklist in Excel e caricarla col CSV del registro: conviene esportare prima il CSV, anche vuoto, per avere le colonne giuste; un file può contenere più checklist.
- **Rinomina…** (con una checklist scelta) cambia il nome in tutte le sue domande e negli audit che la usano; le risposte restano. **Duplica…** ne fa una copia con un altro nome, per partire da una checklist esistente e farne una variante: le domande sono nuove, senza le risposte degli audit. Un nome già usato da un'altra checklist si rifiuta.

- **Il nome nella finestra della domanda** propone le checklist che ci sono, ma se ne può scrivere uno nuovo (la domanda passa a un'altra checklist, o ne inizia una). Un nome che differisce da uno esistente solo per maiuscole o spazi viene riportato a quello: «audit ai fornitori» finisce in «Audit ai fornitori», senza creare una seconda checklist quasi uguale.
- **Modificare la checklist ISO/IEC 27001**: nella pagina Checklist di audit, con un audit che usa la checklist ISO/IEC 27001, **Copia per modificarla…** chiede un nome e copia le 139 domande in una checklist personalizzata, con capitolo, riferimento e informazione documentata. Da lì si correggono, si tolgono quelle che non servono, se ne aggiungono altre. Il numero d'ordine va di dieci in dieci, così una domanda nuova si mette in mezzo.
- **Usarla**: nella scheda dell'audit, «Checklist da usare», si sceglie il nome. La pagina Checklist di audit mostra allora le sue domande, per sezione, con esito, evidenze e note come per la checklist ISO/IEC 27001; «Modifica le domande» porta al registro.

Le risposte, la stampa (tutte le domande o i soli rilievi), il pulsante **Registra la non conformità** sotto una domanda con esito NC o RACC funzionano come per la checklist ISO/IEC 27001; la non conformità nomina la domanda nel campo «Domanda della checklist personalizzata». Domande, risposte e collegamenti viaggiano con l'esportazione in XML. Eliminando una domanda le risposte già date restano nel registro, ma non si vedono più.

La copertura del programma di audit

Il programma di audit (9.2.2) deve verificare, nel tempo, tutto il sistema: in pratica ogni requisito e ogni controllo applicabile almeno una volta nel ciclo di certificazione, che dura tre anni. La pagina **Copertura degli audit** della sezione Sistema lo ricava dalle checklist: per ogni punto della ISO/IEC 27001 (dal 4.1 al 10.2) e per ognuno dei 93 controlli dell'Appendice A, l'ultimo audit che vi ha dato un esito (OK, NC, RACC o n.a.; «n.v.» vuol dire non verificato), la data, i rilievi di quell'audit, e la copertura: **verificato** negli ultimi 36 mesi, **da riverificare** se l'ultima volta è più vecchia, **mai verificato**. Conta la data di svolgimento dell'audit (o quella pianificata, se manca); gli audit annullati non contano. Serve per pianificare gli audit successivi: si guardano i punti in rosso.

Contano anche le domande delle checklist personalizzate che indicano il punto o il controllo: «9.2» o «A.5.19» (anche «a 5.19»). Un sottopunto vale per il suo punto («9.2.1» conta per il 9.2); un numero senza «A.» è un punto della norma, non un controllo («5.1» è la leadership, il controllo è «A.5.1»). Le domande senza riferimento non contano nella copertura.

In fondo la pagina ricorda gli audit svolti senza il campo **Obiettività e imparzialità di chi fa l'audit**, che la norma chiede di garantire (nessuno verifica il proprio lavoro). Si stampa dalla pagina o dal menu delle stampe.

Il fascicolo per il riesame

Il riesame della direzione (9.3) deve considerare una serie di elementi in ingresso, che nel programma stanno già tutti nei registri. Nella finestra di un riesame il riquadro **Elementi in ingresso dai registri** li raccoglie per il periodo dal riesame precedente a questo (o dai dodici mesi prima, se è il primo):

- le decisioni e le azioni del riesame precedente;
- dall'analisi del contesto, i fattori interni ed esterni rivalutati nel periodo (o un promemoria, se nessuno lo è stato) e il documento dell'analisi con la sua prossima revisione; poi i cambiamenti registrati e i rischi aperti per il sistema;
- le parti interessate rivalutate nel periodo, con le loro esigenze e se diventano requisiti (o il promemoria); i requisiti legali e contrattuali, con quelli non o parzialmente rispettati, e le comunicazioni esterne;
- le non conformità del periodo, quelle ancora aperte (in maiuscolo le scadute) e le azioni verificate efficaci;

- gli indicatori per esito, con quelli fuori soglia e da migliorare, e le esecuzioni degli adempimenti con rilievi;
- gli audit svolti, con gli esiti delle checklist, e la copertura del programma;
- gli obiettivi aperti o in scadenza, con l'avanzamento;
- segnalazioni, reclami e incidenti del periodo;
- la sintesi del rischio e del piano di trattamento, i fornitori da rivalutare o con riserva, la continuità operativa;
- le opportunità di miglioramento, le raccomandazioni degli audit.

Proponi i testi nei campi vuoti li scrive nei campi del riesame che sono ancora vuoti, come modifiche da confermare: si leggono, si correggono e si salva. I campi già scritti non si toccano. **Stampa il fascicolo** li mette in un documento da portare alla riunione; dal menu delle stampe si ha il fascicolo «a oggi», dall'ultimo riesame. È una raccolta di dati: le decisioni (9.3.3) le scrive la direzione.

Allegare file

A ogni riga di un registro si possono **allegare file**: la politica firmata, il rapporto dell'audit, il verbale del riesame, il foglio firme di un corso, la prova di un incidente. Nella scheda della riga, in fondo, il riquadro **Allegati** elenca i file con dimensione e data; **Allega file** ne aggiunge uno o più, il nome scarica il file, la × lo toglie. In griglia una graffetta accanto al nome dice quanti allegati ha la riga, e la stampa del registro ne riporta i nomi.

- Si allegano **subito**, senza passare da Salva; anche toglierne uno ha effetto immediato (dopo la conferma).
- Sono ammessi PDF (anche firmati .p7m), immagini, documenti di testo, fogli di calcolo e presentazioni, messaggi di posta, archivi compressi, .xml e .json; al massimo **15 MB per file**, 30 file per riga, 300 MB per registro. Un file con lo stesso nome di uno già allegato non lo sostituisce: prende un numero in coda.
- Gli allegati sono del registro e li vede solo chi lo possiede. Eliminando una riga si cancellano anche i suoi allegati (la conferma lo dice); archiviando il registro gli allegati vengono archiviati con lui.
- L'esportazione in XML porta le righe, **non i file**: reimportando il file nello stesso registro gli allegati restano sulle loro righe; importandolo in un altro registro le righe arrivano senza allegati.
- **Allegati rimasti senza riga.** Se un'importazione sostituisce i registri e una riga con allegati non c'è più, i suoi file non vengono cancellati subito: vengono **messi da parte per 30 giorni** (il messaggio dell'importazione lo dice). Se nel frattempo la riga torna — per esempio reimportando il proprio registro esportato prima — gli allegati tornano al loro posto da soli; passati i 30 giorni vengono cancellati. Chi ha importato il file sbagliato ha quindi un mese per rimediare. I file messi da parte non contano nei 300 MB del registro.
- Le revisioni consolidate conservano le righe com'erano, non i file: se un documento cambia, conviene allegare la nuova versione senza togliere la precedente.

> **Versione di prova**
>
> Nella versione di prova non si allegano file: il registro di prova è condiviso da chi si collega dalla stessa rete. Servono un'utenza e un registro proprio.

Conformità e miglioramento

La sezione **Conformità** raccoglie i registri che completano i punti della norma rimasti fuori dalla valutazione del rischio. Funzionano come quelli della sezione Sistema: griglia, finestra, Salva, filtri, stampa, CSV, allegati, revisioni ed esportazione. I pulsanti seguono l'ordine in cui di solito si lavora: per primo il gruppo **Analisi del contesto** (la pagina dell'analisi, i fattori del contesto e le parti interessate, su una seconda riga quando il gruppo è aperto), poi requisiti legali, rischi e opportunità, continuità operativa, piano di comunicazione, contatti con autorità e gruppi, fornitori, cambiamenti, e per ultime le non conformità.

