



LINEE GUIDA DEL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI

Approvato dal Consiglio di Amministrazione di Avio S.p.A.

- 1ª Edizione Marzo 2004: Delibera del 29 Marzo 2004
- 2ª Edizione Settembre 2008: Delibera del 23 Settembre 2008
- 3ª Edizione Aprile 2015: Delibera del 02 Ottobre 2015
- 4ª Edizione Maggio 2017: Delibera del 28 Giugno 2017
- 5ª Edizione Giugno 2023: Delibera del 20 Giugno 2023

Indice

Premessa	3
1. Riferimenti e principi generali di indirizzo	3
2. Soggetti coinvolti, compiti e responsabilità	6
2.1 Consiglio di Amministrazione	7
2.2 Comitato Controllo e Rischi	7
2.3 Amministratore Delegato e Amministratore incaricato del SCIGR.....	9
2.4 Collegio Sindacale.....	9
2.5 Organismo di Vigilanza ex D.Lgs. 231/2001	10
2.6 Management	10
2.7 Funzioni/Enti di controllo di secondo livello	11
2.7.1 Dirigente Preposto alla redazione dei documenti contabili societari ..	11
2.7.2 Risk Manager	12
2.7.3 Altri presidi con ruolo di secondo livello di controllo	13
2.8 Ente di controllo di terzo livello: Internal Audit	13
3. Attuazione del Sistema di Controllo Interno e Gestione dei Rischi	14
3.1 Gestione dei rischi.....	14
3.2 Attuazione del SCIGR nelle società controllate	19
3.3 Verifica e valutazione continua dell'efficacia del SCIGR	19
3.4 Modalità di coordinamento e collaborazione tra i soggetti coinvolti nel SCIGR	20
3.5 Flussi informativi tra i soggetti coinvolti nel SCIGR	21

Premessa

Il Sistema di Controllo Interno e di Gestione dei Rischi ("**SCIGR**") rappresenta un elemento qualificante ed essenziale della Corporate Governance delle società del Gruppo Avio ("**Gruppo**") ed assume un ruolo fondamentale nella individuazione, misurazione, gestione e monitoraggio dei rischi significativi, rendendoli compatibili con gli obiettivi strategici aziendali e contribuendo quindi alla creazione di valore nel medio-lungo periodo.

Un efficace SCIGR favorisce l'assunzione di decisioni consapevoli e concorre ad assicurare la salvaguardia e la protezione degli investimenti degli azionisti e dei beni delle società, l'efficienza e l'efficacia dei processi e delle operazioni aziendali, nonché l'affidabilità delle informative finanziarie, il rispetto di leggi, norme e regolamenti di riferimento, dello Statuto Sociale e degli strumenti normativi interni.

Le presenti Linee Guida, emanate da Avio S.p.A. ("**Avio**" o "**Società**" o "**Capogruppo**") nell'ambito del proprio ruolo di indirizzo e coordinamento delle società del Gruppo, hanno l'obiettivo di rappresentare sinteticamente in modo organico tutti i diversi aspetti del SCIGR completamente applicabili ad Avio, e alle quali devono coerentemente far riferimento tutte le società controllate del Gruppo, seppur nella loro autonoma responsabilità di definizione e funzionamento del proprio SCIGR. In particolare, le società controllate ricevono le presenti Linee Guida e le adottano adeguandole, ove necessario, alle peculiarità della propria impresa e tenendo conto della disciplina ad esse applicabile (ad esempio specifiche normative del settore di riferimento).

1. Riferimenti e principi generali di indirizzo

Il SCIGR di Avio è conforme ai principi contenuti nella vigente edizione del Codice di Corporate Governance delle società quotate promosso da Borsa Italiana S.p.A. ("**Codice**") e più in generale, alle best practices esistenti in ambito nazionale e internazionale.

Le presenti linee guida dettano da un lato i principi generali secondo i quali viene condotta la gestione dei principali rischi del Gruppo, coerentemente con gli obiettivi strategici individuati, dall'altro le modalità di coordinamento tra i soggetti coinvolti al fine di massimizzare l'efficacia e l'efficienza del SCIGR stesso.

Il SCIGR è, in particolare, costituito da un insieme di regole, procedure e strutture organizzative volte a contribuire in modo proattivo, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, alla salvaguardia del patrimonio sociale del Gruppo Avio, ad una efficiente ed efficace conduzione del Gruppo in linea con le strategie aziendali definite dal Consiglio di Amministrazione della Capogruppo, all'attendibilità, accuratezza e affidabilità delle informazioni fornite agli Organi Sociali ed al mercato e, più in generale, al rispetto delle vigenti disposizioni legislative e regolamentari.

Per la definizione del proprio SCIGR, il Gruppo Avio si è ispirato alle best practices vigenti e in particolare allo standard internazionale "Enterprise Risk Management-Integrated Framework" ("ERM Integrated Framework"), predisposto ed aggiornato dall'organismo americano "Committee of Sponsoring Organizations of the Treadway Commission"

(COSO); tale framework è noto anche come “COSO Report” o “COSO ERM”.¹



I 5 componenti del framework sono indissolubilmente legati fra loro; per funzionare devono esserci tutti, altrimenti l'intera struttura si sfalda.

Governance e cultura: definisce l'approccio dell'organizzazione nella gestione dei rischi di Gruppo definendo le relative responsabilità. La cultura si riferisce ai valori etici, ai comportamenti nonché alla comprensione dei rischi della Società.

Strategia e impostazione degli obiettivi: la strategia, gli obiettivi e i rischi dell'impresa sono correlati tra loro nel più ampio processo di pianificazione strategica. Il risk appetite è definito e allineato alla strategia; gli obiettivi di business declinano la strategia e servono come base per l'identificazione, valutazione e risposta ai rischi.

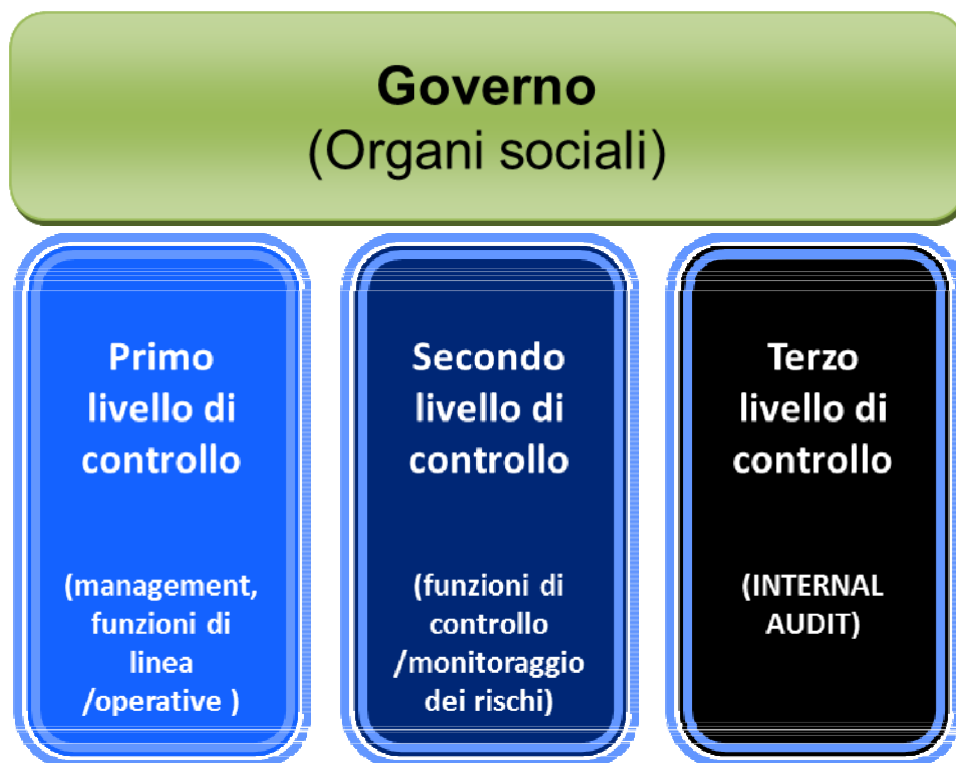
Performance: i rischi che possono incidere sul raggiungimento della strategia e degli obiettivi aziendali devono essere identificati e valutati. I rischi sono classificati per gravità in relazione al risk appetite. L'organizzazione individua le risposte al rischio e valuta il livello di rischio che ha assunto complessivamente. I risultati di questo processo sono comunicati ai principali stakeholder.

