APPUNTI CONDIVISI

Risk Assessment e Audit Interno nel Safeguarding

Quello che abbiamo visto insieme e alcune cornici per continuare a pensarci

Modulo Safeguarding — Politiche, prassi e applicazione contestuale

Traccia di lavoro post-corso

Prima di iniziare

Questi non sono una dispensa. Sono appunti. Cioè: un modo per fermare per iscritto quello che abbiamo fatto insieme durante le due sessioni del corso, con dentro anche qualche cornice teorica che in aula abbiamo solo sfiorato o che è utile riprendere adesso, a mente fredda.

Li scrivo in questa forma perché il corso è stato costruito su un'esperienza vostra, e sarebbe strano trasformarlo ora in una lezione impartita da qualcun altro. Quello che sappiamo su risk assessment e audit lo sappiamo perché lo abbiamo tirato fuori insieme dagli scenari e dalla policy di San Vittore: gli appunti hanno il compito di consolidare questa cosa, non di ripartire da capo.

Sono organizzati in tre parti. La prima ripercorre il metodo con cui abbiamo lavorato — perché siamo andati per intuizione prima di ricevere le definizioni, e cosa dice la pedagogia di questa scelta. La seconda torna sul risk assessment, mette insieme quello che è emerso dai gruppi e le cornici tecniche che lo codificano nella letteratura internazionale. La terza fa lo stesso con l'audit interno, con particolare attenzione alle distinzioni con altre forme di verifica che spesso ci vengono confuse. In fondo c'è una bibliografia essenziale per chi voglia continuare a lavorarci.

Parte I — Il metodo con cui abbiamo lavorato

Una premessa che riguarda il modo in cui ci siamo mossi in queste due sessioni. La scelta di non spiegare prima i concetti e di farli emergere dopo l'esperienza non è stata una stranezza didattica. Ha una sua fondazione teorica precisa, e vale la pena nominarla.

1. Perché non abbiamo cominciato dai concetti

La forma tradizionale di un corso su temi tecnici come il risk assessment e l'audit prevede una sequenza lineare: prima si definisce il concetto, poi si illustra il metodo, infine lo si applica a un caso. È la sequenza che spesso chiamiamo "deduttiva", nel senso classico: dal generale al particolare. Ha il vantaggio della chiarezza, ma ha un limite serio: il concetto arriva come qualcosa di esterno, che va accettato dall'esterno prima di essere sperimentato.

In queste due sessioni abbiamo fatto il contrario. Siamo partiti da tre scenari narrativi — Il Girasole, Acquablu, Don Bosco — e abbiamo chiesto ai gruppi di lavorarci senza alcun metodo, senza matrice, senza cornice. Solo il vostro sguardo. È stato solo dopo, quando dal confronto tra i gruppi sono emersi i pattern ricorrenti, che abbiamo nominato ciò che stavate facendo (il risk assessment) e vi abbiamo consegnato il metodo dei cinque passi codificato dalla letteratura. Poi, con quel metodo in mano, siete tornati al vostro scenario a riguardarlo. Un percorso in tre fasi: esperienza, confronto, nominazione.

Prima fase — L'esperienza grezza

Venerdì sera abbiamo lavorato sugli scenari senza alcuna griglia. È stata una fase volutamente disordinata. Alcuni gruppi hanno detto "non sapevamo da che parte cominciare", altri hanno prodotto liste di rischi identificati con grande intuito. Non aveva importanza la qualità del prodotto: aveva importanza il fatto stesso che ognuno di voi si sia messo lì, con il proprio sguardo, senza filtri.

Serve a mobilitare quello che già si sa, a fare emergere le precomprensioni, ad attivare l'intuizione. Ed è qualcosa che non si può saltare: senza questa fase, quello che viene dopo galleggia in astratto.

Seconda fase — La sospensione e il confronto

Fra le due sessioni abbiamo lasciato passare la notte. È una scelta didattica, non solo logistica. La notte ha fatto sedimentare quello che era emerso, senza chiudere il pensiero con una conclusione anticipata. Sabato mattina, invece di ripartire con una lezione, siamo tornati al lavoro con la griglia di confronto cross-scenario: abbiamo messo fianco a fianco quello che i gruppi diversi avevano prodotto su scenari diversi, e abbiamo visto — l'abbiamo visto tutti insieme, non l'ho detto io — che gli stessi pattern ritornavano in contesti radicalmente diversi.