Registro	Che cosa contiene	Riferimento
Fattori del contesto	Facoltativo, nel gruppo Analisi del contesto. I fattori interni ed esterni che contano per la sicurezza delle informazioni: categoria (compreso il cambiamento climatico), se sono un rischio o un'opportunità per il sistema, rilevanza, effetto, come se ne tiene conto, il rischio o l'opportunità del sistema e la minaccia collegati	4.1
Parti interessate	Facoltativo, nel gruppo Analisi del contesto. Chi ha interesse nel sistema, che cosa si aspetta, se le sue esigenze diventano requisiti (con il requisito collegato), come se ne tiene conto, chi tiene il rapporto	4.2
Requisiti legali e contrattuali	Gli obblighi di legge, di regolamento e di contratto: da dove vengono, che cosa chiedono, se si applicano, come si rispettano, con quali controlli, chi ne risponde, la conformità e l'ultima verifica	4.2; controlli 5.31–5.34
Rischi e opportunità del sistema	I rischi e le opportunità per il sistema di gestione stesso (non per le informazioni): da dove nascono, rilevanza, azioni, valutazione della loro efficacia	6.1.1
Continuità operativa	L'analisi d'impatto dei processi (fermo massimo tollerabile, tempo di ripristino, dati perdibili), le dipendenze, la strategia, il piano e le sue prove	controlli 5.29, 5.30
Piano di comunicazione	Su che cosa si comunica, a chi, quando o con che frequenza, chi lo fa e come; interne ed esterne	7.4
Contatti con autorità e gruppi	Autorità per la protezione dei dati, CSIRT, forze dell'ordine, emergenze, associazioni di settore, fornitori critici, assicurazione: recapiti, in quali casi si chiamano, chi lo fa, quando sono stati verificati	controlli 5.5, 5.6
Fornitori	Chi tratta informazioni dell'organizzazione o ne gestisce i sistemi, compresi i servizi cloud: servizio, criticità, dove stanno i dati, nomina a responsabile del trattamento, clausole e accordo di riservatezza, certificazioni, valutazione con la data della prossima, come si esce dal rapporto	8.1; controlli 5.19–5.23
Cambiamenti	I cambiamenti pianificati prima di farli: perché, che cosa cambia, effetti su rischi e controlli, chi approva, come si torna indietro, la verifica dopo	6.3; controllo 8.32
Non conformità e azioni correttive	Ogni non conformità o osservazione, da dove viene (audit, incidente, riesame, indicatori, adempimento, segnalazione, reclamo), il requisito non soddisfatto, la correzione immediata, l'analisi delle cause, l'azione correttiva con responsabile e scadenza, la verifica dell'efficacia e la chiusura	10.2

Le non conformità si aprono da dove nascono. Oltre che con «Nuovo» (numero proposto «NC-anno-progressivo», stato «Aperta», data di oggi), una non conformità si apre già collegata:

- dalla checklist di audit, sotto una domanda con esito NC o RACC;
- dalla finestra di un **audit** o di un **incidente**, con **Apri una non conformità** (per un incidente prende descrizione, cause, azioni immediate e correttive, rischio e responsabile);
- dalla finestra di un'**esecuzione** di un adempimento con esito «con rilievi» o «non eseguito».

Il collegamento si vede in testa alla finestra della non conformità («Nasce dall'audit…, domanda 239 della checklist») e nella finestra di partenza, con lo stato. Se l'audit, l'incidente o l'esecuzione si eliminano, la non conformità resta, senza collegamento. Le non conformità aperte, con quelle che hanno la scadenza passata, sono anche nel Riepilogo e nel fascicolo per il riesame.

Collegamenti. Un fornitore e un cambiamento si collegano a un asset, un cambiamento e una non conformità al rischio che toccano, un processo della continuità all'asset principale e al fornitore da cui dipende. I controlli che un fornitore o un requisito riguardano si scrivono per codice, come negli indicatori, e sotto se ne leggono i titoli. La valutazione periodica di un fornitore, la verifica di un requisito, la prova di un piano di continuità si possono seguire come adempimenti, con gli avvisi.

L'analisi del contesto (facoltativa)

I punti 4.1 e 4.2 chiedono di conoscere i fattori interni ed esterni che contano per la sicurezza delle informazioni — dal 2024 anche di stabilire se il **cambiamento climatico** è rilevante — e le parti interessate con le loro esigenze. Il programma lascia due strade:

- **c'è già un'analisi**, fatta per un altro sistema di gestione (qualità, ambiente) o da un consulente: la si registra nella Documentazione di sistema come ogni documento, con **«4.1, 4.2»** nel campo «Clausola o controllo di riferimento», e la si allega se si vuole. La mappa della norma la trova da lì;
- **la si fa qui**: il gruppo **Analisi del contesto**, il primo della sezione Conformità, che si apre sulla pagina dell'analisi («Testi e documento»), con accanto i registri dei fattori e delle parti interessate (ci si arriva anche dal rimando nella sezione Organizzazione).

Nella pagina:

1. i **fattori del contesto**, uno per riga: interno o esterno, categoria (politica, economica, sociale, tecnologica, legale, ambientale, cambiamento climatico, organizzativa…), se per il sistema è un rischio, un'opportunità o neutro, la rilevanza, che effetto può avere e come se ne tiene conto, collegandolo se serve al rischio o all'opportunità del sistema che ne deriva o a una minaccia del registro dei rischi;
2. le **parti interessate**: interna o esterna, categoria, esigenze e aspettative, se diventano requisiti (con il requisito legale o contrattuale collegato), come se ne tiene conto, chi tiene il rapporto;
3. tre testi: il **metodo** (come si è fatta l'analisi, chi ha partecipato, ogni quanto si riesamina), il **cambiamento climatico** (è rilevante? perché) e le **conclusioni**. Si confermano con Salva;
4. **Genera il documento**: lo registra nella Documentazione di sistema — codice CTX-01, tipo «Analisi o valutazione», riferimento «4.1, 4.2», versione 1, stato «Bozza» — e ne apre la finestra, dove si completa (responsabile, approvazione, prossima revisione) come ogni documento. Le volte successive il pulsante diventa **Aggiorna il documento**: la stessa riga passa alla versione successiva e torna in bozza, da approvare di nuovo.

Sotto, l'**anteprima** del documento: scopo e campo di applicazione, metodo, fattori esterni e interni, una sintesi in quattro riquadri (punti di forza, debolezze, opportunità, minacce), il cambiamento climatico, le parti interessate, le conclusioni. Si compone dai registri al momento, come le altre stampe: **Stampa** lo apre pronto per la stampa o per il PDF. Le versioni passate del contenuto restano nelle revisioni consolidate.

La verifica del 4.1 sul cambiamento climatico è soddisfatta dalla conclusione scritta qui o da un fattore di quella categoria: anche chi usa un'analisi fatta altrove può scrivere qui soltanto la conclusione.

