INTERNAL CONTROL AND RISK MANAGEMENT SYSTEM GUIDELINES

Approved by Avio S.p.A. Board of Directors:

- 1st Issue March 2004: Meeting of 29 March 2004
- 2nd Issue September 2008: Meeting of 23 September 2008
- 3rd Issue April 2015: Meeting of 02 October 2015
- 4th Issue May 2017: Meeting of 28 June 2017

Contents

Introduction

The Internal Control and Risk Management System (hereinafter also referred to as the "ICRMS") is an essential and qualifying element of the Corporate Governance of the companies in the Avio Group (Avio S.p.A. and its subsidiaries) and plays a fundamental role in the identification, measurement, management and monitoring of significant risks, making them compatible with the company's strategic objectives and thus contributing to the creation of medium and long-term value.

An effective ICRMS fosters aware decision-making processes and helps to safeguard and protect the shareholders' investments and company assets, ensure the efficiency and effectiveness of company processes and operations, as well as the reliability of financial information and compliance with statutory laws and regulations, the Articles of Association and other internal rules.

These Guidelines, issued by Avio S.p.A. within the framework of its role of guidance and coordination of the companies in the Avio Group, aim to represent an organic summary of all the various aspects of the ICRMS which are fully applicable to Avio S.p.A., and which must coherently refer to all the subsidiaries of the Group, each one with its own autonomous responsibility for the definition and operation of its own ICRMS.
In particular, the subsidiaries receive these Guidelines and adopt them, adapting them where necessary to the special features of their own companies and considering the applicable legislation (for example, specific regulations for their own sector).

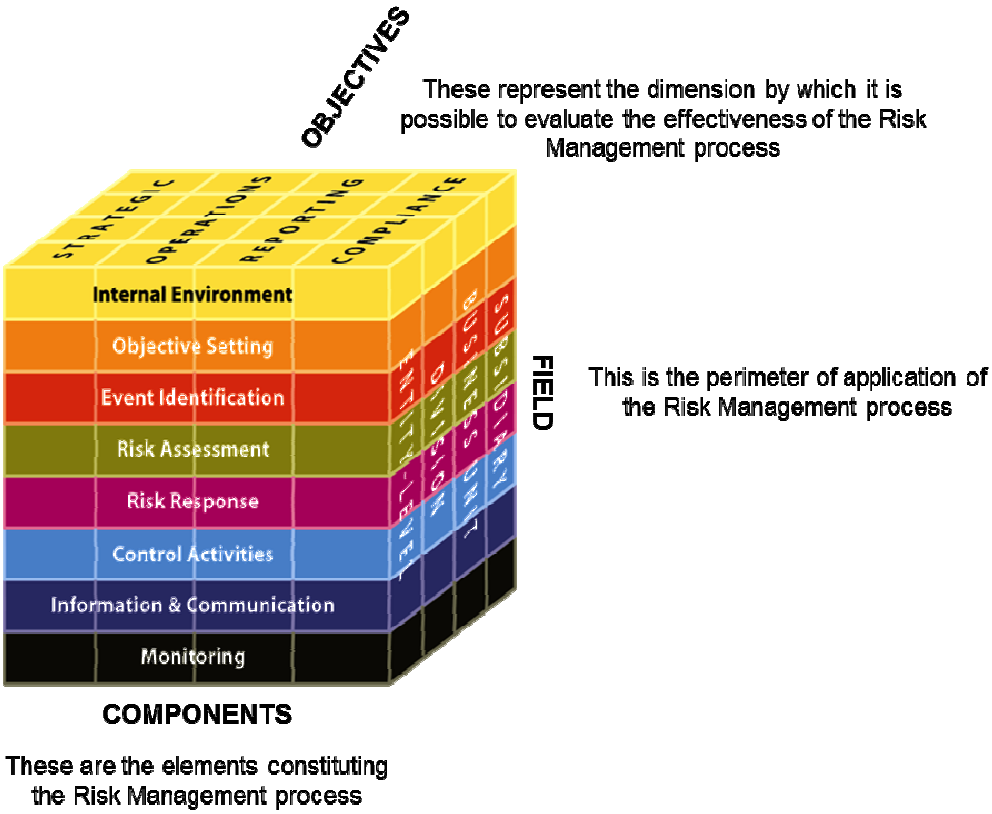
1. References and general principles

The Avio S.p.A. Internal Control and Risk Management System complies with the principles of the current edition of the Corporate Governance Code for listed companies promoted by Borsa Italiana S.p.A. (hereinafter the "Corporate Governance Code") and generally the best practices adopted nationally and internationally.