È stato il momento in cui la parola "pattern" ha smesso di essere astratta ed è diventata visibile.

Terza fase — La nominazione e la riapplicazione

Solo a quel punto vi ho detto: quello che avete fatto ha un nome, si chiama risk assessment, ha una tradizione internazionale, si articola in cinque passi. E ve li ho mostrati. Poi vi ho chiesto di tornare al vostro scenario — lo stesso di ieri sera — e di rileggerlo applicando il metodo. Non era una ripetizione. Era una ristrutturazione: quel che intuivate diventava metodo, quel che avevate detto in modo generico diventava misurabile, quel che era rimasto vago diventava documentabile.

Questa fase è cruciale perché in essa il metodo non viene subito, viene riconosciuto. Non è qualcuno che vi dice come dovete pensare: è la formalizzazione di quello che stavate già facendo, resa condivisibile.

Parte II — Il risk assessment: quello che abbiamo visto e il perché

1. Provo una definizione

Se dovessimo formulare adesso, a mente fredda, cosa è il risk assessment organizzativo nel safeguarding, potremmo dire una cosa così: è un processo sistematico e preventivo attraverso il quale un'organizzazione che lavora con minori o adulti vulnerabili identifica le situazioni in cui le proprie attività possono produrre danno, stima la probabilità e la gravità di tale danno, e pianifica misure proporzionate per ridurli a un livello accettabile.

È una definizione asciutta, ma dentro ha tre elementi che meritano di essere isolati perché sono quelli su cui abbiamo lavorato di più.

Primo: l'oggetto è l'organizzazione, non la persona

Il risk assessment che abbiamo fatto non ha valutato singoli individui per stabilire chi fosse pericoloso. Ha valutato le condizioni organizzative — strutture, procedure, spazi, ruoli — per identificare dove l'organizzazione produce o consente il rischio. Questa distinzione è fondamentale perché orienta l'intervento verso la prevenzione sistemica, non verso il giudizio personale.

Il principio sottostante è il "do no harm" organizzativo, mutuato dall'etica medica e applicato alle organizzazioni di servizio. È formulato esplicitamente nei documenti della Pontificia Commissione per la Tutela dei Minori (PCTM, 2023) e nei Catholic Safeguarding Standards (CSSA, 2021): un'organizzazione che si occupa di persone vulnerabili ha il dovere primario di non diventare essa stessa fonte di danno. È un principio che dobbiamo tenere fermo: senza di esso il risk assessment scivola facilmente nel sospetto generalizzato.

Secondo: probabilità e gravità sono distinte

Ve ne siete accorti quasi tutti quando avete affrontato il passo 4. Un evento può essere altamente probabile e di bassa gravità (un ragazzo che si fa male giocando a calcio), oppure raro ma catastrofico (un abuso sessuale da parte di un adulto in posizione di fiducia). Vanno valutati separatamente perché

richiedono strategie diverse: per il primo tipo di rischio serve la formazione sulla sicurezza generale, per il secondo servono procedure rigorose di selezione, controllo e supervisione.

Questa distinzione è radicata nella tradizione della scienza del rischio (Aven, 2016) e codificata nello standard internazionale ISO 31000:2018 sulla gestione del rischio in qualsiasi settore.

Terzo: la misura di mitigazione deve essere proporzionata

Anche questo è emerso nei vostri lavori. Una misura sproporzionata in eccesso — per esempio vietare ogni contatto fisico — impedisce il funzionamento educativo dell'organizzazione e produce danno di ritorno. Una misura sproporzionata in difetto — "più attenzione", "più sensibilità" — non riduce il rischio e crea l'illusione di averlo affrontato. La proporzionalità è il criterio di valutazione della qualità di una misura di mitigazione: né sotto, né sopra.

