# SG COMPLIANCE 231

Guida operativa al Modello di Organizzazione, Gestione e Controllo

**Edizione RC2 - 21 agosto 2026**
Dal perimetro del progetto alle prove di attuazione: processi, interviste, risk assessment, protocolli, documenti MOG, OdV, formazione, whistleblowing, adozione e aggiornamento.

| Layer | Oggetto |
|---|---|
| **Progetto** | Ente, perimetro, owner, date di avvio e riesame |
| **Analisi** | Processi, interviste, attivita sensibili, scenari e reati-presupposto |
| **Controlli** | Protocolli, gap, action plan, evidenze e test |
| **MOG** | Parte Generale, Parti Speciali, Codice Etico, disciplina, procedure e versioni |
| **OdV** | Flussi, riunioni, verifiche, rilievi e follow-up |
| **Attuazione** | Formazione, whistleblowing, adozione, audit e aggiornamento |

# 1. Perimetro e logica del sistema 231

Il Modello non coincide con un documento: e un sistema di organizzazione, regole, controlli, vigilanza e prove di attuazione.

## Responsabilita dell’ente

Il progetto deve partire dai rischi concreti dell’ente e dai processi in cui possono verificarsi i reati-presupposto nel suo interesse o vantaggio.

## Sistema, non fascicolo statico

Parte Generale, Parti Speciali, Codice Etico, sistema disciplinare, OdV, formazione, flussi e whistleblowing sono componenti collegate. Un documento ben scritto ma non attuato resta insufficiente sul piano organizzativo.

## Checklist operativa

- perimetro ente definito
- processi concreti
- responsabilita assegnate

**SG Compliance 231 struttura il lavoro e le evidenze, ma non certifica automaticamente l’idoneita o l’efficacia esimente del Modello.**

# 2. Avvio del progetto

L’organo dirigente definisce obiettivi, perimetro, responsabilita, documenti e tempi.

## Project charter

Identificare societa/enti coinvolti, sedi, funzioni, processi, referenti, documenti disponibili, consulenti e tempistiche.

## Governance

Registrare organo amministrativo, deleghe/procure, organigramma, poteri di spesa, controlli esistenti e relazioni con eventuali sistemi ISO, privacy, HSE o altri modelli di compliance.

## Checklist operativa

- delibera/mandato progetto
- owner
- perimetro
- calendario interviste

# 3. Profilo dell’ente

Il risk assessment deve essere contestualizzato a settore, dimensione e modalita operative.

## Dati essenziali

Attivita, ATECO, sedi, personale, governance, rapporti con PA, appalti, finanziamenti, ambiente, sicurezza, sistemi IT, fornitori, intermediari, operativita estera e flussi finanziari.

## Rilevanza

Non tutte le famiglie di reato hanno lo stesso peso per ogni ente. La rilevanza emerge dal collegamento tra attivita effettive e possibili scenari di commissione.

## Checklist operativa

- settore
- governance
- PA
- HSE
- ambiente
- IT
- terze parti

# 4. Process library

Una libreria di processi accelera il lavoro, ma deve essere adattata all’organizzazione reale.

## Aree SG

Governance; rapporti PA; acquisti; vendite; tesoreria; amministrazione/fisco; HR; salute e sicurezza; ambiente; IT; legale/contenzioso; terze parti; operations; proprieta intellettuale; attivita estere.

## Per ogni processo

Owner, descrizione, flussi finanziari, sistemi, terze parti, documenti/procedure e indicazione preliminare di sensibilita 231.

## Checklist operativa

- processi caricati
- owner
- flussi finanziari
- sistemi
- terze parti

# 5. Interviste e raccolta dati

La mappatura non deve limitarsi alle procedure scritte: occorre capire come si lavora davvero.

## Intervista

Associare ogni intervista a un processo o mantenerla trasversale; registrare funzione/intervistato, data, risultanze ed evidenze visionate.

## Validazione

Distinguere bozza, intervista validata e follow-up. Le incoerenze tra procedura e pratica operativa sono input del gap assessment.

## Checklist operativa

- intervistati chiave
- evidenze
- follow-up

# 6. Attivita sensibili

L’attivita sensibile e il punto concreto in cui un rischio-reato puo manifestarsi.

## Scheda rischio

Collegare processo, attivita sensibile, scenario/modalita potenziale, funzioni coinvolte, flussi finanziari e famiglia di reato.