Riesame e revisione: nell'analisi delle performance, un'organizzazione può valutare le componenti dell'ERM anche alla luce di modifiche sostanziali.

Informazione, comunicazione e reporting: l'ERM richiede un processo continuo per ottenere e condividere le informazioni necessarie, sia da fonti interne che esterne, che confluiscono verso l'alto, verso il basso e all'interno dell'organizzazione.

Il SCIGR, quale parte integrante dell'attività d'impresa, coinvolge e si applica pertanto a tutta la struttura organizzativa delle società del Gruppo, cioè a ciascuno per il proprio ambito di responsabilità: dal Consiglio di Amministrazione e Amministratore Delegato di Avio e delle società dalla stessa controllate, al Management di Gruppo ed al personale aziendale.

Il Sistema di Controllo Interno e Gestione dei Rischi, in linea con le normative e le best practice di riferimento, si articola sui seguenti livelli:



Governo

Di competenza/responsabilità degli Organi sociali: definisce, approva e verifica il Sistema e Controllo Interno e Gestione dei Rischi.

Primo livello di controllo

Di competenze/responsabilità delle linee/strutture operative: identifica, valuta, gestisce e monitora i rischi di competenza in relazione ai quali individua e attua specifiche azioni di trattamento dirette ad assicurare il corretto svolgimento delle operazioni.

È costituito dall'insieme delle attività di controllo che le singole unità operative svolgono sui propri processi al fine di assicurare il corretto svolgimento delle operazioni. Tali attività di controllo sono demandate alla responsabilità primaria del management operativo e sono considerate parte integrante di ogni processo aziendale. Le strutture operative sono, quindi, le prime responsabili del processo di controllo interno e di gestione dei rischi. Nel corso dell'operatività giornaliera tali strutture sono chiamate a identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi e le procedure interne applicabili.

Secondo livello di controllo

Affidato a funzioni autonome, indipendenti e distinte da quelle operative; esse concorrono alla definizione delle politiche di governo e del processo di gestione dei rischi (individuazione, valutazione e controllo). A tale livello si monitorano i rischi aziendali, si propongono le linee guida sui relativi sistemi di controllo e si verifica l'adeguatezza degli stessi al fine di assicurare efficienza ed efficacia delle operazioni, adeguato controllo dei rischi, prudente conduzione del business, affidabilità delle informazioni, conformità a leggi, regolamenti e procedure interne.

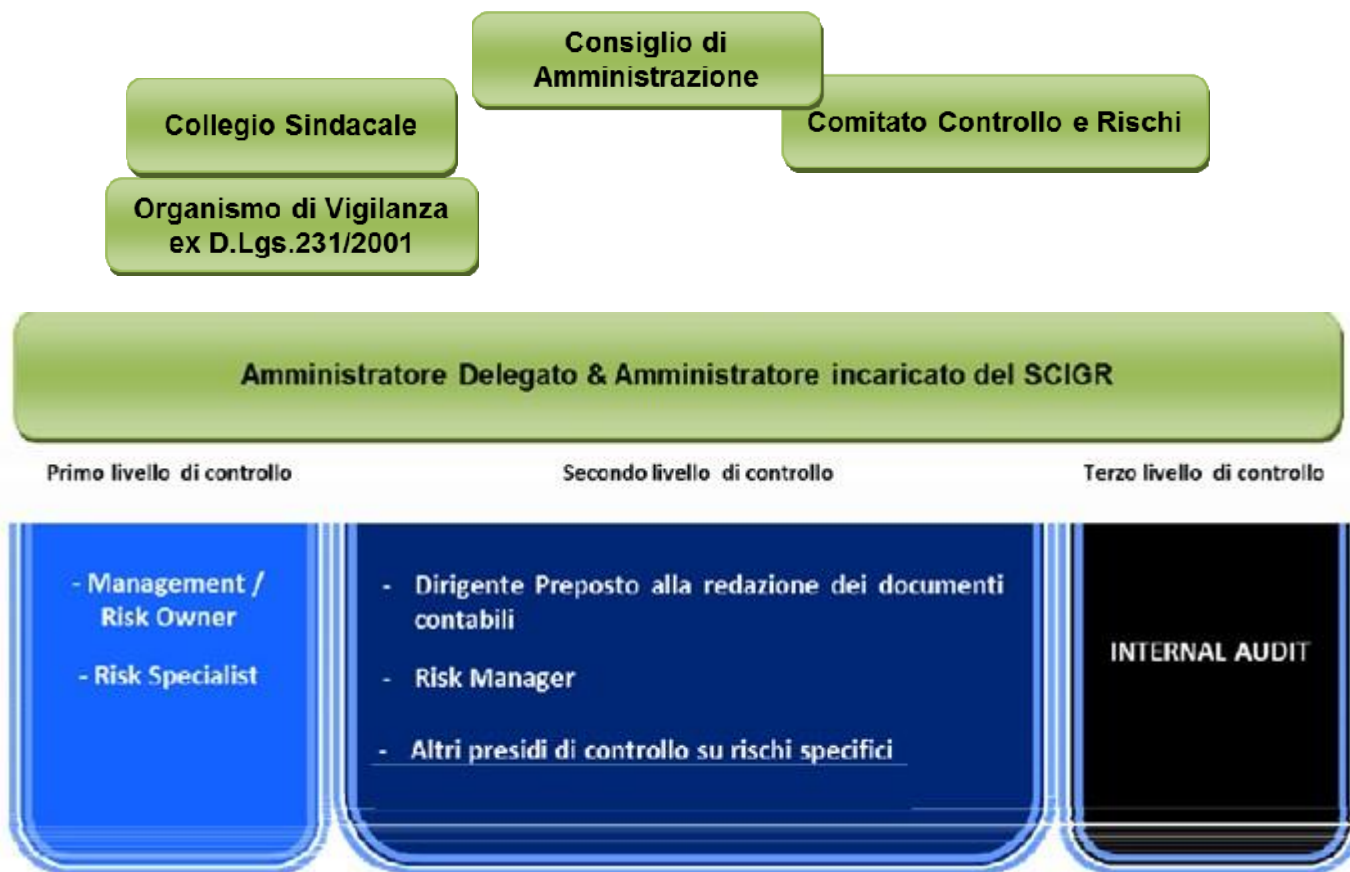
Terzo livello di controllo

Di competenza/responsabilità della funzione di Internal Audit: fornisce assurance indipendente sull'adeguatezza ed effettiva operatività del primo e secondo livello di controllo e, in generale, sul SCIGR. Ha la finalità di valutare la completezza, l'adeguatezza, la funzionalità e l'affidabilità in termini di efficienza ed efficacia del sistema dei controlli interni nonché di individuare violazioni delle procedure e delle norme applicabili.

2. Soggetti coinvolti, compiti e responsabilità

Il SCIGR è un sistema integrato svolto da una pluralità di organi e funzioni aziendali, le cui componenti risultano tra loro coordinate e interdipendenti e caratterizzate da complementarità nelle finalità perseguite, nelle caratteristiche di impianto e nelle regole di funzionamento.

Di seguito si riporta la vista di sintesi degli attori del SCIGR rispetto al modello di corporate governance e all'architettura basata sui tre livelli di controllo.



I compiti e le responsabilità spettanti agli attori del SCIGR, riportate nei paragrafi successivi, sono definiti sulla base di quanto previsto da normative e regolamenti applicabili (a titolo esemplificativo Codice di Corporate Governance, D.Lgs 231/2001, L. 262/2005), disposizioni e normative interne e best practices di riferimento.

2.1 Consiglio di Amministrazione

Il Consiglio di Amministrazione (“**CdA**”) svolge il ruolo ed i compiti previsti dal Codice di Corporate Governance e, nell’ambito della propria principale funzione di indirizzo e di valutazione dell’adeguatezza del SCIGR, rappresenta l’Organo avente la responsabilità finale del Sistema stesso.