2. Il metodo dei cinque passi: da dove viene e come si tiene insieme

Il metodo dei cinque passi che vi ho presentato è il modello internazionale standard. È stato codificato a partire dagli anni Duemila da organizzazioni di riferimento nel settore — prima fra tutte Keeping Children Safe — e ripreso da tutti i framework successivi (UNICEF, Save the Children, OMS). Non è un'invenzione italiana e non è un'invenzione ecclesiale: è lo strumento che il mondo usa per fare questo lavoro.

Passo	Operazione	Domanda guida
1	**Stabilire il contesto**	Quale organizzazione? Quali persone vulnerabili? Quali spazi? Quale supervisione?
2	**Identificare i punti di contatto**	In quali momenti e spazi adulti e minori entrano in contatto?
3	**Identificare i rischi specifici**	Per ciascun punto di contatto, cosa concretamente può andare storto?
4	**Valutare probabilità e gravità**	Quanto è probabile (1-5)? Quanto sarebbe grave (1-5)? R = P × I
5	**Misure di mitigazione proporzionate**	Chi fa cosa, entro quando, con quale verifica documentale?

Sulla matrice probabilità × impatto val la pena una nota. Non è un calcolo scientifico. È uno strumento standard della valutazione del rischio in tutti i settori, dal medico all'ingegneristico. Nel safeguarding la utilizziamo come supporto al passo 4 per dare consistenza intersoggettiva al giudizio: anche se la stima rimane qualitativa (nessuno sa davvero se un rischio è "3" o "4"), l'obbligo di attribuire un numero richiede una disciplina di pensiero che riduce l'arbitrio. È un vincolo formale che ci obbliga a essere espliciti su cosa stiamo valutando e perché. Non serve la precisione — serve la disciplina.

3. I pattern che sono emersi: perché non ci hanno sorpreso

Quando abbiamo compilato insieme la griglia di confronto cross-scenario, ci siamo accorti che i tre scenari — pur essendo diversissimi — mostravano gli stessi tipi di problema. La letteratura internazionale sui casi di abuso documentati nelle organizzazioni educative — religiose e non — ha identificato una serie ricorrente di pattern di rischio organizzativo, coerente con l'approccio ecologico alla prevenzione descritto da Wurtele e Kenny (2012). Mettendo a confronto i tre scenari sono emersi sette pattern che si ritrovano nella maggioranza dei casi documentati in letteratura. Sono, sostanzialmente, quelli che voi avete trovato:

- **Selezione informale del personale** — assenza di casellario giudiziale, di referenze documentate, di colloqui strutturati. Apertura a chiunque venga "raccomandato" o sia "di fiducia". Nei tre scenari: il Girasole non chiede casellario ai volontari, Acquablu "chiude un occhio" sui contratti a progetto, Don Bosco non chiede casellario agli animatori.
- **Formazione assente o ridotta** — formazione una tantum, non obbligatoria, non differenziata per ruolo, non aggiornata. Il Girasole fa un incontro all'anno, Acquablu non fa formazione specifica sul safeguarding, Don Bosco fa formazione degli animatori ma su animazione e giochi, non su tutela.
- **Spazi non visibili o isolati** — stanze chiuse, ambienti sotterranei, spazi usati fuori orario senza supervisione. La stanza dei colloqui del Girasole senza finestre interne, la stanza del fisioterapista di Acquablu, i locali sotterranei del Don Bosco.
- **Concentrazione di potere su una figura** — una sola persona che cumula ruoli di selezione, supervisione, valutazione, ascolto. Marta al Girasole, Andrea ad Acquablu, Stefano al Don Bosco: nomi diversi, funzione strutturale identica.
- **Relazioni uno-a-uno fuori controllo** — incontri individuali ricorrenti, accompagnamento privato, mentoring senza protocolli. Il doposcuola individualizzato a casa del Girasole, il "mentoring uno-a-uno" di Acquablu, il tutoraggio nei sotterranei del Don Bosco.
- **Segnali deboli interrotti o non raccolti** — comportamenti cambiati nei minori, ritiri improvvisi, allontanamenti delle famiglie senza spiegazione. Il caso della bambina del Girasole, quello della ragazza di Acquablu, quello del ragazzino del Don Bosco: tre casi diversi, tutti chiusi senza domande.
- **Canali di segnalazione interni alla catena gerarchica** — se l'unico canale per segnalare è il superiore diretto, le segnalazioni che riguardano quella stessa catena non hanno spazio.