## Esempio metodologico

“Gestione omaggi e sponsorizzazioni” non e un rischio in se: bisogna descrivere chi decide, chi autorizza, come si paga, quali terze parti intervengono e quale scenario illecito si vuole prevenire.

## Checklist operativa

- attivita descritta
- scenario
- funzioni
- flussi

# 7. Catalogo reati-presupposto

Il catalogo e una base normativa da collegare ai processi, non una checklist da segnare integralmente come rilevante.

## Famiglie

SG mantiene le famiglie di reato del D.Lgs. 231/2001 e le collega a parole chiave/aree per aiutare la pre-selezione.

## Aggiornamento

Ogni modifica normativa richiede una revisione del catalogo e una verifica di impatto sui processi dell’ente.

## Checklist operativa

- catalogo aggiornato
- rilevanza motivata
- data revisione

# 8. Scenari di commissione

La qualita del risk assessment dipende dalla qualita dello scenario.

## Scenario utile

Descrive in modo plausibile come il reato potrebbe essere commesso nel processo, da quali funzioni, attraverso quali decisioni, dati, pagamenti o terze parti.

## Scenario inutile

Formule generiche come “possibile corruzione” senza processo, poteri, passaggi decisionali o controlli non aiutano a progettare presidi.

## Checklist operativa

- scenario concreto
- soggetti
- decisioni
- pagamenti
- terze parti

# 9. Metodologia di risk assessment

La legge richiede un’analisi coerente e motivata; la scala numerica SG serve a rendere confrontabili i giudizi.

## Rischio inerente

SG usa probabilita 1-5 e impatto 1-5; il prodotto e un indice interno di priorita.

## Controlli

Si valutano separatamente design e funzionamento su scala 0-5. Il punteggio controllo e la media dei due.

## Residuo SG

Il residuo applica una riduzione massima dell’80% in funzione del punteggio dei controlli. E una metodologia gestionale interna SG, non una formula prescritta dal D.Lgs. 231/2001.

## Checklist operativa

- probabilita motivata
- impatto motivato
- design
- operating effectiveness
- evidenze

**Il numero non sostituisce il giudizio professionale. Ogni valutazione deve avere razionale ed evidenze.**

# 10. Valutazione dei controlli

Un controllo “esistente” non e automaticamente efficace.

## Design

Il controllo e progettato per prevenire/rilevare lo scenario? Ha un owner, una frequenza e regole comprensibili?

## Funzionamento

Esistono prove che venga applicato? Campioni, log, autorizzazioni, verbali, report, firme o altre evidenze.

## Esito

Separare “presente” da “testato” e da “inefficace”. Questa distinzione alimenta il gap e il piano di azione.

## Checklist operativa

- owner
- frequenza
- evidenza
- test

# 11. Gap analysis

Il gap e la distanza tra presidio necessario e presidio effettivo.

## Tipi di gap

Procedura assente; autorizzazione debole; mancanza segregazione; tracciabilita insufficiente; controllo IT mancante; evidenza non conservata; formazione insufficiente; flusso OdV non previsto.

## Priorita

Collegare ogni gap al rischio residuo e trasformarlo in azione con responsabile, data, stato ed evidenza di chiusura.

## Checklist operativa

- gap collegato a rischio
- azione
- owner
- scadenza

# 12. Action plan

La remediation deve essere gestita come progetto, non come elenco di buone intenzioni.

## Campi minimi

Titolo, rischio/gap, responsabile, priorita, scadenza, stato, evidenza attesa e note di chiusura.

## Follow-up

Le azioni scadute o incomplete devono comparire nella dashboard e nei flussi verso organo dirigente/OdV se rilevanti.

## Checklist operativa

- priorita
- responsabile
- scadenza
- evidenza

# 13. Protocolli 231

I protocolli traducono il rischio in regole operative.

## Struttura

Autorizzazioni e soglie; segregazione; tracciabilita/documentazione; controlli IT; monitoraggio/escalation; owner; frequenza; evidenza richiesta.

## Stato

Da implementare, attivo, testato, inefficace. Il protocollo deve poter essere collegato a uno o piu rischi.

## Checklist operativa

- autorizzazione
- segregazione
- tracciabilita
- IT
- monitoraggio
- evidenza

# 14. Flussi finanziari

L’articolazione dei processi finanziari e un presidio trasversale centrale.