Analisi del contesto: lo scenario di lavoro

L'analisi del contesto non è un documento da scrivere per l'auditor: è il punto da cui il sistema prende la sua forma. Dice **che cosa c'è attorno all'organizzazione** e **che cosa le chiedono**, e da lì discendono il campo di applicazione, una parte delle minacce, i requisiti da rispettare, i rischi e le opportunità per il sistema stesso. Il programma l'ha pensata così:

- **Chi**: la direzione, con chi coordina la sicurezza delle informazioni e, se c'è, il consulente o il fornitore informatico. Chi conosce il mercato e i clienti è indispensabile quanto chi conosce i sistemi.
- **Quando**: all'inizio del percorso, **prima o mentre** si valutano i rischi (Fase 2 di Da dove cominciare), perché ne vengono minacce e requisiti; poi a ogni riesame della direzione, e ogni volta che cambia qualcosa di importante (una nuova sede, un nuovo cliente che chiede garanzie, un fornitore critico, una legge).
- **Quanto**: per una piccola organizzazione basta una riunione di mezza giornata; per una media, due incontri. Non serve un elenco lungo: servono i fattori che **cambiano qualcosa** nelle decisioni. Cinque fattori e cinque parti interessate ben scelti valgono più di cinquanta generici.
- **Con che cosa**: i contratti e le gare dell'ultimo anno, le richieste dei clienti, le leggi e i regolamenti che si applicano, gli incidenti registrati, l'organigramma, la mappa dei fornitori. Il metodo può essere una griglia PESTLE (politica, economia, società, tecnologia, legge, ambiente) per i fattori esterni e una SWOT per il quadro d'insieme: il documento la compone da sé, dai fattori registrati.
- **Dove si scrive**: un fattore o una parte interessata per riga, nei due registri; tre testi brevi nella pagina; il documento si genera con un clic. Ogni riga che produce una conseguenza si **collega** al registro dove la conseguenza si gestisce: è il collegamento a dimostrare, in audit, che l'analisi non è rimasta sulla carta.

Analisi del contesto: un esempio completo

Il primo registro di esempio, lo **studio tecnico associato** (cinque persone, una sede, progettazione e direzione lavori, gestionale in cloud, un NAS in sede, un consulente informatico esterno), ha l'analisi già fatta: si apre dalla pagina iniziale e si segue passo per passo nella sezione Conformità › Analisi del contesto.

1. I fattori del contesto. Cinque, ciascuno con la sua conseguenza:

Fattore	Interno / esterno, categoria	Per il sistema è	Rilevanza	Dove finisce
Committenti pubblici che chiedono garanzie sulla riservatezza dei progetti	Esterno, economico e di mercato	Opportunità	Alta	Registro **Rischi e opportunità del sistema**: «Usare il sistema di gestione nelle gare pubbliche» (6.1.1)
Attacchi ransomware contro gli studi professionali	Esterno, tecnologico	Rischio	Alta	**Registro dei rischi**: minaccia «Manomissione del software (ransomware)», trattata con la copia in cloud e la prova di ripristino (6.1.2, 6.1.3)
Gestione dei sistemi affidata a un solo consulente esterno	Interno, persone e competenze	Rischio	Alta	**Rischi e opportunità del sistema**: «Dipendenza da un solo consulente informatico», con le azioni decise (6.1.1)

Fattore	Interno / esterno, categoria	Per il sistema è	Rilevanza	Dove finisce
Studio piccolo, decisioni rapide dei soci	Interno, organizzazione e governo	Opportunità	Media	Nessun registro: è un punto di forza, compare nella sintesi del documento
Ondate di calore estive nel locale del NAS	Esterno, cambiamento climatico	Rischio	Bassa	**Registro dei rischi**: minaccia «Guasto delle apparecchiature»; risponde alla domanda sul clima del 4.1

La regola che l'esempio segue: un fattore che minaccia **le informazioni** (riservatezza, integrità, disponibilità) si collega a una **minaccia** del registro dei rischi; un fattore che minaccia o favorisce **il sistema di gestione** (le persone che lo fanno funzionare, il mercato, l'organizzazione) va nei **rischi e opportunità del sistema**; un fattore neutro o un punto di forza senza azioni resta nell'analisi e basta.

2. Le parti interessate. Cinque: committenti pubblici, committenti privati, autorità per la protezione dei dati, personale e collaboratori, consulente informatico. Per le prime tre le esigenze **diventano requisiti** («Le sue esigenze diventano requisiti» = Sì) e si collegano ai **Requisiti legali e contrattuali**: «Riservatezza degli elaborati per un committente pubblico» e «Sicurezza del trattamento dei dati personali». Per il personale e il consulente no: si dice come se ne tiene conto (sensibilizzazione annuale, contratto in revisione con le clausole di sicurezza) e come si comunica con loro.

3. I tre testi.

- **Metodo**: «Analisi PESTLE e SWOT in una riunione dei soci con il consulente informatico, sulla base dei contratti in corso, delle gare dell'ultimo anno e degli incidenti registrati. Si riesamina a ogni riesame della direzione.»
- **Cambiamento climatico**: «Rilevante in misura bassa: una sola sede, non in zona a rischio; le ondate di calore possono far spegnere il NAS nel locale tecnico non climatizzato.» Una risposta motivata, anche «non rilevante, perché…», è quello che la norma chiede.
- **Conclusioni**: che cosa ne viene per il sistema — il campo di applicazione (progettazione, direzione lavori e pratiche edilizie, in sede e in mobilità), un rischio e un'opportunità per il sistema, i requisiti sulla protezione dei dati e sulla riservatezza degli elaborati.

4. Il documento. «Genera il documento» ha registrato la riga CTX-01 «Analisi del contesto e delle parti interessate» nella Documentazione di sistema, riferimento «4.1, 4.2»; i soci l'hanno approvata e messa in vigore.

Analisi del contesto: dove ha effetto

Da che cosa	A che cosa	Dove nel programma	Punto della norma
Fattore che minaccia le informazioni	Una minaccia da valutare e trattare (nuova, o già presente e confermata)	Minacce, Trattamento; campo «Minaccia del registro dei rischi collegata» del fattore	6.1.2, 6.1.3, 8.2, 8.3
Fattore che tocca il sistema di gestione	Un rischio o un'opportunità del sistema, con le azioni e la verifica della loro efficacia	Conformità › Rischi e opportunità del sistema; campo «Rischio o opportunità del sistema che ne deriva»	6.1.1
Azioni su rischi e opportunità	Obiettivi e attività, indicatori se serve misurarle	Sistema › Obiettivi e attività, Indicatori	6.2, 9.1

Da che cosa	A che cosa	Dove nel programma	Punto della norma
Parte interessata con esigenze vincolanti	Un requisito legale o contrattuale, con i controlli che lo rispettano	Conformità › Requisiti legali e contrattuali; campo «Requisito … collegato»	4.2; controlli 5.31–5.34
Parte interessata da informare	Una voce del piano di comunicazione	Conformità › Piano di comunicazione	7.4
Fornitori fra le parti interessate	La loro valutazione, le clausole, il rapporto	Conformità › Fornitori	8.1; controlli 5.19–5.23
Conclusioni	Il campo di applicazione e i suoi confini; le esclusioni della SoA motivate di conseguenza	Organizzazione (campo di applicazione, confini e interfacce); Controlli e SoA	4.3, 6.1.3 d
Il documento generato	Informazione documentata da approvare, far leggere e rivedere	Sistema › Documentazione di sistema (CTX-01), prese visione	7.5, 7.3
Tutta l'analisi	Le verifiche dei punti 4.1 e 4.2, compresa quella sul clima	Riepilogo › Mappa della norma	4.1, 4.2
I cambiamenti nel tempo	Un elemento in ingresso del riesame	Sistema › Registri › Riesame della direzione, campo «Cambiamenti nei fattori interni ed esterni»	9.3.2 b, c
Le domande sul contesto in audit	Le domande 1 e 2 della checklist di audit (4.1, clima), con il documento come evidenza	Sistema › Audit › Checklist di audit	9.2

Nessuno di questi collegamenti cambia da solo un numero del registro dei rischi: il calcolo resta quello di sempre. Il collegamento serve a ritrovare, da una parte e dall'altra, il perché di una decisione.