Il fatto che questi sette pattern siano emersi in tre contesti diversissimi non è coincidenza. È la conferma che il rischio organizzativo è una categoria strutturale: dipende da come è fatta un'organizzazione, non da chi la abita. Ed è per questo che vale la pena, tornati alle nostre realtà, cercare questi pattern proprio nella nostra parrocchia, nel nostro istituto, nella nostra diocesi.

Una precisazione che ci tengo a fare

Nessuno di questi pattern, da solo, è la prova che si sta verificando un abuso. La presenza di un singolo pattern non dice nulla di quello che sta succedendo davvero. È la concentrazione di più pattern sullo stesso contesto che produce l'esposizione al rischio.

Il risk assessment è uno strumento di prevenzione strutturale, non un dispositivo di accusa. Identifica le condizioni organizzative che vanno modificate, non le persone da escludere. È una distinzione cruciale.

Parte III — L'audit interno: cosa abbiamo scoperto e come si distingue

1. Provo una definizione anche qui

Se dovessimo dire adesso cosa è l'audit interno nel safeguarding, potremmo dire così: è una verifica strutturata, indipendente, basata su evidenze, retrospettiva, condotta su mandato dell'organizzazione stessa per accertare in quale misura ciò che la policy e le procedure dichiarano corrisponda alla prassi reale, e per formulare raccomandazioni che riducano la distanza fra dichiarazione e azione.

Anche qui, la definizione contiene cinque attributi (verifica, indipendente, basata su evidenze, retrospettiva, su mandato dell'organizzazione stessa) che qualificano l'audit interno e lo distinguono da forme di verifica adiacenti. Torniamo fra un attimo su queste distinzioni.

Lo standard professionale di riferimento

L'audit interno come professione è codificato a livello internazionale dagli Standard professionali pubblicati dall'Institute of Internal Auditors (IIA), aggiornati nel 2024 con la pubblicazione dei Global Internal Audit Standards. Sebbene nati nel mondo finanziario e aziendale, questi standard sono ormai applicati anche alle organizzazioni non profit, alle organizzazioni religiose e ai contesti di servizio sociale.

"L'audit interno è un'attività indipendente, obiettiva di assurance e consulenza finalizzata a migliorare l'efficacia dell'organizzazione attraverso un approccio professionale e sistematico" (IIA, 2024).

2. I tre criteri che ci hanno guidato

Durante il Momento 2 ho insistito su tre criteri che qualificano un audit. Tre criteri che, se manca anche solo uno di essi, fanno scivolare l'attività dalla categoria "audit" alla categoria "opinione personale" o "controllo informale". Li rimetto qui per iscritto.

Indipendenza

Chi audita non deve essere chi gestisce. In una diocesi, il referente diocesano per la tutela non può auditare il proprio operato. Serve una figura fuori dalla catena di responsabilità diretta: una funzione di audit interno strutturalmente separata, oppure un consulente esterno incaricato dall'organizzazione, oppure un gruppo di pari di altre diocesi in audit incrociato.

L'indipendenza non è un valore astratto: è una condizione tecnica. Se chi audita ha un interesse al risultato dell'audit — anche solo perché ha contribuito a costruire ciò che sta auditando — la sua

valutazione è inevitabilmente influenzata, anche in buonafede. Non è una questione di onestà personale, è una questione di posizione strutturale.

Evidenza

Questo è il punto che ci ha messo in crisi con la policy di San Vittore. Ogni constatazione deve essere documentabile e verificabile. Non basta l'impressione, serve il documento, il registro, il verbale, la firma, l'intervista trascritta. La fonte dell'audit è la traccia oggettiva di quello che è stato fatto.

La conseguenza pratica è forte, e vale la pena tenerla a mente: ciò che non lascia traccia è auditabile come se non fosse stato fatto. Una formazione svolta ma senza registro presenze, una procedura applicata ma senza protocollo scritto, una segnalazione ricevuta ma senza registrazione — dal punto di vista dell'audit tutto questo equivale al suo non aver avuto luogo. Non significa che non sia effettivamente accaduto: significa che l'organizzazione non può dimostrarlo. E in un audit, quello che non si può dimostrare non conta.