## Mappatura

Per ogni processo sensibile descrivere origine della richiesta, approvazione, disposizione, registrazione, riconciliazione e controlli successivi.

## Presidi

Poteri di firma, limiti, doppia autorizzazione, segregazione, anagrafiche fornitori, variazioni IBAN, riconciliazioni e tracciabilita.

## Checklist operativa

- poteri di spesa
- pagamenti
- riconciliazioni
- IBAN
- evidenze

# 15. Parte Generale

La Parte Generale descrive l’architettura comune del sistema 231.

## Contenuti

Quadro normativo; ente e governance; metodologia; adozione; destinatari; sistema documentale; OdV; flussi; sistema disciplinare; formazione; diffusione; aggiornamento.

## Versione

Ogni approvazione deve avere numero/versione, data, organo approvante, data efficacia e archivio della versione precedente.

## Checklist operativa

- versione
- approvazione
- efficacia
- storico

# 16. Parti Speciali

Le Parti Speciali devono nascere dai rischi effettivamente rilevanti.

## Per ogni area

Processi/attivita sensibili; famiglie di reato; scenari; funzioni coinvolte; principi di comportamento; protocolli; evidenze; flussi OdV.

## Generazione SG

La bozza dinamica del plugin aggrega i rischi e i protocolli censiti, ma resta una bozza da validare e adottare formalmente.

## Checklist operativa

- solo aree rilevanti
- protocolli collegati
- flussi OdV

# 17. Codice Etico

Il Codice Etico e un presidio trasversale, non una copia della Parte Generale.

## Contenuti

Valori, integrita, conflitti di interesse, rapporti con PA, fornitori, personale, mercato, dati, sicurezza, ambiente e meccanismi di segnalazione/violazione coerenti con l’organizzazione.

## Diffusione

Registrare approvazione, comunicazione, disponibilita e presa visione nei casi appropriati.

## Checklist operativa

- approvato
- diffuso
- coerente con protocolli

# 18. Sistema disciplinare

Le violazioni devono avere conseguenze definite e coerenti con i diversi destinatari.

## Destinatari

Dipendenti, dirigenti, amministratori, organi di controllo, consulenti, fornitori e altri soggetti rilevanti possono richiedere regole contrattuali differenti.

## Coerenza

Il sistema disciplinare deve coordinarsi con whistleblowing e divieto di ritorsione.

## Checklist operativa

- categorie destinatari
- violazioni
- misure
- clausole terzi

# 19. Organismo di Vigilanza

L’OdV vigila su funzionamento, osservanza e aggiornamento del Modello.

## Governance

Composizione, requisiti, durata, poteri, budget, accesso alle informazioni e regolamento.

## SG

Il modulo gestisce flussi, riunioni/verifiche, agenda, risultanze, azioni e riferimenti alle evidenze. L’OdV non deve essere confuso con chi redige e approva il Modello.

## Checklist operativa

- nomina
- regolamento
- budget
- calendario

# 20. Flussi informativi verso OdV

I flussi devono essere progettati per processo e evento, non raccolti casualmente.

## Periodici

Report acquisti, contenzioso, HSE, ambiente, HR, finanza, audit, IT o altri flussi in base ai rischi.

## Ad evento

Violazioni, ispezioni, incidenti, contenziosi rilevanti, anomalie, operazioni straordinarie, modifiche organizzative o altri trigger definiti dal Modello.

## Checklist operativa

- owner flusso
- frequenza
- destinatario
- evidenza

# 21. Riunioni e verifiche OdV

La vigilanza deve lasciare una traccia ordinata.

## Registro SG

Data, titolo, agenda, risultanze, azioni, stato ed evidenze. I rilievi possono alimentare action plan o proposta di aggiornamento.

## Follow-up

Un rilievo non e chiuso finche non esiste evidenza della remediation o una decisione motivata.

## Checklist operativa

- agenda
- verbale
- rilievi
- follow-up

# 22. Formazione e diffusione

La formazione rende il Modello concretamente attuato.

## Piano

Destinatari, contenuti, data, durata, docente, modalita, presenza e eventuale test/evidenza.

## Risk-based

Le funzioni esposte a rischi specifici devono ricevere formazione coerente con il loro ruolo e i protocolli applicabili.

## Checklist operativa

- destinatari
- ore
- contenuti
- presenze
- evidenza

# 23. Whistleblowing

Il presidio whistleblowing deve essere coordinato con il Modello e il D.Lgs. 24/2023.