Analisi del contesto: i passi dopo la compilazione

1. **Genera il documento** e aprine la finestra: responsabile, approvato da, data, **prossima revisione** (di solito un anno); lo stato passa da «Bozza» a «In vigore» quando la direzione l'ha approvato. Se si vuole, si allega la versione firmata.
2. **Riporta le conseguenze nei registri**, riga per riga, come nella tabella qui sopra: le minacce nuove nel registro dei rischi (con asset, verosimiglianza, controlli), i rischi e le opportunità del sistema con le loro azioni, i requisiti, le voci del piano di comunicazione, i fornitori. Poi collega il fattore o la parte interessata alla riga creata.
3. **Rileggi il campo di applicazione** nella sezione Organizzazione alla luce delle conclusioni (attività, sedi, confini, interfacce con fornitori e clienti), e controlla che le esclusioni della SoA siano coerenti.
4. **Valuta i rischi e decidi i trattamenti** delle minacce che ne sono nate: è la parte che l'auditor seguirà di più.
5. **Fallo conoscere**: dalla finestra del documento, le prese visione dei responsabili interessati.
6. **Controlla la mappa della norma** (Riepilogo › Mappa della norma): i punti 4.1 e 4.2 devono risultare completi, e i collegamenti portano dritti alle righe da mostrare.

7. **Tienila viva**:
    - un adempimento annuale «Riesame dell'analisi del contesto» (sezione Adempimenti), assegnato a chi coordina la sicurezza, con gli avvisi prima della scadenza;
    - ogni cambiamento importante nel registro dei Cambiamenti, che il fascicolo del riesame raccoglie da sé;
    - nel riesame della direzione, i campi «Cambiamenti nei fattori interni ed esterni» e «Cambiamenti nelle esigenze delle parti interessate»: il fascicolo ci propone i fattori e le parti rivalutati dall'ultimo riesame (con la data del campo «Valutato il»), il documento dell'analisi con la sua prossima revisione e, se nel periodo non è stato rivalutato niente, un promemoria che dice di riprendere l'analisi. Per questo, ogni volta che si riguarda un fattore o una parte interessata, conviene aggiornarne la data di valutazione, anche se il resto non cambia;
    - un fattore o una parte che non vale più si mette a «Superato» / «Superata»: resta nello storico ma esce dal documento;
    - a lavoro fatto, **Aggiorna il documento**: la stessa riga sale di versione e torna in bozza, da approvare di nuovo; la versione di prima resta nelle revisioni consolidate del registro.

Impostazioni: estensioni e campi codificati

In testa alla sezione, la scheda **Catalogo dei controlli** accende le **estensioni**: **cloud** (ISO/IEC 27017 e 27018) e **privacy** (ISO/IEC 27701). Spente, i controlli e la Dichiarazione di Applicabilità mostrano solo l'Appendice A della ISO/IEC 27001; accese, i loro controlli compaiono come temi in più. La scelta vale per questo registro, si conferma con Salva e viaggia con l'esportazione. Spegnerle non cancella niente: i controlli già valutati o collegati restano visibili. Nei registri di esempio è accesa solo nel terzo, il fornitore di software in cloud.

Un **campo codificato** è un campo che si riempie scegliendo da un **elenco**: la classificazione di un asset, il tipo di un documento, lo stato di un audit. Codificato vuol dire confrontabile: «Riservato» scritto in tre modi diversi sono tre valori diversi per un filtro, per una stampa, per chi legge. Dove è possibile, quindi, i campi non sono a testo libero.

La sezione **Impostazioni** (l'ingranaggio in fondo alla barra delle sezioni) elenca tutti gli elenchi, raggruppati: Asset, Minacce, Controlli e trattamento, e uno per ogni menu dei registri di sistema. Aprendo un elenco si vedono le **voci, una per riga**: si aggiungono, si tolgono, si mettono nell'ordine in cui devono comparire nei menu. Le modifiche si confermano con Salva, come ogni altro campo.

- Gli elenchi sono **del registro**, non del programma: ogni organizzazione ha i suoi livelli di classificazione, le sue unità, i suoi tipi di documento. Il programma propone delle voci predefinite; «Voci predefinite» le rimette nel campo.
- Gli elenchi regolati **viaggiano con l'esportazione** ed entrano nelle revisioni consolidate. Importando un file che non li porta (per esempio dal foglio di calcolo) restano quelli del registro; aprire un registro di esempio li riporta ai predefiniti.
- **Togliere una voce non cambia i dati già scritti**: le schede che la portano la tengono, segnata «non in elenco» nel menu, e l'elenco dice quante sono («fuori elenco»). Si rimette la voce, o si correggono le schede.
- Alcune voci **non si possono togliere** perché il programma le usa: un trattamento «Completato» non è più un'azione aperta né scaduta; negli altri registri, le voci di chiusura (per esempio «Chiuso», «Superato», «Annullato») fanno sì che una data passata non venga più segnalata. Se ne possono aggiungere altre accanto.
- «Aggiungi le voci già usate nelle schede» porta nell'elenco i valori già scritti: è il modo più rapido per compilare un elenco in un registro già avviato. Serve soprattutto per un registro importato dal foglio di calcolo, che nella categoria delle minacce porta i gruppi invece delle origini: le minacce importate restano com'erano, segnate «non in elenco» finché le voci non si aggiungono all'elenco o le schede non si correggono.

Gli elenchi sono di tre tipi, e il tipo decide come si presenta il campo nella scheda:

Tipo	Il campo nella scheda	Esempi
Chiuso («menu»)	Un menu: si sceglie una delle voci, e basta	Classificazione, categoria, ruolo, base giuridica, stati, opzioni di trattamento, tutti i menu dei registri
Aperto («proposte»)	Un testo con le voci come proposte: se ne sceglie una e la si completa, o si scrive altro	Archivi, tipi di dati personali
Vuoto («testo libero»)	Un testo libero, finché nell'elenco non si scrive almeno una voce: da quel momento è un menu	Unità organizzative

Gli elenchi che si regolano

Elenco	Campo	Voci predefinite
Categorie degli asset	Asset › Categoria	Informativi, Software, Hardware, Infrastrutture, Human, Intangibili
Classificazione delle informazioni	Asset › Classificazione	Pubblico, Interno, Riservato, Strettamente riservato
Unità organizzative	Asset › Unità organizzativa	Nessuna: testo libero finché non si compila
Archivi (proposte)	Asset › Archivi	Server in sede, NAS in sede, Servizio in cloud (SaaS), Cloud pubblico (IaaS/PaaS), Postazioni e portatili, Dispositivi mobili, Archivio cartaceo in sede, Supporti rimovibili, Presso un fornitore
Ruolo dell'organizzazione	Asset › Ruolo	Titolare, Contitolare, Responsabile
Base giuridica del trattamento	Asset › Base giuridica	Consenso, Contratto, Obblighi legali, Salvaguardia interessi vitali, Interesse pubblico, Interessi legittimi del titolare
Tipi di dati personali (proposte)	Asset › Tipi di dati	Nessun dato personale, Personali comuni, Particolari (art. 9), Giudiziari (art. 10), Con profilazione
Ambito delle minacce	Minacce › Ambito	Gli otto gruppi del catalogo ISO/IEC 27005 (Danni fisici, Eventi naturali, Perdita di servizi essenziali, Disturbi da radiazioni, Compromissione delle informazioni, Guasti tecnici, Azioni non autorizzate, Compromissione delle funzioni) e Sicinfo, l'ambito generico
Categoria delle minacce	Minacce › Categoria	L'origine: D (deliberata), A (accidentale), E (ambientale) e le loro combinazioni
Stato di attuazione dei controlli	Controlli › Stato di attuazione	Non attuato, Pianificato, Parzialmente attuato, Attuato
Opzioni di trattamento	Trattamento › Opzione	Mitigare, Accettare, Trasferire, Evitare
Stato delle azioni di trattamento	Trattamento › Stato	Da avviare, Pianificato, In corso, Completato (non si toglie)
I menu dei registri di sistema	Sistema › ogni campo a scelta di ogni registro (tipo, stato, esito, gravità…)	Quelle del registro; le voci di chiusura non si tolgono

Che cosa non si regola

Le scale del calcolo — valori R/I/D e conseguenze (1-4), verosimiglianza (1-3), valutazione dei controlli (1-4), esiti della checklist — l'applicabilità sì/no e lo stato degli asset (ONLINE, OFFLINE, ELIMINATO) non sono elenchi: sono il metodo, e cambiarli cambierebbe i numeri di tutti i registri.