Ai fini di un adeguato svolgimento dei compiti demandati alla sua responsabilità, il CdA:

- a) istituisce il Comitato Controllo e Rischi attribuendogli le funzioni consultive e propositive in relazione al SCIGR previste dal Codice di Corporate Governance, ne nomina i componenti e tra questi, il Presidente del Comitato stesso;
- b) nomina l’Amministratore Delegato della società quale Amministratore incaricato dell’istituzione e del mantenimento di un efficace SCIGR;

con il supporto dei quali effettua le valutazioni ed assume le decisioni relative al SCIGR e assicura che i compiti e le responsabilità siano allocati in modo chiaro ed appropriato, e che il Responsabile dell’Internal Audit, l’Organismo di Vigilanza ex D.Lgs. 231/2001 e il Dirigente Preposto alla redazione dei documenti contabili societari, siano dotati di risorse adeguate allo svolgimento delle loro attività e godano di un appropriato grado di autonomia all’interno della struttura.

Quindi il CdA, previo parere del Comitato Controllo e Rischi:

- a) definisce, emette ed aggiorna le presenti linee guida, in modo che i principali rischi risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati, determinando, inoltre, il grado di compatibilità dei medesimi con una gestione dell’impresa coerente con gli obiettivi strategici individuati;
- b) valuta, con cadenza almeno annuale, l’adeguatezza del SCIGR rispetto alle caratteristiche dell’impresa e al profilo di rischio assunto, nonché la sua efficacia;
- c) su proposta dell’Amministratore incaricato del SCIGR, previo parere favorevole del Comitato Controllo e Rischi, sentito il Collegio Sindacale, nomina (e revoca) il Responsabile Internal Audit (Chief Audit Officer o CAO) e ne definisce la remunerazione coerentemente con quanto stabilito dalle politiche aziendali, assicurando che lo stesso sia dotato di adeguate risorse per l’espletamento delle proprie funzioni e la copertura delle proprie responsabilità;
- d) approva, con cadenza almeno annuale, il piano di lavoro predisposto dal Chief Audit Officer, sentito il Collegio Sindacale e l’Amministratore incaricato del SCIGR, ed esamina le risultanze dell’attività svolta, valutandone l’adeguatezza;
- e) descrive, nella relazione sul governo societario, le principali caratteristiche del SCIGR e le modalità di coordinamento tra i soggetti in esso coinvolti, esprimendo la propria valutazione sull’adeguatezza dello stesso; valuta, sentito il Collegio Sindacale, i risultati esposti dal revisore legale nella eventuale lettera di suggerimenti e nella relazione sulle questioni fondamentali emerse in sede di revisione legale.

2.2 Comitato Controllo e Rischi

Il Comitato Controllo e Rischi ha funzioni consultive e propositive rispetto al Consiglio di Amministrazione, con il compito di supportarlo attraverso un’adeguata attività istruttoria, nelle valutazioni e nelle decisioni relative al SCIGR, nonché in quelle relative all’approvazione delle relazioni finanziarie periodiche.

In particolare, il Comitato Controllo e Rischi, in conformità a quanto previsto nel Codice di Corporate Governance, nell'assistere il Consiglio di Amministrazione:

- c) valuta, unitamente al Dirigente Preposto alla redazione dei documenti contabili societari, e sentiti il revisore legale e il collegio sindacale, il corretto utilizzo dei principi contabili e la loro omogeneità ai fini della redazione del bilancio consolidato;
- d) esprime pareri su specifici aspetti inerenti alla identificazione dei principali rischi aziendali;
- e) esamina le relazioni periodiche, aventi per oggetto la valutazione del sistema di controllo interno e di gestione dei rischi, e quelle di particolare rilevanza predisposte dalla funzione di Internal Audit;
- f) monitora l'autonomia, l'adeguatezza, l'efficacia e l'efficienza della funzione di Internal Audit;
- g) può chiedere alla funzione di Internal Audit lo svolgimento di verifiche su specifiche aree operative, dandone contestuale comunicazione al Presidente del Collegio Sindacale; a fini di coordinamento, ne dà altresì comunicazione al Presidente del Consiglio di Amministrazione e all'Amministratore incaricato del sistema di controllo interno e di gestione dei rischi, salvo il caso in cui l'oggetto della richiesta di verifica riguardi specificamente l'attività di tali soggetti;
- h) riferisce al Consiglio di Amministrazione, almeno trimestralmente, in occasione dell'approvazione della relazione finanziaria annuale e semestrale, nonché in occasione dell'approvazione delle relazioni finanziarie periodiche aggiuntive (trimestrali), sull'attività svolta nonché sull'adeguatezza del sistema di controllo interno e di gestione dei rischi;
- i) supporta, con un'adeguata attività istruttoria, le valutazioni e le decisioni del Consiglio di Amministrazione relative alla gestione di rischi derivanti da fatti pregiudizievoli di cui il Consiglio di Amministrazione sia venuto a conoscenza;
- j) svolge gli ulteriori compiti ad esso attribuiti dal Codice di Corporate Governance o dal Consiglio di Amministrazione.

Il Comitato Controllo e Rischi rilascia, inoltre, il proprio parere preventivo al Consiglio di Amministrazione:

- (i) ai fini della definizione delle linee di indirizzo del sistema di controllo interno e di gestione dei rischi, in modo che i principali rischi afferenti la Società e le sue controllate risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati, e della determinazione del grado di compatibilità di tali rischi con una gestione dell'impresa coerente con gli obiettivi strategici individuati, tenuto conto anche dei rischi che possono assumere rilievo nell'ottica della sostenibilità nel medio-lungo periodo dell'attività della Società;
- (ii) ai fini della valutazione, con cadenza almeno annuale, dell'adeguatezza del sistema di controllo interno e di gestione dei rischi rispetto alle caratteristiche dell'impresa e al profilo di rischio assunto, nonché della sua efficacia;
- (iii) ai fini dell'approvazione, con cadenza almeno annuale, del piano di lavoro predisposto dal responsabile della funzione Internal Audit ferma restando l'esigenza per il Consiglio di Amministrazione di sentire altresì il Collegio Sindacale e l'amministratore incaricato del sistema di controllo interno e gestione dei rischi;
- (iv) ai fini della descrizione, contenuta nella relazione sul governo societario, delle principali caratteristiche del sistema di controllo interno e di gestione dei rischi e sulle modalità di coordinamento tra i soggetti in esso coinvolti, nonché della

- valutazione sull'adeguatezza del sistema stesso;
- (v) ai fini della valutazione dei risultati esposti dalla società di revisione nella eventuale lettera di suggerimenti e nella relazione sulle questioni fondamentali emerse in sede di revisione legale, ferma restando l'esigenza per il Consiglio di Amministrazione di sentire altresì il Collegio Sindacale;
 - (vi) sulla proposta relativa alla nomina, alla revoca e alla definizione, coerentemente con le politiche aziendali, della remunerazione del responsabile della funzione di Internal Audit, nonché sull'adeguatezza delle risorse assegnate a quest'ultimo per l'espletamento delle proprie responsabilità.

2.3 Amministratore Delegato e Amministratore incaricato del SCIGR

L'Amministratore Delegato della società, oltre ai poteri necessari per compiere tutti gli atti operativi pertinenti l'attività sociale, è stato nominato quale amministratore incaricato dell'istituzione e del mantenimento di un efficace sistema di controllo interno e gestione dei rischi ("Amministratore incaricato del SCIGR").

Conformemente al Codice di Corporate Governance, l'Amministratore incaricato:

- cura l'identificazione dei principali rischi aziendali, tenendo conto delle caratteristiche delle attività svolte dalla Società e dalle sue controllate, e li sottopone periodicamente all'esame del Consiglio di Amministrazione;
- dà esecuzione alle linee di indirizzo definite dal Consiglio di Amministrazione, curando la progettazione, realizzazione e gestione del sistema di controllo interno e di gestione dei rischi, verificandone costantemente l'adeguatezza e l'efficacia, nonché curandone l'adattamento alla dinamica delle condizioni operative e del panorama legislativo e regolamentare;
- può affidare alla funzione di Internal Audit lo svolgimento di verifiche su specifiche aree operative e sul rispetto delle regole e procedure interne nell'esecuzione di operazioni aziendali, dandone contestuale comunicazione al Presidente del Consiglio di Amministrazione, al Presidente del Comitato Controlli e Rischi e al Presidente del Collegio Sindacale;
- riferisce tempestivamente al Comitato Controllo e Rischi (o al Consiglio di Amministrazione) in merito a problematiche e criticità emerse nello svolgimento della propria attività o di cui abbia avuto notizia, affinché il Comitato Controllo e Rischi (o il Consiglio) possa prendere le opportune iniziative.