## Configurazione SG

Tipo di canale/provider, stato, ultimo test, privacy, antiritorsione, allineamento sistema disciplinare e retention.

## Scelta di sicurezza

SG Compliance 231 non conserva nella tabella di configurazione il contenuto delle segnalazioni. Il canale di whistleblowing deve mantenere la separazione e le garanzie richieste.

## Checklist operativa

- canale
- gestore
- privacy
- anti-ritorsione
- test

**Il fascicolo 231 non deve diventare un archivio indiscriminato di contenuti delle segnalazioni.**

# 24. Sistema documentale MOG

Un modello vivo ha documenti versionati e collegabili alle evidenze.

## Registro

Tipo documento, titolo, versione, stato, owner, data approvazione, efficacia, link/file e note.

## Tipi

Parte Generale, Parte Speciale, Codice Etico, sistema disciplinare, regolamento OdV, procedure/protocolli, organigrammi, deleghe, policy e allegati.

## Checklist operativa

- versione
- stato
- approvazione
- efficacia

# 25. Adozione e delibere

Il Modello e adottato formalmente dall’organo dirigente.

## Registro versioni

Data, versione, tipo evento, organo, riferimento alla delibera, data di efficacia, sintesi delle modifiche.

## Eventi

Prima adozione, revisione ordinaria, aggiornamento normativo, aggiornamento organizzativo o altra modifica significativa.

## Checklist operativa

- organo competente
- delibera
- data efficacia
- versione

# 26. Trigger di aggiornamento

L’aggiornamento e parte del ciclo di vita del Modello.

## Trigger

Nuove norme/reati; variazioni di processi o attivita; nuovi prodotti/servizi; acquisizioni; nuove sedi; modifiche di deleghe; incidenti; violazioni; esiti di audit; rilievi OdV; inefficacia di un protocollo.

## Workflow

Trigger -> impact assessment -> eventuale nuovo risk assessment -> protocolli/documenti -> approvazione -> formazione/diffusione.

## Checklist operativa

- trigger registrato
- impatto
- decisione
- approvazione

# 27. Audit trail e prove di attuazione

La tracciabilita consente di dimostrare non solo cosa e scritto, ma cosa e stato fatto.

## Evidenze

Interviste, documenti visionati, test controlli, azioni, verbali, formazione, flussi, revisioni, approvazioni e audit.

## Registro eventi

SG mantiene lo storico delle operazioni principali del progetto; le evidenze documentali restano collegate e versionate.

## Checklist operativa

- evento
- utente
- data
- oggetto
- evidenza

# 28. Dashboard di completezza

La dashboard aiuta a capire cosa manca nel progetto, non se il Modello sia giuridicamente idoneo.

## Metriche

Processi, rischi, protocolli, azioni aperte, documenti MOG, flussi/riunioni OdV e una percentuale di copertura basata sulla presenza dei componenti.

## Regola SG

Il messaggio “copertura fascicolo != idoneita” deve restare visibile: la qualita dipende dal contenuto, dall’attuazione e dal contesto dell’ente.

## Checklist operativa

- nessun semaforo “esimente”
- gap visibili

# 29. SG Check 231

Il check pubblico e un pre-screening di maturita, non un audit.

## 12 aree

Governance/deleghe; PA/gare; amministrazione-finanza-fisco; acquisti/terze parti; HSE; ambiente; IT; HR; mercato/IP; whistleblowing; OdV; attuazione/aggiornamento.

## 48 domande

L’esito evidenzia aree da approfondire e puo produrre un PDF dell’esito senza salvare le singole risposte.

## Checklist operativa

- linguaggio prudente
- nessuna attestazione

# 30. Uso dell’intelligenza artificiale

L’AI puo accelerare ipotesi e bozze, ma non assumere decisioni professionali.

## Usi utili

Suggerire processi/attivita sensibili da verificare; correlare parole chiave con famiglie di reato; proporre checklist di intervista; riassumere gap; predisporre bozze di Parti Speciali.

## Limiti

Nessuna selezione automatica definitiva dei reati rilevanti; nessuna attestazione di idoneita; nessuna sostituzione dell’OdV; nessuna invenzione di controlli non esistenti.

## Checklist operativa

- evidence-first
- validazione umana
- traccia delle modifiche

# 31. Checklist HSE e ambiente

Salute, sicurezza e ambiente richiedono una mappatura settoriale delle attivita e dei presidi.