Riepilogo

Il cruscotto del registro: asset, minacce, controlli valutati, rischi alti, rischi medi o alti senza decisione, azioni aperte; la distribuzione del rischio attuale; la matrice verosimiglianza × conseguenze (il colore è la fascia del rischio inerente, il numero quante minacce stanno nella casella); le dieci minacce a rischio più alto con il residuo atteso; lo stato della Dichiarazione di Applicabilità; i registri del sistema di gestione e, se ce ne sono, gli indicatori: quanti in obiettivo, da migliorare e fuori soglia, con l'elenco di quelli che non sono in obiettivo; e gli adempimenti scaduti o in scadenza, con la data e il ruolo; le non conformità aperte (in rosso quelle con la scadenza passata), i fornitori da rivalutare e i requisiti non rispettati.

La mappa della norma ISO/IEC 27001

La seconda pagina del Riepilogo, **Mappa della norma ISO/IEC 27001**, segue la norma punto per punto — dal 4.1 al 10.2, più i quattro temi dell'Appendice A — e serve sia a chi compila il registro, per sapere che cosa manca, sia a chi deve rispondere all'auditor, per arrivare in un clic alle registrazioni che dimostrano ogni punto. Per ogni punto:

- **che cosa si chiede**, in poche righe e con parole nostre (il testo della norma va letto nella norma);
- **dove si compila** nel portale: la sezione, il registro, la pagina, la stampa;
- le **verifiche** sui dati del registro, ciascuna con il segno verde o rosso: per esempio, per la politica (5.2) che ce ne sia una in vigore, che sia approvata e che tutto il personale ne abbia preso visione — e, se manca qualcuno, chi. Accanto a ogni verifica i **collegamenti**: un clic apre il registro, la riga (nella sua finestra), la pagina o i controlli del tema che la provano;
- lo **stato** del punto: **completo** se tutte le verifiche sono soddisfatte, **parziale** se solo alcune, **da fare** se nessuna;
- **chi ne risponde** (un ruolo, proposto mentre si scrive, o una persona) e una **nota** — dove stanno le evidenze che non sono nel portale, che cosa resta da fare. Si salvano con Salva, viaggiano con l'esportazione ed entrano nelle revisioni.

I filtri mostrano solo i punti da fare, parziali, completi, o da fare e parziali insieme, e un capitolo alla volta. **Stampa** produce la mappa con le verifiche e i nomi delle righe che le provano, da portare all'audit o da usare per prepararlo.

Le verifiche dicono se i dati che documentano un punto **ci sono**, non se sono **adeguati**: un punto «completo» ha le sue registrazioni, ma è l'audit a giudicarle. L'analisi del contesto (4.1) e delle parti interessate (4.2) la mappa la trova nella Documentazione di sistema, dal campo «Clausola o controllo di riferimento»: un documento fatto altrove e registrato lì, o quello generato dall'analisi del contesto.

Documenti da stampare

Dal menu con la stampante (o dai pulsanti del Riepilogo) si aprono, in una nuova scheda, diciotto documenti pronti per la stampa o per il salvataggio in PDF dal browser (pulsante «Stampa / salva in PDF»):

- **Registro dei rischi**: metodo e criteri, asset con i valori R/I/D, minacce con il calcolo, in ordine di rischio;
- **Elenco degli asset**: l'inventario delle informazioni e degli asset, raggruppato per categoria, con stato, unità organizzativa, referente, classificazione, archivi, valori R/I/D, MTPD, a quante minacce è collegato ciascuno e il rischio attuale più alto fra quelle; in testa i conteggi per categoria, per stato e per classificazione, e in fondo i dati personali trattati (ruolo, interessati, tipi di dati, base giuridica, fornitori, destinatari, trasferimenti, conservazione) per gli asset che ne hanno. Dalla sezione Asset, il pulsante **Stampa** lo produce **con i filtri in uso** (categoria, stato, testo cercato): il documento dice allora di essere un elenco parziale e quanti asset riporta sul totale;
- **Elenco delle minacce**: le minacce in ordine di rischio attuale, con ambito, categoria, parametri R/I/D, asset e controlli collegati, verosimiglianza, conseguenze, rischio puro, inerente, attuale e residuo atteso, e il trattamento deciso (opzione, stato, scadenza); in testa quante sono per fascia di rischio e per ambito. Dalla sezione Minacce il pulsante **Stampa** lo produce con la categoria e il testo scelti nei filtri (quando si guarda una matrice, lo stesso pulsante stampa le matrici);
- **Elenco dei controlli**: un elenco di lavoro, non la Dichiarazione di Applicabilità: per ogni controllo applicabilità, stato di attuazione, valutazione, attuazione secondo la checklist, minacce collegate, responsabile, ultima verifica, come è attuato e carenze. Dalla sezione Controlli il pulsante **Stampa** lo produce con il tema, il testo e il filtro in uso: per esempio i soli controlli non valutati di un tema, o quelli con l'applicabilità ancora da decidere;
- **Dichiarazione di Applicabilità (SoA)**: i controlli dell'Appendice A (e delle estensioni accese), inclusi o esclusi con la giustificazione, quante minacce trattano, stato e valutazione;
- **Piano di trattamento del rischio**: opzione, azioni, responsabili, scadenze (in rosso quelle passate di azioni non completate), residuo atteso, proprietario e accettazione, e gli obiettivi collegati a ogni rischio con stato e avanzamento. Di norma i rischi medi e alti e quelli già trattati; dalla sezione Trattamento il pulsante **Stampa** lo produce con le righe che la sezione mostra, quindi anche i rischi bassi se è spuntata «Mostra anche i rischi bassi senza trattamento»;
- **Verifica dei controlli**: le risposte alla checklist con evidenze e percentuale di attuazione;
- **Matrici dei collegamenti**: le tre matrici — minacce × asset, controlli × minacce, controlli × asset. Sulla carta le colonne portano una sigla (M1, M2… le minacce, A1, A2… gli asset) e la legenda è in testa al documento; in fondo a ogni matrice stanno conseguenze e rischio attuale di ogni minaccia, o quanti controlli proteggono ogni asset. Dei controlli sono elencati quelli collegati ad almeno una minaccia. I valori sono scritti nelle caselle: il documento si legge anche stampato in bianco e nero. Quando le colonne sono più di venti la matrice è divisa in **blocchi di venti colonne**, uno sotto l'altro con le stesse righe («Colonne da M1 a M20», «da M21 a…»), perché stia nella larghezza del foglio; il totale di riga conta tutte le colonne e sta nell'ultimo blocco.
- **Rapporto sugli obiettivi**: in testa quanti obiettivi per stato, quanti aperti hanno la scadenza passata e l'avanzamento medio; poi il quadro, prima gli aperti per scadenza e poi i chiusi (in grigio): stato, responsabile, scadenza (in rosso se passata), avanzamento con la barra, il rischio trattato con rischio attuale → residuo atteso, il suo trattamento e gli indicatori che ne misurano l'efficacia con il loro esito, e come si misura l'obiettivo (valore atteso e rilevato). Sotto, gli obiettivi uno per uno con tutti i campi compilati. Si apre anche dal pulsante **Rapporto** del registro «Obiettivi e attività»; il pulsante **Stampa l'obiettivo** nella finestra di un obiettivo stampa quello solo;