Criteri espliciti

L'auditor dichiara prima — e in modo trasparente — rispetto a quale standard sta valutando. Senza criterio dichiarato non c'è audit, c'è solo opinione personale dell'auditor.

Negli audit di safeguarding, i criteri sono solitamente uno standard pubblico (per esempio gli otto standard internazionali CSSA, o i sei standard della Pontificia Commissione, o gli standard CEI per le diocesi italiane) sovrapposto alla policy specifica dell'organizzazione auditata. La sovrapposizione fra standard e policy genera la griglia di valutazione. Senza uno standard esplicito, l'audit rischia di essere un giudizio soggettivo travestito da metodo.

3. Le distinzioni con concetti adiacenti

Un chiarimento che vale la pena fare, perché nell'esperienza pratica "audit" viene spesso confuso con altre cose. Sono confusioni che producono malintesi, e vale la pena scioglierle.

Cos'è	Differenza dall'audit interno
Audit esterno	Condotto da revisori indipendenti esterni con valenza certificativa, su mandato di un'autorità (per esempio un organismo di certificazione, un'autorità di vigilanza, una conferenza episcopale). L'audit interno è invece commissionato dall'organizzazione stessa.
Ispezione	Ha valenza autoritativa: viene condotta da un organo superiore con potere di intervento diretto (sanzionatorio, sostitutivo, correttivo). L'audit non sanziona: raccomanda. La risposta alle raccomandazioni resta nella libertà dell'organizzazione auditata.
Visita pastorale	Nella tradizione ecclesiale è uno strumento di natura pastorale: ascolto, presenza, comunione, discernimento. Ha funzioni precipuamente spirituali e

	relazionali. L'audit ha funzioni tecniche di verifica documentale. I due strumenti non si sostituiscono, possono integrarsi.
Monitoraggio	È un'attività continua di osservazione di indicatori durante l'operatività. L'audit è invece un'attività puntuale, periodica, con un mandato definito e un report finale. Il monitoraggio è continuo, l'audit è discreto.

4. Come si fa un audit: le fasi in breve

Un audit interno strutturato si articola in fasi che la letteratura professionale (IIA, 2024) descrive con discreta uniformità. Le riporto in forma sintetica per fissare la struttura di quello che, in miniatura, abbiamo fatto sabato mattina.

1. **Pianificazione.** Definizione del mandato, dell'ambito (cosa si audita), degli obiettivi, dei criteri (rispetto a quali standard), delle risorse, dei tempi.
2. **Raccolta delle evidenze.** Analisi documentale (policy, procedure, registri), interviste strutturate a soggetti chiave, eventuali ispezioni sul campo, eventuali questionari.
3. **Valutazione.** Confronto fra le evidenze raccolte e i criteri dichiarati. Identificazione delle aree di conformità, di parziale conformità, di non conformità.
4. **Redazione del report.** Documento formale che descrive metodo, evidenze, valutazioni, raccomandazioni. Le raccomandazioni sono concrete e con destinatari identificati.
5. **Restituzione.** Il report viene presentato all'organizzazione auditata in forma di dialogo, non di sentenza. L'organizzazione ha diritto di replica e di chiarificazione.
6. **Follow-up.** A distanza di tempo (tipicamente 6-12 mesi), si verifica se le raccomandazioni sono state implementate e con quale efficacia.

Senza il follow-up, l'audit perde gran parte del suo valore: rischia di diventare un esercizio cartaceo, un rito senza conseguenze. È nel ciclo audit-raccomandazione-implementazione-follow-up che si costruisce il miglioramento reale.

5. Come stanno insieme risk assessment e audit

Chiudo la parte sull'audit con un'osservazione che tira insieme quello che abbiamo detto finora. I due strumenti sono complementari ma distinti, e insieme formano un sistema di governance del safeguarding.

Il risk assessment è prospettico: guarda al futuro, identifica cosa potrebbe andare storto, pianifica misure di mitigazione. La sua domanda è: cosa rischiamo? L'audit è retrospettivo: guarda al presente e al passato recente, verifica se le misure pianificate sono state effettivamente attuate. La sua domanda è: stiamo davvero facendo quello che diciamo?