These guidelines dictate, on one hand, the general principles by which the main risks of the group are managed, according to established strategic goals, and on the other hand the methods of coordination between the parties involved (listed below) to maximise the efficiency and effectiveness of the ICRMS.

The ICRMS is, in particular, composed of a set of rules, procedures and organisational structures aiming to proactively contribute, through an appropriate process of identification, measurement, management and monitoring of the main risks, to safeguarding the corporate heritage of the Avio Group, the effective and efficient running of the Group in line with the corporate strategies defined by the Board of Directors of the parent company, the reliability, accuracy and soundness of the information provided to corporate bodies and the market and, generally, compliance with legislative and regulatory provisions.

To define its own ICRMS, the Avio Group was inspired by the best practices in force and in particular the international standard "Enterprise Risk Management-Integrated Framework" ("ERM Integrated Framework"), drafted and updated by the US "Committee of Sponsoring Organizations of the Treadway Commission" (COSO); this framework is also known as the "COSO Report" or "COSO ERM".

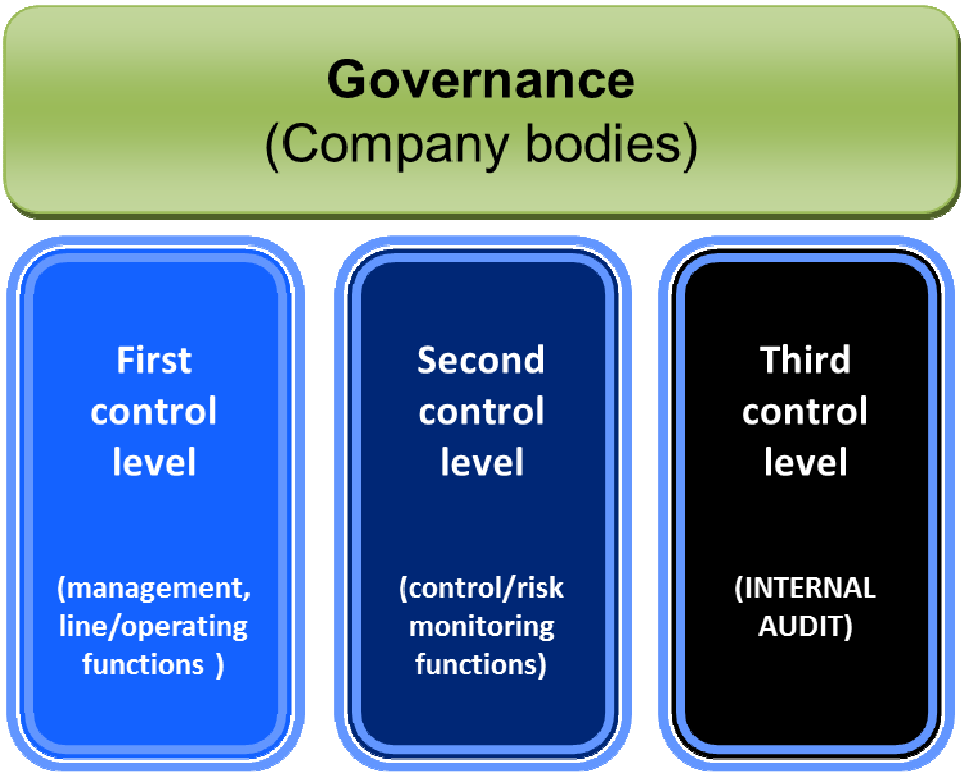


The aforementioned ERM Framework identifies a direct relationship between company objectives (strategic, operational, reporting and conformity) to be pursued and the components of the risk control and management system, as well as the organisational structure adopted by the company/Group.
The main components interconnected and integrated in the processes and all levels of the organisation, identified by this Framework as constituent parts of the ICRMS are described in brief below:

- **Internal Environment**: the essential identity of the organisation. This determines the way in which the risk is considered and tackled by the company resources, as well as the philosophy of risk management, the levels of acceptability of the risk, the integrity, ethical values and working environment generally.
- **Objective Setting**: the objectives must be set before proceeding with the identification of the events which may potentially compromise their achievement, they must support the company mission and be coherent with the mission and in line with the acceptable levels of risk.
- **Event Identification**: this concerns the correct and complete identification and classification of all events, of internal or external origin, which may wholly or partially compromise the achievement of the company objectives and which may represent potential risks to be managed by the company.
- **Risk Assessment**: this introduces a component of evaluation to quantify the level of "potential" risk (risk in the absence of any intervention) and the level of "residual" risk (risk remaining after the actions implemented to reduce it have been taken into consideration). The levels of risk must be quantified by taking into consideration their impact on the achievement of the company objectives linked to any occurrence of the event and the associated probability that the event may occur.
- **Risk Response**: this concerns the choice and activation by the management of measures aiming to manage the emerging risk, reducing it and aligning it to the levels of "tolerated risk" or "accepted risk".
- **Control Activities**: these concern the need to define, implement and apply suitable policies and procedures aiming to guarantee that the responses to risk and the measures defined to eliminate or contain it are effectively and efficiently implemented.
- **Information & Communication**: the information must be identified, gathered and disseminated in the times and methods ensuring that all resources involved in the process can act correctly and effectively.
- **Monitoring**: this is understood as the "ability" of the company to assess its own activities and update/improve constantly over time.

The ICRMS, which is an integral part of the company activities, involves and is applied to all organisational structures of the companies in the Group, each within its own area of responsibility: from the Board of Directors and Managing Director of Avio S.p.A. and its subsidiaries, to the Group Management and company employees.

In line with the referred regulations and best practices, the Internal Control and Risk Management System is divided into the following levels:



Governance
Under responsibility of the company bodies: to define, approve and check the Internal Control and Risk Management System.

First control level
Under responsibility of the operational lines/departments: to identify, assess, manage and monitor the risks for which they are responsible, for which they identify and implement specific actions to directly handle and ensure the correct performance of the operations.
It consists of the set of control activities which the individual operational units perform on their own processes in order to ensure the correct performance of the operations. These control activities are the primary responsibility of the operational management and are considered a part of every company process. The operational departments are therefore the key parties in charge of the internal control and risk management process. During their everyday operations, these departments are required to identify, measure or assess, monitor, reduce and report on the risks deriving from the ordinary company activities, in conformity with the risk management process and the applicable internal procedures.

Second control level

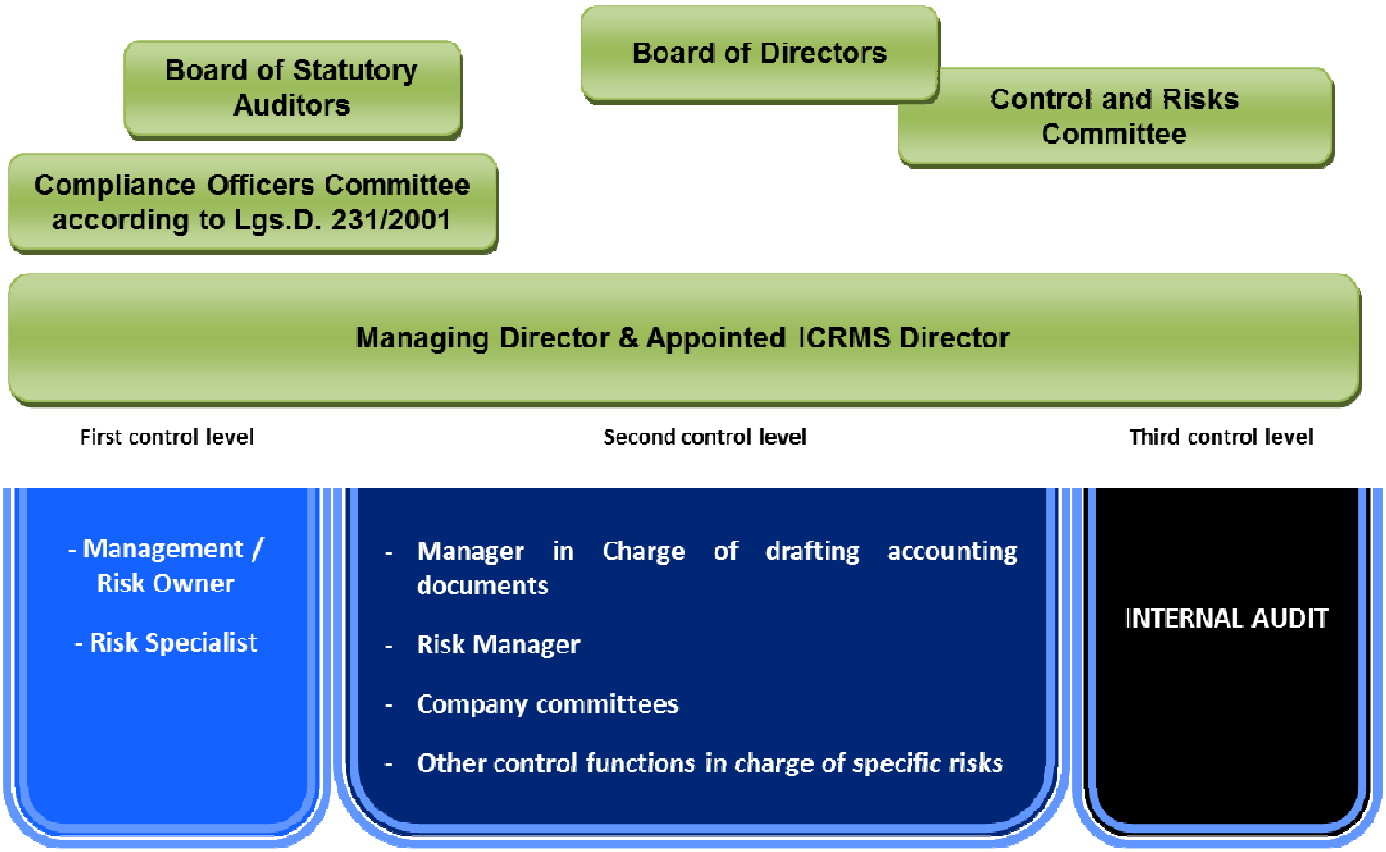
Appointed to autonomous, independent and non-operational departments; they assist in the definition of governance policies and the risk management process (identification, evaluation and control). At this level, the company risks are monitored, proposing guidelines on the relative control systems and checking their appropriateness for ensuring the efficiency and effectiveness of operations, appropriate risk controls, prudent business management, reliability of information, conformity to laws, regulations and internal procedures.