## HSE

Ruoli, deleghe, DVR/procedure, formazione, manutenzioni, appalti, incidenti/near miss, vigilanza e flussi OdV.

## Ambiente

Autorizzazioni, rifiuti, emissioni/scarichi se pertinenti, fornitori, registri, emergenze, controlli e non conformita.

## Checklist operativa

- responsabili
- documenti
- controlli
- incidenti
- flussi

# 32. Checklist PA, acquisti e terze parti

Rapporti pubblici e third-party risk sono spesso trasversali.

## PA

Gare, autorizzazioni, contributi, ispezioni, omaggi, spese di rappresentanza, intermediari, tracciabilita dei contatti e poteri di firma.

## Acquisti/terzi

Qualifica, conflitti, beneficial ownership ove pertinente, condizioni economiche, variazioni IBAN, consulenti/intermediari, clausole 231 e monitoraggio.

## Checklist operativa

- due diligence
- autorizzazioni
- tracciabilita
- clausole

# 33. Checklist societario, fiscale e finanza

Le aree amministrative richiedono un collegamento stretto tra responsabilita e controlli.

## Societario

Delibere, comunicazioni, operazioni con parti correlate, capitale, informazioni a soci/controllori e documentazione.

## Fiscale/finanza

Dichiarazioni, versamenti, crediti, fatture, tesoreria, pagamenti, finanziamenti, riconciliazioni, segregazione e supervisione.

## Checklist operativa

- responsabili
- review
- tracciabilita
- riconciliazioni

# 34. Checklist IT, dati e cyber

L’area digitale deve essere analizzata in relazione ai reati e ai processi effettivamente rilevanti.

## Presidi

Accessi, privilegi, segregazione, logging, backup, change management, incident response, fornitori IT, credenziali, pagamenti digitali e dati sensibili.

## Evidenze

Log, ticket, report accessi, audit, test backup, incidenti, revisioni privilegi e attestazioni fornitori ove pertinenti.

## Checklist operativa

- accessi
- log
- backup
- incidenti
- terzi IT

# 35. Checklist HR, mercato e proprieta intellettuale

Le persone e il mercato generano rischi distinti da valutare sul contesto.

## HR

Selezione, assunzione, incentivi, rimborsi, disciplina, formazione, relazioni sindacali, sicurezza e segnalazioni.

## Mercato/IP

Vendite, marketing, concorrenza, marchi/contenuti, licenze, rapporti commerciali e controlli sui materiali utilizzati.

## Checklist operativa

- processi HR
- incentivi
- materiali/licenze
- controlli commerciali

# 36. Fascicolo 231

Il fascicolo deve consentire di ricostruire il progetto e la sua attuazione nel tempo.

## Indice minimo

Perimetro; process map; interviste; catalogo reati; risk assessment; gap/action; protocolli; MOG; Codice Etico; disciplina; OdV; flussi; formazione; whistleblowing; adozioni/versioni; audit/evidenze.

## Qualita

Non basta avere tutti i file: occorre coerenza tra rischio, protocollo, owner, evidenza e vigilanza.

## Checklist operativa

- indice
- versioni
- evidenze
- coerenza

# 37. Checklist di chiusura del progetto

Prima dell’adozione o di una revisione significativa, effettuare un controllo di completezza sostanziale.

## Controlli

Perimetro approvato; processi/interviste completi; rischi motivati; gap trattati o pianificati; protocolli assegnati; documenti coerenti; OdV configurato; flussi definiti; formazione programmata; whistleblowing coordinato; delibera/versione pronte; piano di riesame.

## Checklist operativa

- processi
- rischi
- protocolli
- MOG
- OdV
- formazione
- whistleblowing
- adozione
- riesame

# 38. Fonti e manutenzione

Il modulo deve essere aggiornato senza trasformarsi in un modello standardizzato.

## Baseline

D.Lgs. 231/2001 vigente alla data di revisione; D.Lgs. 24/2023 per il whistleblowing; materiali professionali e linee guida pertinenti al settore dell’ente.

## Regola SG

Aggiornare catalogo reati e template senza sovrascrivere le valutazioni storiche gia approvate; ogni progetto mantiene la propria versione e le proprie evidenze.

## Checklist operativa

- data normativa
- versione catalogo
- storico progetto