2.4 Collegio Sindacale

Il Collegio Sindacale svolge i compiti ad esso attribuiti dalla legge e dallo statuto sociale. In particolare, vigila:

- sull'osservanza delle norme di legge e dello Statuto;
- sul rispetto dei principi di corretta amministrazione e di adeguatezza dell'assetto organizzativo;
- sulla completezza, adeguatezza ed efficacia del SCIGR;
- sulla completezza, adeguatezza ed efficacia del sistema amministrativo- contabile e sull'affidabilità di quest'ultimo nel rappresentare correttamente i fatti di gestione;
- sull'adeguatezza delle disposizioni impartite alle società controllate al fine del corretto adempimento degli obblighi di comunicazione previsti.

A tal proposito, il Collegio Sindacale in linea con il ruolo e i compiti previsti dal Codice di Corporate Governance:

- condivide tempestivamente con il Comitato Controllo e Rischi le informazioni rilevanti per l'espletamento dei rispettivi compiti;
- ha la facoltà di avvalersi della funzione Internal Audit per lo svolgimento di verifiche su specifiche aree operative od operazioni aziendali.

2.5 Organismo di Vigilanza ex D.Lgs. 231/2001

L'Organismo di Vigilanza ("OdV") viene nominato dal Consiglio di Amministrazione ed è dotato di adeguate risorse finanziarie per lo svolgimento delle proprie attività, tra le quali:

- verificare l'efficacia e l'adeguatezza del Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001 (di seguito il "Modello" o "MOGC") ovvero l'idoneità dello stesso a prevenire il verificarsi dei reati di cui al D.Lgs. 231/2001 sulla base di un piano annuale di verifiche presentato al Consiglio di Amministrazione;
- verificare l'adeguatezza delle soluzioni organizzative adottate per l'attuazione del Modello;
- predisporre una relazione almeno semestrale inviata al Comitato Controllo e Rischi, al Collegio Sindacale e al Consiglio di Amministrazione in merito alle proprie attività informando gli stessi sulle eventuali violazioni che abbia riscontrato riguardo al Modello.

All'OdV devono essere fornite tutte quelle informazioni che riguardano, anche indirettamente, la commissione o i tentativi di reato e di elusione del Modello nonché, in generale, i comportamenti a rischio reato.

2.6 Management

Tutti i dipendenti del Gruppo, in funzione dei compiti loro affidati nell'organizzazione aziendale, assicurano un efficace funzionamento del Sistema di Controllo Interno e Gestione dei Rischi, come parte della loro responsabilità nel raggiungimento degli obiettivi. Rappresentano, a tutti i livelli dell'organizzazione, i responsabili del primo livello di controllo del sistema.

Essi, pertanto, devono avere la necessaria conoscenza, preparazione e capacità per agire ed operare nell'ambito del SCIGR e deve essere loro consentito di adempiere ai compiti conseguenti al proprio ruolo ed assolvere alle proprie responsabilità.

Questo implica, pertanto, il diritto ed il dovere di ogni singolo dipendente di avere piena conoscenza e comprensione della società in cui opera e del Gruppo, dei meccanismi operativi, degli obiettivi, dei mercati in cui opera e dei rischi cui è quotidianamente esposto.

Nel corso dell'operatività giornaliera, il Management è chiamato ad identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi e delle procedure interne applicabili.

2.7 Funzioni/Enti di controllo di secondo livello

Le funzioni di controllo di secondo livello sono figure con compiti specifici e responsabilità di controllo su diverse aree/tipologie di rischio. Tali funzioni monitorano i rischi aziendali, propongono le linee guida sui relativi sistemi di controllo e verificano l'adeguatezza degli stessi al fine di assicurare efficienza ed efficacia delle operazioni, adeguato controllo dei rischi, prudente conduzione del business, affidabilità delle informazioni, conformità a leggi, regolamenti e procedure interne.

Le funzioni preposte a tali controlli sono autonome e distinte da quelle operative; esse concorrono alla definizione delle politiche di governo dei rischi e del processo di gestione dei rischi.

2.7.1 Dirigente Preposto alla redazione dei documenti contabili societari

Ai sensi dell'articolo 154-bis del TUF, il dirigente preposto sarà tenuto:

- (i) ad attestare che gli atti e le comunicazioni della società diffusi al mercato e relativi all'informativa contabile anche infra-annuale della società siano corrispondenti alle risultanze documentali, ai libri e alle scritture contabili;
- (ii) a predisporre adeguate procedure amministrative e contabili per la formazione del bilancio di esercizio e del bilancio consolidato, nonché di ogni altra comunicazione di carattere finanziario;
- (iii) ad attestare, congiuntamente all'Amministratore Delegato, con apposita relazione allegata al bilancio di esercizio, al bilancio semestrale abbreviato e al bilancio consolidato, tra l'altro, l'adeguatezza e l'effettiva applicazione delle procedure sub (ii), nel corso del periodo cui si riferiscono i documenti e ad attestare, altresì, la corrispondenza di questi alle risultanze dei libri e delle scritture contabili e la loro idoneità a fornire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria della società e dell'insieme delle società eventualmente incluse nel consolidamento.

Quanto sopra, attribuendo a tal fine allo stesso i seguenti poteri:

- (a) accesso libero ad ogni informazione ritenuta rilevante per l'assolvimento dei propri compiti, sia all'interno della società, sia all'interno delle eventuali società del gruppo facente capo alla società;
- (b) partecipazione alle riunioni del Consiglio di Amministrazione che prevedano la trattazione di materie rientranti nelle sue competenze;
- (c) facoltà di dialogare con ogni organo amministrativo e di controllo della società e delle società controllate;
- (d) facoltà di approvare le procedure aziendali, quando esse hanno impatto sul bilancio, sul bilancio consolidato o sugli altri documenti soggetti ad attestazione;
- (e) partecipazione al disegno dei sistemi informativi che abbiano impatto sulla situazione economica, patrimoniale e finanziaria della società;
- (f) possibilità di utilizzo dei sistemi informativi.

Al fine di consentire al Consiglio di Amministrazione un corretto esercizio dei propri poteri di vigilanza, il dirigente preposto dovrà, inoltre, riferire almeno trimestralmente al Consiglio in merito alle attività svolte, nonché in merito alle eventuali criticità emerse.

2.7.2 Risk Manager

Avio si è dotata di una struttura trasversale dedicata specificatamente alla gestione dei rischi strategici generali del Gruppo.

Tutti i processi realizzativi che concorrono alla progettazione, sviluppo e realizzazione di un prodotto o servizio, nonché i processi trasversali ovvero di supporto, inoltre, sono oggetto di mappatura nell'ambito del Sistemi di Gestione della Qualità, rispondente allo standard ISO 9001:2015 e EN 9100:2018.

In relazione alla gestione di rischi specifici, gli altri Sistemi di Gestione dell'azienda (Incidenti Rilevanti, Salute e Sicurezza, Ambiente) hanno loro procedure dedicate per la gestione di tali rischi specifici, rispondenti a precise indicazioni di legge e/o di sistema dedicato.

Il Gruppo adotta un modello di gestione integrata dei rischi (Enterprise Risk Management - ERM) che coinvolge, in ragione delle specifiche competenze, l'intera organizzazione aziendale. L'obiettivo principale delle attività di ERM è garantire un'ottimale identificazione, misurazione, gestione e monitoraggio dei rischi aziendali.

Il modello ERM considera tutte le tipologie di rischio che possono pregiudicare il raggiungimento degli obiettivi strategici aziendali.

I rischi vengono classificati in diverse categorie in funzione del tipo di impatto sulle attività di Avio.