Third control level

Under responsibility of the Internal Audit function: it provides independent assurance of the appropriateness and effective operations of the first and second control levels, and generally on the ICRMS. It aims to assess the completeness, appropriateness, functionality and reliability in terms of the efficiency and effectiveness of the internal control system and identify breaches of procedures and applicable regulations.

2. Parties involved, tasks and responsibilities

The ICRMS is an integrated system performed by a number of different company functions and bodies, the members of which coordinate together and interdependently, it is characterised by the complementarity of the purposes pursued, the organisational characteristics and the operating rules.
The summary below shows the key players in the ICRMS in relation to the corporate governance model and the architecture based on the three control levels.



The tasks and responsibilities of the ICRMS players, described in the following paragraphs, were defined in accordance with the provisions of applicable standards and regulations (including the Corporate Governance Code, Italian Legislative Decree no. 231/2001, Italian Law no. 262/2005), internal provisions and regulations and applicable best practices.

2.1 Board of Directors

The Board of Directors (hereinafter also the BoD) performs the role and tasks laid down in the Corporate Governance Code and, within its own key function of guidance and evaluation of the appropriateness of the ICRMS, is the body with ultimate responsibility for the System.

For the purposes of the appropriate performance of the tasks it is responsible for, the BoD

a) establishes the Control and Risks Committee, assigning it a consultative and proactive role in relation to the ICRMS as laid down in the Corporate Governance Code, appoints its members, including the Chairman of the Committee;
b) appoints the Managing Director of the company as the Director appointed to establish and maintain the efficacy of the ICRMS;

with the support of these, it carries out the evaluations and takes decisions concerning the ICRMS and ensures that the tasks and responsibilities are assigned clearly and appropriately, and that the Head of Internal Audit function, the Compliance Officers Committee ("*Organismo di Vigilanza*") as per Italian Legislative Decree no. 231/2001 and the Manager in Charge of drafting accounting documents, are given appropriate resources to perform their activities and have an appropriate level of autonomy within the structure.