- **Rapporto sugli indicatori**: in testa il quadro degli indicatori in uso (non sospesi né dismessi), uno per riga, prima i fuori soglia e poi quelli da migliorare: ultimo valore con i dati di base, obiettivo, riferimento statistico, esito, andamento rispetto alla misurazione precedente, controlli, rischio e prossima misurazione (in rosso se passata); poi, per ciascuno, l'esito, il grafico e la tabella delle misurazioni. Si apre anche dal pulsante **Rapporto** del registro «Indicatori» (sezione Sistema); il pulsante **Stampa l'indicatore** nella finestra di un indicatore stampa quello solo, con la sua scheda;
- **Organigramma**: i ruoli con le persone che li ricoprono, in un albero dai ruoli di vertice;
- **Mansionari**: per ruolo o per persona, uno per pagina, in verticale, con compiti e responsabilità e quello che nel registro è assegnato a ciascuno (asset, controlli, trattamenti, adempimenti, righe dei registri);
- **Scadenzario degli adempimenti**: gli adempimenti dal più urgente, con ruolo, persone, ripetizione, prossima scadenza, arretrate, ultima esecuzione e avvisi, e le scadenze dei prossimi 90 giorni; dove ci sono chi verifica e chi approva, anche i loro ruoli e le esecuzioni da verificare e da approvare;
- **Checklist di audit**: le domande di un audit interno con esito ed evidenze, o solo i rilievi (NC e RACC): si stampa dalla pagina della checklist o dalla finestra dell'audit;
- **Analisi del contesto e delle parti interessate**: il documento composto dai fattori del contesto e dalle parti interessate, con la sintesi in quattro riquadri, il cambiamento climatico e le conclusioni (L'analisi del contesto);
- **Mappa della norma ISO/IEC 27001**: punto per punto che cosa si chiede, lo stato, le verifiche con le righe che le provano, chi ne risponde e le note (La mappa della norma);
- **Copertura del programma di audit**: punti e controlli della ISO/IEC 27001 con l'ultimo audit che li ha verificati (La copertura del programma di audit);
- **Fascicolo per il riesame**: gli elementi in ingresso del riesame raccolti dai registri, dalla finestra di un riesame o, a oggi, dal menu (Il fascicolo per il riesame).

Anche i registri della sezione Conformità si stampano, ciascuno dal suo pulsante Stampa, come quelli della sezione Sistema.

Ogni documento riporta l'intestazione dell'organizzazione, la data di stampa, l'ultima revisione consolidata e gli spazi per le firme.

Quando un documento occupa più pagine, **su ogni pagina** compaiono in alto il titolo del documento con il nome dell'organizzazione e il numero di pagina sul totale («Pagina 2 di 12»), e in testa a ogni tabella che continua viene **ripetuta la riga con i titoli delle colonne**. Titolo e numero di pagina sono scritti dal browser nel margine del foglio: li disegnano Chrome ed Edge aggiornati; con un altro browser le tabelle ripetono comunque i titoli delle colonne, e per i numeri di pagina si può attivare «Intestazioni e piè di pagina» nella finestra di stampa. Con Chrome ed Edge conviene invece lasciare quella voce spenta, altrimenti il browser aggiunge anche le sue.

Verticale o orizzontale. In alto, accanto a «Stampa / salva in PDF», due pulsanti scelgono l'orientamento del foglio prima di stampare o di produrre il PDF. Di norma i documenti sono orizzontali, perché le tabelle sono larghe; i mansionari e le stampe dei registri di ruoli, personale e prese visione sono verticali, perché si leggono come un testo. L'organigramma resta orizzontale. Si può sempre cambiare.

Importare ed esportare

Esporta scarica il registro in XML, nello stesso formato del foglio di calcolo «Registro dei rischi ISO/IEC 27005»: lo si può riaprire con quel foglio, archiviare o importare in un altro registro. **Importa** legge un file XML esportato dal foglio o da CyberSic e **sostituisce** il contenuto del registro (le revisioni consolidate restano). Prima di importare conviene consolidare una revisione o esportare.

Quello che il foglio non gestisce (applicabilità e giustificazione, stato di attuazione, checklist, opzione e stato del trattamento, accettazione del rischio, soglie, registri di sistema, elenchi dei campi codificati) viaggia nello stesso file ed è ignorato dal foglio quando lo rilegge.

Domande frequenti e avvertenze

CYBERSIC BASTA PER OTTENERE LA CERTIFICAZIONE?

No. È uno strumento per svolgere e documentare la valutazione e il trattamento del rischio; la certificazione la rilascia un organismo accreditato dopo l'audit del sistema di gestione, che comprende molto altro (politiche, procedure, formazione, audit interni, riesame).

POSSO CAMBIARE I VALORI PROPOSTI DAL CATALOGO?

Sì: una minaccia aggiunta dal catalogo diventa del registro, e ogni campo si modifica. Il catalogo resta com'è.

PERCHÉ UN CONTROLLO NON VALUTATO PEGGIORA IL RISCHIO?

Perché finché non se ne conosce l'efficacia si assume l'ipotesi peggiore (fattore 4), come per una minaccia senza controlli.

I RISULTATI VANNO VERIFICATI

CyberSic non sostituisce il giudizio di chi valuta i rischi: prima di approvare o presentare un documento, controllarne i contenuti.

Appendice — I modelli delle finestre

Per chi cura il programma, non per chi lo usa. La disposizione dei campi in ogni scheda — dove sta un campo, quanto è largo, in che ordine, con quale etichetta, dentro quale riquadro — non è scritta nel programma: sta in un **modello**, un file di testo nella cartella `apps\csic` del sito, uno per scheda. Cambiando il modello cambia l'aspetto della scheda (e della stessa scheda aperta in finestra dalla griglia); le funzioni restano del programma.

Modello	Scheda	Blocchi
`_organizzazione.inc`	Organizzazione	—
`_criteri.inc`	Criteri di valutazione del rischio	spiegazione
`_asset.inc`	Asset	avviso
`_minaccia.inc`	Minaccia	parametri, asset, controlli, calcolo
`_controllo.inc`	Controllo	percentuale, checklist
`_trattamento.inc`	Trattamento del rischio	simulazione, obiettivi
`_reg-documenti.inc`, `_reg-procedure.inc`, `_reg-audit.inc`, `_reg-incidenti.inc`, `_reg-inventario.inc`, `_reg-obiettivi.inc`, `_reg-formazione.inc`, `_reg-riesami.inc`	Le righe dei registri di sistema	allegati (e trattamento, negli obiettivi; controlli e misure, negli indicatori)

Le regole, ripetute in testa a `_asset.inc`:

- Il modello è HTML con le righe e le colonne di Bootstrap (`div.row`, `div.col-md-N`: dodici colonne per riga).
- Per bilanciare le righe con molti campi piccoli c'è anche la **griglia da 24**, come in data-set.it: `col-24-N` prende N parti su 24. `col-24-3`, un ottavo di riga, è la misura giusta per una data o un numero, che la griglia da 12 non ha. Le due griglie si mischiano nella stessa riga purché la somma faccia la riga intera (`col-md-N` vale `col-24-2N`: per esempio `col-md-6` + `col-24-9` + `col-24-3`). Sotto i 768 pixel, come le `col-md`, ogni campo va a tutta larghezza.
- Un **campo** è un elemento con `data-tag='NomeDelCampo'`: `<input data-tag='Informazioni' />`, `<select data-tag='Categoria'></select>`, `<textarea rows="3" data-tag='Note'></textarea>`. I nomi dei campi di ogni scheda sono elencati nel commento in testa al suo modello. L'etichetta è il `<label>` accanto: il testo è libero.
- Un **blocco** è una parte che non è un campo solo (l'elenco degli asset collegati, la checklist, gli allegati): si scrive `<TAG>nome</TAG>` nel punto in cui deve comparire.
- Valori, voci dei menu, spiegazione sotto il campo, «?» della guida, salvataggio con conferma: li mette il programma. Se un campo è un menu o un testo lo decide il programma (per i campi codificati, l'elenco delle Impostazioni), non il modello.
- **Niente si perde**: un campo che il modello dimentica viene aggiunto in fondo alla scheda sotto «Altri campi», un blocco dimenticato in fondo; un `data-tag` con un nome sbagliato resta un campo spento, su fondo rosa. Se il file manca, la scheda si compone da sola.
- Il file si salva in UTF-8; dopo una modifica basta ricaricare la pagina del registro.