Le principali figure aziendali responsabili del processo di gestione dei rischi sono:

- Risk Manager: è la figura responsabile del coordinamento e della gestione dell'intero processo. Riporta direttamente all'Amministratore incaricato del SCIGR e garantisce la corretta applicazione delle modalità di gestione dei rischi aziendali e ne richiede, ove necessario, le adeguate riserve o coperture assicurative.
- Risk Owners: sono i Responsabili che coprono tutte le aree di possibile rischio aziendale e, pertanto, sono i primi livelli della Direzione Generale.
- Risk Specialists: sono, nell'ambito dell'area di propria competenza, coloro che conoscono le modalità di gestione del rischio, ne sanno analizzare e valutare gli impatti e sono in grado di proporre ed attuare adeguate azioni di mitigazione.

In particolare, è compito del Risk Manager:

- assicurare la definizione delle metodologie e degli strumenti funzionali al processo di risk management di Gruppo per individuare, misurare, rappresentare e monitorare i principali rischi e i relativi piani di trattamento;
- assicurare le attività di risk assessment e di monitoraggio dei principali rischi di Gruppo, supportando il management nell'identificazione, valutazione e trattamento dei rischi e, ove possibile e opportuno, nella definizione dei relativi indicatori e nello svolgimento di analisi quali-quantitative e approfondimenti;
- curare l'elaborazione del piano di lavoro e del reporting periodico all'Amministratore incaricato del SCIGR e al Comitato Controllo e Rischi in relazione alle attività di assessment e monitoraggio dei rischi a livello di Gruppo e l'elaborazione della documentazione predisposta per i comitati direzionali e per gli organi di amministrazione e controllo.

Il Risk Manager redige una sintesi riepilogativa delle attività svolte e dei principali rischi aziendali individuati, valutati ed oggetto di monitoraggio. Le risultanze di tali relazioni sono presentate, con periodicità definite, all'Amministratore Incaricato del SCIGR, all'Amministratore Delegato, al Comitato Controllo e Rischi, nonché al

Collegio Sindacale ed al Consiglio di Amministrazione.

2.7.3 Altri presidi con ruolo di secondo livello di controllo

In Avio sono presenti altri presidi organizzativi di secondo livello di controllo, dedicati a ciò anche in via non esclusiva.

Tali presidi monitorano specifici rischi aziendali (quali, ad esempio, quelli connessi alla gestione della salute e sicurezza sui luoghi di lavoro ex D.Lgs. 81/2008, della security, degli aspetti ambientali, della frode, della sicurezza informatica, della qualità, delle segnalazioni in materia di "whistleblowing", etc.), propongono le linee guida sui relativi sistemi di controllo e verificano l'adeguatezza degli stessi al fine di assicurare efficienza ed efficacia delle operazioni, adeguato controllo dei rischi, affidabilità delle informazioni, conformità a leggi, regolamenti e procedure interne. Tali presidi di controllo di secondo livello si coordinano con la funzione di Risk Management aziendale attraverso modalità operative specifiche e scambio di flussi informativi.

All'interno di questi ulteriori presidi, in riferimento alla gestione delle segnalazioni, Avio ha adottato, ai sensi del D.Lgs. 24/2023 ("Decreto Whistleblowing"), la Procedura Whistleblowing, che disciplina il processo di ricezione, analisi e trattamento delle segnalazioni e che, in conformità a quanto previsto dalla normativa in parola, prevede un canale di segnalazione interno idoneo a garantire la riservatezza dell'identità del segnalante (la "Procedura Whistleblowing"). Pertanto, le Segnalazioni devono essere inoltrate mediante il canale dedicato e messo a disposizione dal Gruppo Avio e, in particolare, utilizzando la piattaforma on-line all'indirizzo <https://areariservata.mygovernance.it/#!/WB/avio> accessibile ai soggetti deputati alla gestione delle segnalazioni in conformità al D.Lgs. 24/2023.

Per ogni altro dettaglio sulle modalità e gestione delle Segnalazioni si rimanda alla Procedura Whistleblowing consultabile al seguente link <https://www.avio.com/it/corporate-governance>

2.8 Ente di controllo di terzo livello: Internal Audit

L'Internal Audit è responsabile dell'attività di controllo di terzo livello e pertanto gli viene riconosciuta una posizione rilevante nel SCIGR. Come funzione di controllo di terzo livello gli è affidato il compito di fornire assurance indipendente sul SCIGR finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione.

L'Internal Audit è incaricato di verificare che il SCIGR sia funzionante ed adeguato rispetto alle dimensioni e all'operatività del Gruppo, verificando, in particolare, che il Management abbia identificato i principali rischi, che gli stessi siano stati valutati con modalità omogenee e che siano state definite e attuate le opportune azioni di mitigazione. Verifica, inoltre, che i rischi siano gestiti coerentemente con quanto deliberato dal Consiglio di Amministrazione, con le norme esterne e con le regole interne al Gruppo.

Il Responsabile della Funzione Internal Audit non è responsabile di alcuna area operativa, ha accesso diretto a tutte le informazioni utili per lo svolgimento delle proprie attività, riporta gerarchicamente al Consiglio di Amministrazione e assicura le informazioni dovute al Comitato Controllo e Rischi ed al Collegio Sindacale.

La funzione di Internal Audit è affidata ad un soggetto esterno alla società dotato di adeguati requisiti di professionalità, indipendenza e organizzazione.

Il piano annuale di lavoro dell’Internal Audit (“**Piano di Audit**”), basato su un processo strutturato di analisi e prioritizzazione dei principali rischi, analogamente a quanto previsto per il budget, è soggetto all’approvazione del Consiglio di Amministrazione, previo parere del Comitato Controllo e Rischi, sentito il Collegio Sindacale e l’Amministratore incaricato del SCIGR.

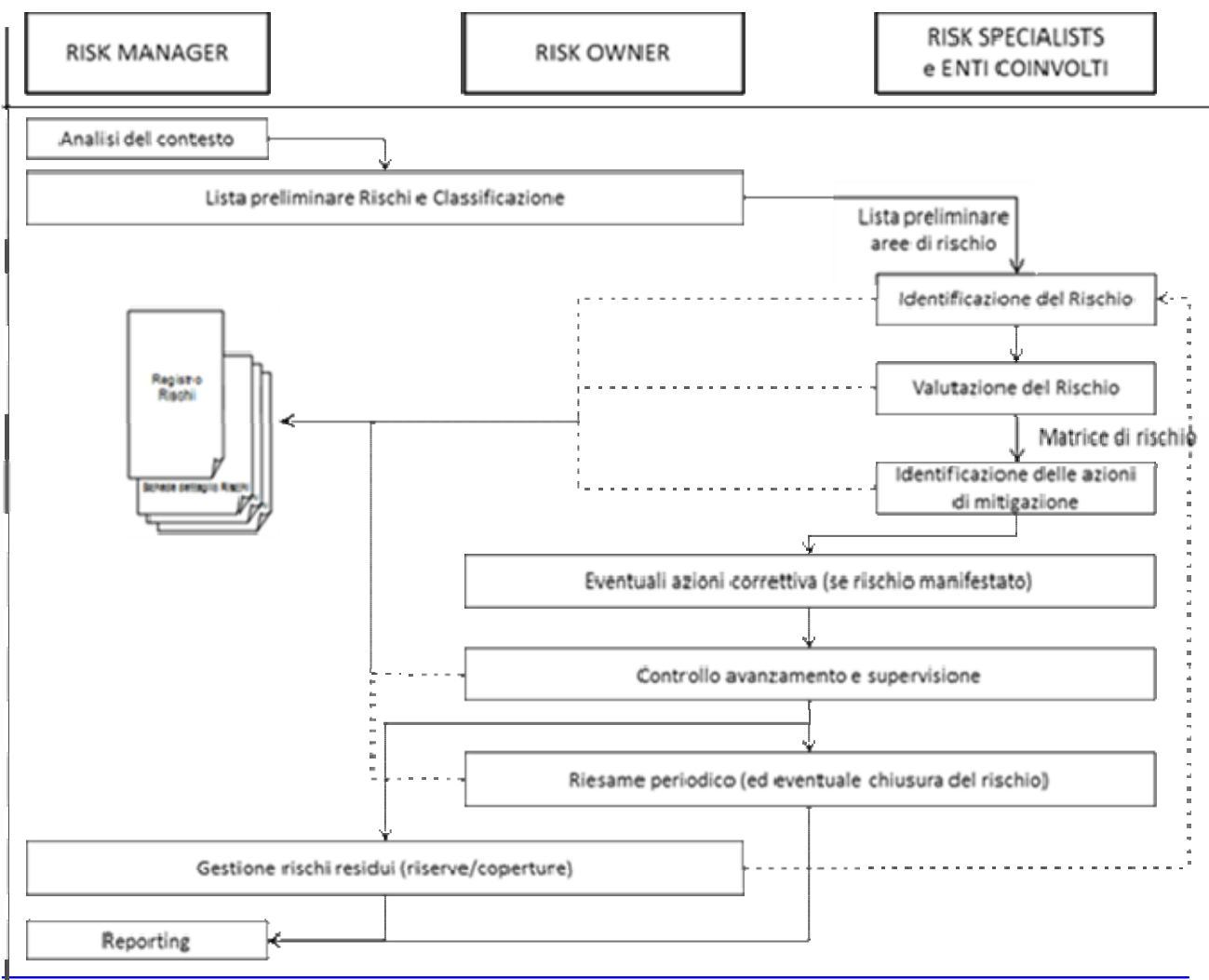
Il Piano di Audit elenca le attività attraverso le quali Internal Audit verifica, sia in via continuativa sia in relazione a specifiche necessità e nel rispetto degli standard internazionali, l’operatività e l’idoneità del SCIGR. Inoltre, l’Internal Audit verifica, nell’ambito del Piano di Audit, l’affidabilità dei sistemi informativi, inclusi i sistemi di rilevazione contabile.