Therefore the BoD, having received the opinion of the Control and Risks Committee:

a) defines, issues and updates these guidelines, to ensure that the main risks are correctly identified, appropriately measured, managed and monitored, also determining the degree of compatibility with a corporate management consistent with the identified strategic objectives;
b) assesses, at least annually, the suitability of the ICRMS in relation to the business characteristics and assumed risk profile, as well as its effectiveness;
c) at the proposal of the Appointed ICRMS Director, having received the favourable opinion of the Control and Risks Committee, having received the opinion of the Board of Statutory Auditors, appoints (and revokes) the Head of Internal Audit function (Chief Audit Officer or CAO) and defines his/her remuneration consistently with the provisions of the company policies, ensuring that the CAO has the appropriate resources to perform his/her functions and cover his/her responsibilities;
d) at least annually, approves the work plan drafted by the Chief Audit Officer, having received the opinion of the Board of Statutory Auditors and the Appointed SCIGR Director, and examines the results of the activities performed, evaluating their suitability;
e) in the corporate governance report, describes the main characteristics of the ICRMS and the methods of coordinating with all parties involved in it, expressing its own evaluation on the suitability of the ICRMS; having received the opinion of the Board of Statutory Auditors, it evaluates the results presented by the External Auditors in any letter of recommendations and in the report on the fundamental issues arising from the audit.

2.2 Control and Risks Committee

The Control and Risks Committee has a consultative and proactive function for the Board of Directors, with the task of supporting the board through appropriate investigating activities, relating to the evaluations and decisions concerning the ICRMS, as well as in relation to the approval of the periodic financial reports.

In particular, in conformity with the provisions of the Corporate Governance Code, in assisting the Board of Directors, the Control and Risks Committee:

a) with the Manager in Charge of drafting accounting documents, and having received the opinion of the External Auditors and the Board of Statutory Auditors, evaluates the correct use of the accounting principles and their uniformity for the purposes of drafting the consolidated financial statements;

b) expresses opinions on specific aspects concerning the identification of key company risks;

c) examines the periodic reports concerning the evaluation of the Internal Control and Risk Management System, and those of particular importance drafted by Internal Audit function;

d) monitors the autonomy, suitability, efficiency and effectiveness of the Internal Audit function;

e) may ask Internal Audit to perform checks on specific operational areas, at the same time notifying the Chairman of the Board of Statutory Auditors; for coordination purposes, it also notifies the Chairman of the Board of Directors and the Appointed Director for the Internal Control and Risk Management System, unless the subject of the requested checks specifically concerns these bodies;

f) reports to the Board of Directors, at least on a six-monthly basis, during the approval of the annual and six-monthly financial report, on the activities carried out and the suitability of the Internal Control and Risk Management System;

g) supports, through appropriate investigations, the evaluations and decisions of the Board of Directors relating to risk management deriving from detrimental facts the Board of Directors has become aware of;

h) performs the other tasks assigned by the Corporate Governance Code or the Board of Directors.

The Control and Risks Committee also issues its own prior opinion to the Board of Directors:

(i) for the purpose of defining the guidelines for the Internal Control and Risk Management System, so that the main risks relating to the company and its subsidiaries are correctly identified, appropriately measured, managed and monitored, and for determining the degree of compatibility of these risks with a company management that is consistent with the identified strategic objectives, also considering the risks which may become important with a view to the medium-long term sustainability of the company's activities;

(ii) for the purpose of evaluating, at least annually, the suitability of the Internal Control and Risk Management System in relation to the business characteristics and assumed risk profile, as well as its effectiveness;

(iii) for the purpose of approving, at least annually, the work plan drafted by the Head of Internal Audit, without prejudice to the need of the Board of Directors to also

receive the opinion of the Board of Statutory Auditors and the Appointed Director of the Internal Control and Risk Management System;

(iv) for the purpose of describing, in the corporate governance report, the main characteristics of the Internal Control and Risk Management System and the methods of coordination between the bodies involved, as well as the evaluation of the suitability of the system;

(v) for the purpose of evaluating the results presented by the statutory auditor in any letter of recommendations and in the report on the fundamental issues arising from the audit, without prejudice to the need of the Board of Directors to also receive the opinion of the Board of Statutory Auditors;

(vi) on the proposal concerning the appointment, revocation and definition, consistently with company policies, of the remuneration for the Head of Internal Audit function, as well as the suitability of the resources assigned to him/her for the performance of his/her duties.

2.3 Managing Director and Appointed ICRMS Director

The Managing Director of the company not only holds the powers necessary to fulfil all operational requirements concerning company activities, but is also the director appointed to establish and maintain an effective internal control and risk management system ("Appointed ICRMS Director").
In compliance with the Corporate Governance Code, the Appointed Director:

- identifies the key company risks, considering the characteristics of the activities of the company and the group it heads, and submits them periodically for review by the Board of Directors;
- ensures that the guidelines defined by the Board of Directors are implemented, overseeing the design, implementation and management of the internal control system, constantly checking its overall suitability, efficiency and effectiveness;
- ensures that the system is adapted in line with the dynamics of the operational conditions and the legislative and regulatory outline;
- may ask Internal Audit to perform audits on specific operational areas and concerning compliance with internal rules and procedures in the performance of company operations, at the same time notifying the Chairman of the Board of Directors, the Chairman of the Control and Risks Committee and the Chairman of the Board of Statutory Auditors;
- reports promptly to the Control and Risks Committee (or the Board of Directors) on problems and issues emerging in the performance of his/her own activities or which he/she has been informed of, so that the Control and Risks Committee (or the Board) can take appropriate action.