Appendice — Revisioni del manuale

Data	Che cosa è cambiato
26/09/2026	Prima stesura: elenco e cruscotto, organizzazione e criteri, asset, minacce e calcolo, controlli con SoA e checklist, trattamento, revisioni e rivalutazione, riepilogo, stampe, importazione ed esportazione.
26/09/2026	Aggiunti i tre registri di esempio (sezione «I registri di esempio»).
26/09/2026	Accesso: recupero della password con un link a scadenza, blocco dopo troppi tentativi falliti, chiusura delle sessioni di utenze sospese o cancellate («Accedere»).
27/09/2026	Le modifiche si confermano con Salva, tutte insieme o nessuna («Il salvataggio»); controlli divisi per temi; la checklist della revisione precedente nella scheda del controllo e nella rivalutazione («La checklist di verifica», «Revisioni e rivalutazione»); schede aperte evidenziate, Apri tutte / Chiudi, filtri sempre visibili.
04/10/2026	Una postazione per volta: un nuovo accesso con la stessa utenza chiude la sessione di prima, che alla prima operazione viene riportata alla pagina iniziale con la spiegazione; lo stesso quando la sessione scade o l'utenza viene sospesa. L'uscita chiude la sessione anche sul server («Accedere»).
05/10/2026	Sette giorni: il registro della versione di prova che nessuno apre né modifica per sette giorni viene cancellato («Versione di prova e con abbonamento»). I registri di chi ha un'utenza non scadono.
12/10/2026	Asset in sei categorie; asset, minacce e controlli anche in griglia, con la modifica in una finestra («Schede e griglia»); la guida ai valori e alle categorie accanto ai campi («Come classificare»); la stampa «Matrici dei collegamenti», a blocchi di venti colonne; la matrice Controlli × asset, che si legge soltanto, e le matrici Asset × minacce e Controlli × minacce, dove si collega con un clic («Le matrici dei collegamenti»).
12/10/2026	La sezione Sistema con gli otto registri del sistema di gestione: documentazione, procedure e revisioni, audit interni, incidenti, inventario, obiettivi e attività (collegati ai trattamenti), formazione, riesame della direzione («Sistema di gestione: i registri»). I tre registri di esempio ne hanno alcune righe. Alle righe si possono allegare file («Allegare file»); quelli rimasti senza riga dopo un'importazione sono messi da parte e cancellati dopo 30 giorni. Gli asset hanno uno stato: ONLINE, OFFLINE, ELIMINATO; gli asset eliminati non contano più nel calcolo delle conseguenze («Passo 1 — Asset», «Come si calcola il rischio»).
12/10/2026	Campi codificati: classificazione, categoria, unità organizzativa, ruolo, base giuridica, stati, opzioni e tutti i menu dei registri di sistema si scelgono da elenchi che ogni registro regola nella nuova sezione Impostazioni («Impostazioni: i campi codificati»); archivi e tipi di dati hanno delle proposte. Che cosa scrivere in archivi e classificazione, con i casi concreti («Archivi e classificazione»). La disposizione dei campi nelle schede sta nei modelli delle finestre («Appendice — I modelli delle finestre»).
13/10/2026	Codificati anche l'ambito e la categoria delle minacce, con le voci del catalogo ISO/IEC 27005 («Gli elenchi che si regolano»).
13/10/2026	Nuove stampe «Elenco degli asset», «Elenco delle minacce» ed «Elenco dei controlli», dal menu delle stampe, dal Riepilogo e dal pulsante Stampa delle sezioni Asset, Minacce e Controlli, che le produce con i filtri in uso («Schede e griglia», «Documenti da stampare»).
13/10/2026	La matrice degli asset e delle minacce è invertita: «Minacce × asset», con le minacce sulle righe, leggibili per intero, e gli asset sulle colonne; lo stesso nella stampa delle matrici («Le matrici dei collegamenti»).
13/10/2026	Stampe su più pagine: in alto, su ogni pagina, il titolo del documento e «Pagina N di M»; la riga dei titoli delle colonne ripetuta a ogni cambio pagina («Documenti da stampare»).

Data	Che cosa è cambiato
13/10/2026	Minacce dal catalogo anche in blocco: una finestra con l'elenco completo da spuntare (una, un gruppo, tutte), senza doppioni («Passo 2 — Minacce e rischio»).
13/10/2026	Asset in CSV: esportazione per il foglio di calcolo e importazione che aggiunge e aggiorna senza eliminare, anche da un altro registro («Gli asset in CSV: esportare e importare»).
13/10/2026	Anche le minacce in CSV, con i collegamenti a controlli e asset che all'importazione si aggiungono («Le minacce in CSV: esportare e importare»).
13/10/2026	Anche i controlli in CSV: applicabilità, stato, valutazione e note di ogni controllo, da compilare in un foglio di calcolo o da riprendere da un altro registro («I controlli in CSV: esportare e importare»).
13/10/2026	Anche l'inventario hardware e software si esporta e si importa in CSV («I registri in CSV: esportare e importare»). Il menu si chiama «CSV» in tutte le sezioni.
13/10/2026	Il CSV è esteso a tutti e otto i registri del sistema di gestione, ciascuno con i suoi campi per riconoscere una riga già presente («I registri in CSV: esportare e importare»).
13/10/2026	Nuova spiegazione «Da dove vengono i trattamenti»: perché ce n'è uno per minaccia, quali compaiono, e come inserire un trattamento che non nasce da un rischio valutato («Passo 4 — Trattamento»).
14/10/2026	Nuovi registri «Indicatori» e «Misurazioni» nella sezione Sistema: per ogni indicatore formula, obiettivo dell'azienda, soglia di allarme e riferimento statistico, i controlli e il rischio di cui misura l'efficacia; le misurazioni in tabella e in grafico, con l'esito dell'ultima (in obiettivo, da migliorare, fuori soglia) e il confronto con il riferimento e con la misurazione precedente. Gli indicatori compaiono nelle schede dei controlli e dei trattamenti, nel Riepilogo e nella stampa del registro; i tre registri di esempio ne hanno alcuni («Gli indicatori»).
14/10/2026	Indicatori con i dati di base: nella misurazione il conteggio e la base (un dato dell'azienda), e il valore lo calcola il programma (in percentuale se l'unità è «%»); una misurazione nuova riprende la base dell'ultima («Gli indicatori»).
14/10/2026	La guida ISO/IEC 27002 ai controlli: in cima alla scheda di ogni controllo enunciato, scopo e attributi; con «Come si legge questo controllo» la guida intera nel pannello a destra, con i rimandi fra i controlli e la spiegazione degli attributi; solo per gli utenti registrati («La guida ISO/IEC 27002 ai controlli»).
14/10/2026	Anche i trattamenti in griglia: il piano di trattamento in una tabella ordinabile, con la scheda in una finestra («Passo 4 — Trattamento», «Schede e griglia»).
14/10/2026	Pulsante Stampa nella sezione Trattamento: il piano di trattamento con le righe mostrate (anche i rischi bassi, se richiesti); nel piano le scadenze passate in rosso e gli obiettivi collegati a ogni rischio («Documenti da stampare»).
14/10/2026	Nuova stampa «Rapporto sugli indicatori»: il quadro degli esiti, poi grafico e misurazioni di ogni indicatore; dal menu delle stampe, dal Riepilogo, dal registro «Indicatori», e per un indicatore solo dalla sua finestra («Documenti da stampare»).
14/10/2026	Nuova stampa «Rapporto sugli obiettivi»: a che punto è ogni obiettivo, entro quando, quale rischio tratta con il suo trattamento e i suoi indicatori, poi il dettaglio di ciascuno; dal menu delle stampe, dal Riepilogo, dal registro «Obiettivi e attività», e per un obiettivo solo dalla sua finestra («Documenti da stampare»).
14/10/2026	Le sezioni principali in una barra a parte, sotto quella in alto, più grandi e in evidenza («La pagina del registro»).