Un'organizzazione che fa solo risk assessment senza audit ha buone intenzioni documentate ma non ha modo di sapere se quelle intenzioni si traducono in pratica. Un'organizzazione che fa solo audit

senza risk assessment verifica conformità a procedure che potrebbero essere inadeguate rispetto al rischio reale. I due strumenti si sostengono a vicenda: il risk assessment definisce cosa si dovrebbe fare, l'audit verifica se lo si sta facendo davvero.

Un ultimo appunto per chiudere

Il corso si è chiuso con un'idea che riprende tutto il percorso, ve la ritrascrivo qui perché mi sembra il modo giusto per chiudere anche questi appunti.

Il risk assessment fa la differenza fra una policy ben scritta e un sistema reale di protezione. L'audit fa la differenza fra un sistema dichiarato e un sistema verificato. Fra dichiarazione e azione c'è uno spazio, e quello spazio è esattamente il luogo dove il safeguarding diventa cultura o resta soltanto carta.

La buona intenzione spera. La buona prassi misura. Per la Chiesa, che ha un patrimonio enorme di buone intenzioni, questo è anche una questione di credibilità: le persone che incontriamo si fidano di noi nella misura in cui noi diamo loro strumenti per verificare che siamo davvero degni di quella fiducia.

Il lavoro che avete fatto in queste due sessioni — il vostro sguardo sui tre scenari, la vostra fatica sul passo 4, la vostra capacità di vedere la convergenza dei pattern, la vostra disponibilità a tornare al vostro contesto reale con domande nuove — è la prova che questo percorso è possibile. Non è semplice, non è veloce, ma è praticabile. E questi appunti sono qui perché, quando serviranno, siano lì con voi.

Per continuare a lavorarci — Riferimenti bibliografici essenziali

Una selezione delle fonti su cui abbiamo costruito questi due giorni. Non è una bibliografia esaustiva: è una traccia per chi voglia approfondire.

Fondamenti pedagogici

Bruner, J. S. (1961). The act of discovery. Harvard Educational Review, 31, 21-32.

Dewey, J. (1938). Experience and Education. New York: Macmillan.

Freire, P. (1970). Pedagogy of the Oppressed. New York: Continuum.

Kolb, D. A. (1984). Experiential Learning: Experience as the Source of Learning and Development. Englewood Cliffs: Prentice Hall.

Schön, D. A. (1983). The Reflective Practitioner: How Professionals Think in Action. New York: Basic Books.

Risk assessment e safeguarding

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253(1), 1-13.

Catholic Safeguarding Standards Agency (CSSA) (2021). National Catholic Safeguarding Standards. Bristol: CSSA.

Conferenza Episcopale Italiana (CEI) e Conferenza Italiana Superiori Maggiori (CISM) (2019, aggiornamento 2023). Linee guida per la tutela dei minori e delle persone vulnerabili. Roma: CEI.

ISO 31000:2018. Risk management — Guidelines. Geneva: International Organization for Standardization.

Keeping Children Safe (2014). Child Safeguarding Standards and How to Implement Them. London: KCS.

Pontificia Commissione per la Tutela dei Minori (2023). Universal Guidelines Framework — Linee guida per il safeguarding nella Chiesa cattolica. Città del Vaticano: PCTM.

Wurtele, S. K., & Kenny, M. C. (2012). Preventing childhood sexual abuse: An ecological approach. In P. Goodyear-Brown (Ed.), Handbook of Child Sexual Abuse: Identification, Assessment, and Treatment (pp. 531-565). Hoboken, NJ: Wiley.

Audit interno

European Confederation of Institutes of Internal Auditing (ECIIA) (2023). Position papers on the role of Internal Audit in ESG — banking and industrial/commercial sectors. Brussels: ECIIA.

Institute of Internal Auditors (2020). The IIA's Three Lines Model. Lake Mary: IIA.

Institute of Internal Auditors (2024). Global Internal Audit Standards. Lake Mary: IIA.

—

Fine degli appunti condivisi

Grazie del lavoro fatto insieme.