I presidenti del Consiglio di Amministrazione, del Collegio Sindacale e del Comitato Controllo e Rischi nonché l’Amministratore incaricato del SCIGR sono destinatari dei flussi informativi, sia periodici che in relazione ad eventi di particolare rilevanza, generati dalla Funzione di Internal Audit con modalità tali da garantire il coinvolgimento contestuale degli stessi.

3. Attuazione del Sistema di Controllo Interno e Gestione dei Rischi

3.1 Gestione dei rischi

Di seguito un modello esemplificativo dei flussi di attività/responsabilità del processo di gestione del rischio e macrodescrizione.



Fase 1: Identificazione Aree di Rischio

Analisi del contesto

Il Risk Manager, con il supporto dei primi livelli direzionali, (Risk Owners), definisce un primo elenco di aree di rischio che possono presentarsi in azienda e che verrà continuamente aggiornato nelle fasi successive.

L'identificazione delle principali aree di rischio si basa su una analisi sistematica e continua di tutti i processi aziendali e del contesto in cui l'azienda è chiamata ad operare (top-down). Nella fase iniziale e nelle fasi periodiche di aggiornamento, queste analisi sono condotte con sessioni di brainstorming promosse e gestite dal Risk Manager con i responsabili delle principali funzioni aziendali (primi livelli direzionali); l'approccio deve essere quello di analizzare tutti i fattori che possono compromettere il raggiungimento dei principali obiettivi aziendali.

Ad integrazione di quanto sopra, ogni responsabile, partendo dalle attività che devono essere effettuate nella propria funzione, analizza tutti gli elementi che possono avere impatti aziendali negativi (bottom-up).

Lista Preliminare dei Rischi e Classificazione

Tutte le aree di rischio individuate devono essere classificate (vedere gli esempi di categorie e sottocategorie nella gestione del rischio sotto riportati); la classificazione, oltre a consentire il raggruppamento per tipo, permette di metterle in ordine di priorità al fine di definire una lista preliminare di intervento. Per ogni area di rischio deve essere identificata, con il supporto del primo livello direzionale maggiormente coinvolto, la persona più adatta a condurre l'analisi sulla base delle conoscenze specifiche possedute (Risk Specialist).

La lista delle aree di rischio viene costantemente aggiornata dal Risk Manager e costituisce un piano di lavoro dinamico di abbattimento dei rischi.

I rischi vengono classificati in diverse categorie in funzione del tipo di impatto sulle attività:

- Rischi Strategici – rischi inerenti le strategie adottate per il perseguimento degli obiettivi di business;
- Rischi Operativi – rischi inerenti i processi realizzativi e di supporto che la Società ha definito per far funzionare la struttura organizzativa, per attuare le strategie aziendali o nella gestione del cambiamento dei processi;
- Rischi Finanziari – rischi inerenti la capacità dell'impresa di adempiere correttamente ai suoi obblighi finanziari;
- Rischi di Compliance – rischi inerenti possibili sanzioni giudiziarie o amministrative o danni reputazionali in conseguenza alla violazione di norme interpretative (di legge o di regolamenti) ovvero di autoregolamentazioni;
- Rischi di Contesto – rischi inerenti il verificarsi di mutamenti del contesto esterno all'impresa (modifiche normative a livello nazionale o europeo, modifiche ai criteri di accesso a fonti di finanziamento comunitarie, etc.);
- Rischi dei Sistemi Informativi – rischi inerenti il malfunzionamento dei sistemi informativi, nonché azioni di manomissione degli stessi al fine di ricavarne un vantaggio economico privato;
- Rischi Cyber: rischio che le informazioni trattate attraverso il sistema informatico aziendale possano essere violate, rubate o cancellate o manomesse a causa di eventi accidentali o di azioni dolose.

Fase 2: Valutazione del Rischio

Identificazione del rischio

Per ogni area di rischio il Risk Specialist, direttamente o con il supporto di esperti degli enti coinvolti, effettua una analisi sistematica delle attività individuando tutti gli eventi potenziali che possono avere impatti negativi sugli obiettivi aziendali valutando conseguenze e cause. Questa fase può basarsi su: esperienze precedenti, brainstorming, diagrammi causa-effetto, benchmarking.

I rischi dovranno essere identificati nella forma di "SE" (ipotesi) "ALLORA" (effetto), in quanto questa impostazione aiuta nel definire accuratamente il rischio e ne facilita la successiva valutazione.

La verifica della esistenza di un rischio concreto deve portare ad aprire una voce nel Registro Rischi (vedere esempio sotto riportato); per ogni rischio deve sempre essere identificato il Risk Owner.

Valutazione del rischio

La valutazione del rischio viene fatta sulla base di una matrice che incrocia probabilità di accadimento (scala 1-5) e impatto (scala 1-5) ottenendo un Indice di Rischio o Magnitudo (IR - su una scala 1-20) che determina il livello di attenzione da dare al rischio nonché la priorità di intervento.

Al fine di standardizzare la valutazione degli elementi di rischio e ridurre la soggettività della valutazione, sono definite delle tabelle indicanti i criteri di probabilità di accadimento (5 livelli) e di impatto (5 livelli), nonché i relativi indici numerici. Di seguito un esempio di tali tabelle.

Esempio di criteri per probabilità di accadimento (Indice di Probabilità)

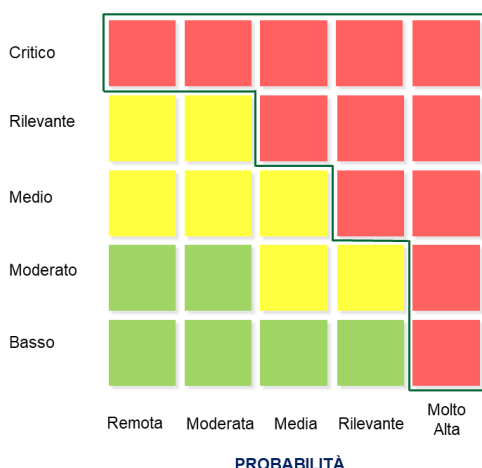
LIV.	DESCRIZIONE	PROBABILITÀ
5	MOLTO ALTA <i>E' quasi certo o certo che l'evento si verificherà nell'orizzonte quinquennale di piano</i>	• > 75% Probabilità di accadimento nell'intero orizzonte temporale in scope
4	RILEVANTE <i>Si prevede / stima, in un caso su due, che l'evento si verificherà sull'orizzonte quinquennale di piano</i>	• 50-75% Probabilità di accadimento nell'intero orizzonte temporale in scope
3	MEDIA <i>L'evento ha discrete possibilità di verificarsi sull'orizzonte quinquennale di piano, ancorché con probabilità inferiore a un caso su due</i>	• 25-50% Probabilità di accadimento nell'intero orizzonte temporale in scope
2	MODERATA <i>L'evento ha basse probabilità di accadere nell'orizzonte quinquennale di piano</i>	• 5-25% Probabilità di accadimento nell'intero orizzonte temporale in scope
1	REMOTA <i>È altamente improbabile che l'evento possa accadere nell'orizzonte quinquennale di piano (evento ritenuto eccezionale)</i>	• < 5% Probabilità di accadimento nell'intero orizzonte temporale in scope