Data	Che cosa è cambiato
14/10/2026	Nuova sezione «Ruoli e persone»: ruoli con compiti e responsabilità, personale con email, assegnazione dal ruolo o dalla persona, i campi dei responsabili che propongono i ruoli, organigramma, mansionario per ruolo e per persona, con le loro stampe («Ruoli e persone», «Documenti da stampare»).
14/10/2026	Nuova sezione «Adempimenti»: attività a scadenza assegnate a un ruolo, con ripetizione, avvisi per email prima e dopo la scadenza, esecuzioni e pulsante «Fatto», cruscotto con calendario e timeline, scadenzario da stampare («Adempimenti»).
14/10/2026	La checklist di audit interno ISO/IEC 27001: esiti ed evidenze per domanda, stampa completa o dei soli rilievi («La checklist di audit»).
15/10/2026	Nuova sezione «Conformità»: non conformità e azioni correttive (aperte anche dalla checklist di audit, da un incidente o da un'esecuzione con rilievi), fornitori, requisiti legali e contrattuali, cambiamenti, rischi e opportunità del sistema, piano di comunicazione, contatti con autorità e gruppi, continuità operativa («Conformità e miglioramento»).
15/10/2026	La copertura del programma di audit, ricavata dalle checklist, e il campo sull'imparzialità di chi fa l'audit («La copertura del programma di audit»); il fascicolo per il riesame, con gli elementi in ingresso raccolti dai registri e proposti nei campi vuoti («Il fascicolo per il riesame»); due stampe in più («Documenti da stampare»).
15/10/2026	Prese visione dei documenti, competenze possedute, partecipanti alla formazione e beni dell'inventario scelti dal personale, e quello che resta da chiudere alla cessazione («Ruoli e persone»); confini, interfacce e dipendenze nel campo di applicazione («Organizzazione e criteri»).
15/10/2026	La mappa della norma ISO/IEC 27001 nel Riepilogo: punto per punto che cosa si chiede, dove si compila, le verifiche sui dati con i collegamenti alle righe che le provano, lo stato, chi ne risponde e le note; e la sua stampa («La mappa della norma ISO/IEC 27001», «Documenti da stampare»).
15/10/2026	Nuova sezione «Da dove cominciare»: i passi da seguire partendo da un registro vuoto, in cinque fasi, con il punto della norma di ciascuno e il ritmo delle attività una volta avviato il sistema.
15/10/2026	Analisi del contesto facoltativa: fattori del contesto e parti interessate, metodo, cambiamento climatico e conclusioni; genera o aggiorna il documento CTX-01 nella Documentazione di sistema con riferimento «4.1, 4.2»; in alternativa resta il documento fatto altrove («L'analisi del contesto», «Da dove cominciare», «Documenti da stampare»).
15/10/2026	Nei modelli delle finestre anche la griglia da 24 (`col-24-N`), come in data-set.it, per bilanciare le righe con molti campi piccoli («Appendice — I modelli delle finestre»).
15/10/2026	Perché, con più controlli collegati a una minaccia, vale il più efficace; pregi e limiti del metodo e la regola pratica: collegare solo i controlli che riducono la minaccia davvero e in modo diretto («Perché vale il controllo più efficace»).
17/10/2026	Negli adempimenti chi verifica e chi approva, facoltativi; nelle esecuzioni esito, autore e data della verifica e dell'approvazione; «da verificare» e «da approvare» nel cruscotto, avvisi per email e mansionari; «Da rifare» e «Non approvato» riaprono la scadenza («Chi verifica e chi approva»).
17/10/2026	Nello scadenzario chi verifica e chi approva ogni adempimento e l'elenco delle esecuzioni da verificare e da approvare («Chi verifica e chi approva», «Documenti da stampare»).
17/10/2026	Verifica e approvazione anche nelle stampe dei registri degli adempimenti e delle esecuzioni («Chi verifica e chi approva»).

Data	Che cosa è cambiato
17/10/2026	Pulsanti delle sezioni a gruppi: in Sistema «Audit» (audit interni ed esterni, checklist di audit, checklist personalizzate, copertura), «Registri» (incidenti, inventario, formazione, riesame) e «Indicatori» (con le misurazioni in secondo piano); in Conformità «Analisi del contesto» (con fattori e parti interessate) e il nuovo ordine dei registri («Sistema di gestione: i registri», «Conformità e miglioramento»).
17/10/2026	Checklist personalizzate: un registro di domande raggruppate per nome, la scelta della checklist nella scheda dell'audit, la copia della checklist ISO/IEC 27001 per modificarla, le non conformità legate alle domande, la copertura dalle domande con il riferimento alla norma («Le checklist personalizzate», «La copertura del programma di audit»).
17/10/2026	Stampe verticali od orizzontali a scelta prima del PDF; mansionari e registri di ruoli e persone in verticale, con un riquadro per ogni ruolo e salti pagina più puliti («Documenti da stampare», «Ruoli e persone»).
17/10/2026	Analisi del contesto: lo scenario di lavoro (chi, quando, con che cosa), un esempio completo sul primo registro di esempio, dove ha effetto nel programma e nella norma, i passi dopo la compilazione («Analisi del contesto: lo scenario di lavoro», «un esempio completo», «dove ha effetto», «i passi dopo la compilazione»; «Da dove cominciare», passo 13).
17/10/2026	Il fascicolo del riesame raccoglie anche i fattori del contesto e le parti interessate rivalutati nel periodo, il documento dell'analisi con la prossima revisione e, se nel periodo non è stato rivalutato niente, il promemoria di riprendere l'analisi («Il fascicolo per il riesame», «i passi dopo la compilazione»).
17/10/2026	Finestre più compatte: negli adempimenti ruolo responsabile, chi verifica, chi approva e controlli su una riga; negli audit «Checklist da usare» al posto del blocco che stava prima. Tolto dalla checklist il riferimento al file di partenza («Chi verifica e chi approva», «La checklist di audit»).
17/10/2026	Più checklist personalizzate, in chiaro: la barra delle checklist in testa al registro, «Nuova checklist…», «Rinomina…», «Duplica…», le domande nuove nella checklist scelta, il nome della checklist proposto nella finestra della domanda e riportato a quello esistente se differisce solo per maiuscole o spazi («Le checklist personalizzate»).
17/10/2026	Il manuale anche in PDF e in Word, dai pulsanti in alto e dalla pagina iniziale: copertina, indice, ogni capitolo da una pagina nuova, numeri di pagina. Stampando la pagina dal browser si ottiene lo stesso del PDF.
17/10/2026	La checklist di audit è solo ISO/IEC 27001: 139 domande, ognuna con il punto o il controllo della norma; i punti seguono la numerazione della 27001 (per esempio 10.1 miglioramento continuo, 10.2 non conformità). Riepilogo degli esiti e stampa per capitolo («La checklist di audit»).
17/10/2026	Controlli più essenziali: di norma solo i 93 dell'Appendice A della ISO/IEC 27001; le estensioni cloud (27017, 27018) e privacy (27701) si accendono nelle Impostazioni; le clausole 4–10 non sono più fra i controlli; i controlli già in uso restano visibili. Nella scheda del controllo la guida ISO/IEC 27002 sempre in vista e la checklist sotto «Approfondisci»; la SoA con l'Appendice A e le estensioni accese («Passo 3 — Controlli e SoA», «Impostazioni»).
18/10/2026	La guida ISO/IEC 27002 ai controlli si vede anche nella versione di prova, nelle schede e nella finestra della griglia; la guida intera si chiude con «Dove si documenta»: in quale registro o sezione di CyberSic si tengono le evidenze del controllo («La guida ISO/IEC 27002 ai controlli»).
18/10/2026	«Vai a…»: al centro della barra viola una ricerca delle funzioni (sezioni, registri, pagine, stampe), che porta dove si sceglie come se si fosse navigato dai menu; Ctrl+K per arrivarci («La pagina del registro»).

Data	Che cosa è cambiato
20/10/2026	Il glossario della ISO/IEC 27002 (termini, definizioni, abbreviazioni) nel pannello a destra, dall'icona della barra viola e da «Vai a…» («Il glossario»). Nei controlli i cinque menu degli attributi (tipo di controllo, proprietà di sicurezza, concetti di cybersecurity, capacità operative, domini) per vederli da ogni punto di vista, anche nella stampa e nel CSV («Passo 3 — Controlli e SoA»).