Esempio di criteri per impatto (Indice di Impatto)

LIV.	DESCRIZIONE	IMPATTO		
		ECONOMICO	REPUTAZIONALE	OPERATIVO
5	CRITICO	<ul style="list-style-type: none"> >5 M€ su EBITDA [$\geq 10\%$] 	<ul style="list-style-type: none"> Immagine della società presso l'opinione pubblica significativamente compromessa con necessità di interventi immediati 	<ul style="list-style-type: none"> Ripercussioni sulla capacità dell'azienda di perseguire una o più strategie "chiave" per la crescita e la continuità del business Blocco operativo prolungato / distruzione asset critici
4	RILEVANTE	<ul style="list-style-type: none"> 1 - 5 M€ su EBITDA [2,5% - 10%] 	<ul style="list-style-type: none"> Conseguenze negative rilevanti sull'opinione pubblica tali da richiedere interventi da parte della società 	<ul style="list-style-type: none"> Ripercussioni sull'efficienza / continuità di processi aziendali critici per il business Blocco operativo temporaneo / perdita funzionalità asset critici
3	MEDIO	<ul style="list-style-type: none"> 0,4 - 1 M€ su EBITDA [1% - 2,5%] 	<ul style="list-style-type: none"> Conseguenze negative moderate sull'opinione pubblica tali da richiedere interventi mirati da parte della società 	<ul style="list-style-type: none"> Ripercussioni sull'efficienza / continuità di più processi aziendali non critici per il business Limitazione operativa / parziale perdita funzionalità asset
2	MODERATO	<ul style="list-style-type: none"> 0,2 - 0,4 M€ su EBITDA [0,5 - 1%] 	<ul style="list-style-type: none"> Conseguenze modeste sull'opinione pubblica 	<ul style="list-style-type: none"> Ripercussioni sull'efficienza / continuità di non più di un processo aziendale non critico per il business
1	BASSO	<ul style="list-style-type: none"> < 0,2 M€ su EBITDA [$< 0,5\%$] 	<ul style="list-style-type: none"> Conseguenze irrilevanti sull'immagine della società 	<ul style="list-style-type: none"> Ripercussioni irrilevanti sull'efficienza di uno o più processi aziendali non critici per il business

Incrociando i due indici di probabilità e impatto è possibile ricavare la magnitudo (IR – su scala 1-20) dalla Matrice di Rischio valida invece per qualsiasi rischio venga valutato in Avio.

IMPATTO



Fase 3: Trattamento del rischio

Identificazione azioni di mitigazione

L'obiettivo è quello di identificare e attuare le azioni necessarie ad abbattere il rischio.

Per ogni rischio è assegnata la responsabilità ad un primo livello direzionale, che dovrà provvedere (o prevedere a Budget) le risorse necessarie a supporto del piano di azione, e viene incaricato un Risk Specialist con il compito di svolgere le analisi necessarie e condurre il piano d'azione, con il supporto di esperti delle diverse funzioni coinvolte.

Per ciascuno rischio identificato viene individuata una strategia di *risk mitigation* tra le seguenti:

- Evitare il rischio attraverso azioni quali l'uscita/abbandono di attività rischiose, il divieto di compiere determinate transazioni o attività ritenute inaccettabili per la loro esposizione al rischio;

- Accettare il rischio attraverso il monitoraggio dell'evoluzione nel tempo dell'esposizione al rischio;
- Ridurre il rischio in termini di probabilità e/o impatto, attraverso l'intensificazione di sistemi di controllo sui processi, piani di contingency, ridisegno dei processi, testing periodici, sviluppo di competenze, etc.;
- Trasferire il rischio a terzi, attraverso, ad esempio, l'assicurazione, la copertura finanziaria (hedging), la condivisione del rischio con un partner.

Eventuali Azioni Correttive

Nel caso in cui il rischio si sia già manifestato occorre intervenire per attuare tutte quelle azioni correttive che consentono di limitare le conseguenze e relativo impatto economico. È compito del Risk Manager convocare immediatamente un team operativo, assegnare la responsabilità ad un primo livello direzionale ed incaricare un Risk Specialist di condurre l'analisi e di definire un piano di azione che il Direttore dovrà validare.

Controllo avanzamento e supervisione

Al fine di garantire l'efficacia del processo di Gestione del Rischio è importante che i primi livelli direzionali effettuino periodicamente, con il supporto dei Risk Specialists, dei controlli sull'avanzamento e sulla efficacia delle azioni correttive definite od implementate di propria responsabilità.

Fase 4: Monitoraggio del Rischio

Riesame periodico Rischi

I fattori che possono influenzare la probabilità e l'impatto di una conseguenza possono cambiare nel tempo, così come i fattori che influenzano l'applicabilità o il costo delle varie azioni individuate.

Di conseguenza è necessario ripetere regolarmente il processo di Gestione del Rischio rianalizzando il contenuto del Registro Rischi e delle relative Schede di Dettaglio Rischio sia per i rischi trattati che per i rischi in corso di mitigazione. I Risk Specialists, ciascuno per le attività di propria competenza, devono periodicamente ripetere la fase di identificazione per verificare se nuovi rischi, inizialmente non previsti, si possono manifestare.

L'eventuale chiusura di un Rischio è fattibile solo quando, a seguito della implementazione delle azioni di mitigazione, la classe di rischio residuo è ormai BASSA.

Il riesame deve essere coordinato dal Risk Manager.

È ragionevole prevedere che il riesame periodico dei rischi avvenga almeno una volta l'anno e che in tale occasione il Risk Manager relazioni i risultati alla Direzione Generale.

Gestione dei Rischi Residui

Ciascun rischio identificato e presente nel Registro Rischi deve essere valutato da parte del Risk Specialist con il supporto del primo livello direzionale in termini di costo che l'azienda dovrebbe sostenere nel caso che il rischio si avverasse.

Reporting

È compito del Risk Manager emettere periodicamente (almeno una volta l'anno) una relazione sulla Gestione dei Rischi.

3.2 Attuazione del SCIGR nelle società controllate

Avio, nell'ambito della propria attività di direzione e coordinamento, adotta un sistema unitario di controllo interno e di gestione dei rischi del Gruppo, che consente l'effettivo controllo sia delle scelte strategiche del Gruppo nel suo complesso, sia dell'equilibrio gestionale delle singole componenti.

Al fine di garantire l'adeguato funzionamento del SCIGR, le società controllate devono quindi attenersi alle presenti linee di indirizzo nell'istituzione e manutenzione del proprio SCIGR coerentemente con le strategie e le politiche di Avio in materia di controlli, fermo restando il rispetto della specifica disciplina eventualmente applicabile su base individuale.

Nell'ambito del SCIGR, Avio definisce alcuni strumenti, ruoli, norme e regole aziendali nell'ambito della propria attività di direzione e coordinamento nei confronti delle società controllate. Ciò al fine di favorire il perseguimento degli obiettivi aziendali mediante un approccio volto alla coerenza complessiva, nonché alla valorizzazione delle caratteristiche comuni anche tramite sinergie.

Tale approccio prevede per tematiche trasversali alle società controllate, azioni comuni e coordinate, adeguati flussi informativi dalle società controllate verso la Capogruppo, nonché l'esecuzione di opportune attività di monitoraggio. Il monitoraggio è finalizzato alla verifica del rispetto da parte delle società controllate delle direttive fornite in materia di SCIGR e quindi non comprende la verifica e la responsabilità che il SCIGR di ciascuna società controllata sia adeguato e funzionante nel suo complesso.

Le società controllate, nell'ambito della propria autonomia e indipendenza, recepiscono le linee guida SCIGR di Avio adeguandole al proprio contesto organizzativo ed operativo nonché ad eventuali specifiche norme applicabili.

In particolare, il CdA, o l'Organo equivalente delle società controllate, ha la responsabilità di garantire un adeguato ed effettivo Sistema di Controllo Interno e Gestione dei Rischi, recependo le presenti linee guida ed assumendo ruoli e responsabilità previsti per il corrispondente Organo di Avio, limitatamente a quanto applicabile al proprio business e organizzazione aziendale, fermo restando il rispetto delle discipline eventualmente applicabili alle singole società.

Gli Amministratori Delegati o figure equivalenti delle società controllate curano l'istituzione e mantenimento di un adeguato ed effettivo SCIGR dando attuazione al presente documento.

Al fine di consentire ad Avio di svolgere al meglio il proprio ruolo di direzione e coordinamento del Gruppo, le eventuali necessità di deroga alla presente linea guida da parte delle società controllate sono comunicate all'AD di Avio.

3.3 Verifica e valutazione continua dell'efficacia del SCIGR

La periodica verifica dell'adeguatezza e dell'effettivo funzionamento e la sua eventuale revisione costituiscono parte essenziale della struttura del SCIGR, al fine di consentire una sua piena e corretta efficacia.

Tale verifica periodica spetta al Consiglio di Amministrazione assistito dal Comitato Controllo e Rischi e dall'Amministratore incaricato del SCIGR.

Nell'effettuare tale verifica il Consiglio di Amministrazione avrà cura non solo di verificare l'esistenza e l'attuazione nell'ambito della società di un SCIGR, ma anche di procedere periodicamente ad un esame dettagliato della struttura del Sistema stesso, della sua idoneità e del suo effettivo e concreto funzionamento.

A tal fine il Consiglio di Amministrazione avrà cura di ricevere ed esaminare i rapporti predisposti dal Responsabile Internal Audit, già preventivamente esaminati dal Comitato Controllo e Rischi e dall'Amministratore incaricato del SCIGR, al fine di verificare se la struttura del Sistema in essere nella società risulti adeguato e concretamente efficace nel perseguimento degli obiettivi e se le eventuali debolezze segnalate implicano la necessità di un miglioramento del Sistema.

Il Consiglio di Amministrazione, inoltre, annualmente, in occasione del Consiglio di Amministrazione di approvazione del bilancio, avrà l'onere di:

- esaminare quali siano i rischi aziendali significativi sottoposti alla sua attenzione dall'Amministratore incaricato del SCIGR e valutare come gli stessi siano stati identificati, valutati e gestiti. A tal fine particolare attenzione dovrà essere posta nell'esame dei cambiamenti intervenuti nel corso dell'ultimo esercizio di riferimento, nella natura ed estensione dei rischi e nella valutazione della risposta della società a tali cambiamenti;
- valutare l'efficacia del SCIGR nel fronteggiare tali rischi, ponendo particolare attenzione alle eventuali inefficienze che siano state segnalate;
- considerare quali azioni siano state poste in essere ovvero debbano essere tempestivamente intraprese per sanare tale carenza;
- predisporre eventuali ulteriori politiche, processi e regole comportamentali che consentano alla società di reagire in modo adeguato a situazioni di rischio nuove o non adeguatamente gestite.

3.4 Modalità di coordinamento e collaborazione tra i soggetti coinvolti nel SCIGR

Il corretto funzionamento del sistema di controllo interno e gestione dei rischi si basa sulla proficua interazione nell'esercizio dei compiti tra le funzioni aziendali di controllo.

Un sistema integrato mira al raggiungimento dei seguenti obiettivi:

- eliminazione delle sovrapposizioni metodologiche / organizzative tra le diverse funzioni di controllo;
- condivisione delle metodologie con cui le diverse funzioni di controllo effettuano le valutazioni;
- miglioramento della comunicazione tra le funzioni di controllo e gli organi aziendali;
- riduzione del rischio di informazioni "parziali" o "disallineate";
- capitalizzazione delle informazioni e delle valutazioni delle diverse funzioni di controllo.

La definizione di modalità di coordinamento e collaborazione tra le funzioni aziendali di controllo favorisce il complessivo funzionamento del SCIGR nonché una rappresentazione univoca e coerente al vertice e agli organi aziendali dei rischi ai quali la Società e le sue controllate risultano esposte.

A tal fine, si prevedono tra i principali momenti di coordinamento e collaborazione tra le funzioni di controllo, quello in fase di programmazione delle attività annuali e gli incontri periodici con tutti i soggetti coinvolti nel SCIGR, alimentati dai flussi informativi previsti, nei quali scambiarsi le informazioni relative alle risultanze delle proprie attività e alle valutazioni effettuate circa le debolezze del sistema dei controlli interni e di gestione dei rischi, nonché la condivisione delle azioni di rimedio definite/suggerite.

3.5 Flussi informativi tra i soggetti coinvolti nel SCIGR

L'insieme delle interrelazioni che intercorrono tra gli organi di governo, le funzioni di controllo e il management di Avio e delle società controllate, rappresenta uno dei fondamentali meccanismi operativi di funzionamento del sistema dei controlli interni e del processo di gestione dei rischi.

La definizione di un modello delle interrelazioni rende identificabili gli obiettivi perseguiti dai diversi soggetti, in termini di esigenze concrete di controllo connesse all'espletamento dei compiti specificamente attribuiti e, al fine di garantire un efficiente ed adeguato coordinamento tra gli attori del SCIGR in termini di contenuti e tempistiche, prevede una chiara definizione dei ruoli e delle responsabilità.

A tal fine, è necessario che il sistema delle interrelazioni tra gli organi e le funzioni coinvolte nel sistema dei controlli interni si ispiri a logiche e a principi di efficacia fornendo informazioni utili al destinatario, di efficienza garantendo il giusto peso tra esigenze informative e costi per produrle, di completezza, chiarezza, accuratezza e certezza delle informazioni inviate, di tempestività nell'invio ed aggiornamento delle informazioni rilevanti, di facile accessibilità delle informazioni agli utenti autorizzati ed infine di riservatezza a tutela delle informazioni stesse.

Flussi informativi verso gli organi aziendali di Avio

I flussi informativi verso gli organi aziendali hanno la finalità di trasmettere ai suddetti organi una tempestiva ed adeguata conoscenza dei risultati dell'attività svolta dalle funzioni aziendali di controllo e delle eventuali disfunzioni riscontrate, in modo da potere attivare rapidamente i necessari interventi correttivi.

Di seguito si riportano i principali flussi verso gli organi aziendali di Avio:

FLUSSO INFORMATIVO	FUNZIONE RESPONSABILE	DESTINATARI	FREQUENZA
Piano di Audit triennale e annuale	INTERNAL AUDIT	CdA Comitato Controllo e Rischi Collegio Sindacale Amministratore Delegato/ Amministratore incaricato SCIGR OdV 231	Annuale
Audit Report	INTERNAL AUDIT	Management Comitato Controllo e Rischi Presidente Collegio Sindacale Amministratore Delegato/ Amministratore incaricato SCIGR OdV 231 (per aspetti di competenza)	Ad evento
Report di sintesi delle attività svolte e principali rilievi	INTERNAL AUDIT	CdA Comitato Controllo e Rischi Collegio Sindacale Amministratore Delegato/ Amministratore incaricato SCIGR OdV 231	Semestrale

FLUSSO INFORMATIVO	FUNZIONE RESPONSABILE	DESTINATARI	FREQUENZA
Relazione delle attività svolte	Organismo di Vigilanza ex D.Lgs.231/2001	CdA Comitato Controllo e Rischi Presidente Collegio Sindacale Amministratore Delegato/ Amministratore incaricato SCIGR	Semestrale
Relazione del Dirigente Preposto	Dirigente Preposto	CdA Comitato Controllo e Rischi Collegio Sindacale Amministratore Delegato/ Amministratore incaricato SCIGR	Semestrale
Piano di Risk Assessment e monitoraggio/gestione dei rischi	Risk Manager	CdA Comitato Controllo e Rischi Collegio Sindacale Amministratore Delegato/ Amministratore incaricato SCIGR ODV 231	Annuale