2.4 Board of Statutory Auditors

The Board of Statutory Auditors performs the tasks assigned by law and by the articles of association. In particular, it monitors:

- compliance with the law and the articles of association;
- compliance with the principles of correct administration and the suitability of the company organisation;
- the completeness, suitability and effectiveness of the ICRMS;

- the completeness, suitability and effectiveness of the administrative and accounting system and the reliability of this in correctly representing the management operations;
- the suitability of the instructions issued to the subsidiaries for the correct fulfilment of the foreseen communication obligations.

In this regard, the Board of Statutory Auditors, in line with the role and tasks laid down in the Corporate Governance Code:

– promptly shares key information with the Control and Risks Committee to allow their respective tasks to be performed;
– has the faculty to ask Internal Audit to audit specific operational areas or company operations.

2.5 Compliance Officers Committee according to Italian Lgs.D. 231/2001

The Compliance Officers Committee ("*Organismo di Vigilanza*", hereinafter "COC") is appointed by the Board of Directors and has appropriate financial resources to perform its activities, including:

- the monitoring of the efficiency and suitability of the Organisation, Management and Control Model pursuant to Italian Legislative Decree no. 231/2001 (hereinafter the "Model" or "OMCM") or its suitability for preventing the occurrence of the crimes listed in Italian Legislative Decree no. 231/2001 on the basis of an annual audit plan presented to the Board of Directors;
- checking the suitability of the organisational solutions adopted for the implementation of the Model;

– drafting a report at least every six months, sent to the Control and Risks Committee, the Board of Statutory Auditors and the Board of Directors relating to its own activities and informing them of any reported breaches of the Model.

The COC must be provided with all information which concerns, even indirectly, attempted or actual crimes or deviations from the Model, and generally all behaviours at risk of crime.

2.6 Management

All Group employees, according to the tasks they are assigned within the company organisation, ensure the effective operation of the Internal Control and Risk Management System, as part of their responsibilities in achieving the objectives.
At all levels of the organisation, they are in charge of the first level control of the system.
They must therefore have the necessary knowledge, experience and skill to work in the framework of the ICRMS and must be allowed to perform their tasks in line with their role and fulfil their own responsibilities.
This therefore implies the right and the duty of each and every employee to have full knowledge and understanding of the company he/she works in and the Group, its operating mechanisms, objectives, markets in which the company operates and the risks to which it is exposed on a daily basis.

During its everyday operations, the Management is required to identify, measure or assess, monitor, reduce and report on the risks deriving from the ordinary company activities, in conformity with the risk management process and the applicable internal procedures.

2.7 Second level control bodies/functions

The second level control functions are figures with specific tasks and responsibilities for controlling different areas/types of risk. These functions monitor company risks, propose guidelines on the relative control systems and check their appropriateness for ensuring the efficiency and effectiveness of operations, appropriate risk controls, prudent business management, reliability of information, conformity to laws, regulations and internal procedures.
The functions in charge of these controls are independent and separate from the operational functions; they assist in the definition of risk management policies and processes.

2.7.1 Manager in Charge of drafting accounting documents

Pursuant to article 154-bis of the Italian Consolidated Finance Act ("TUF"), the Manager in Charge shall be bound to:

(i) certify that the company deeds and communications issued to the market and relating to the company's annual and periodic accounting information correspond to the results of the accounting entries, ledgers and documents;
(ii) draft appropriate administrative and accounting procedures to draft the balance sheets and consolidated financial statements, and all other financial communication; and
(iii) certify, together with the Managing Director, through a specific report annexed to the financial statements, abridged six-monthly balance sheet and consolidated financial statements, among others, the suitability and effective application of the procedures in paragraph (ii), during the period to which the documents refer, and also certify the correspondence of these to the results of the accounting entries and ledgers and their suitability for offering a truthful and correct representation of the company's financial, economic and asset situation and that of any other companies included in the consolidation.

Given the above, he/she shall be assigned the following powers:

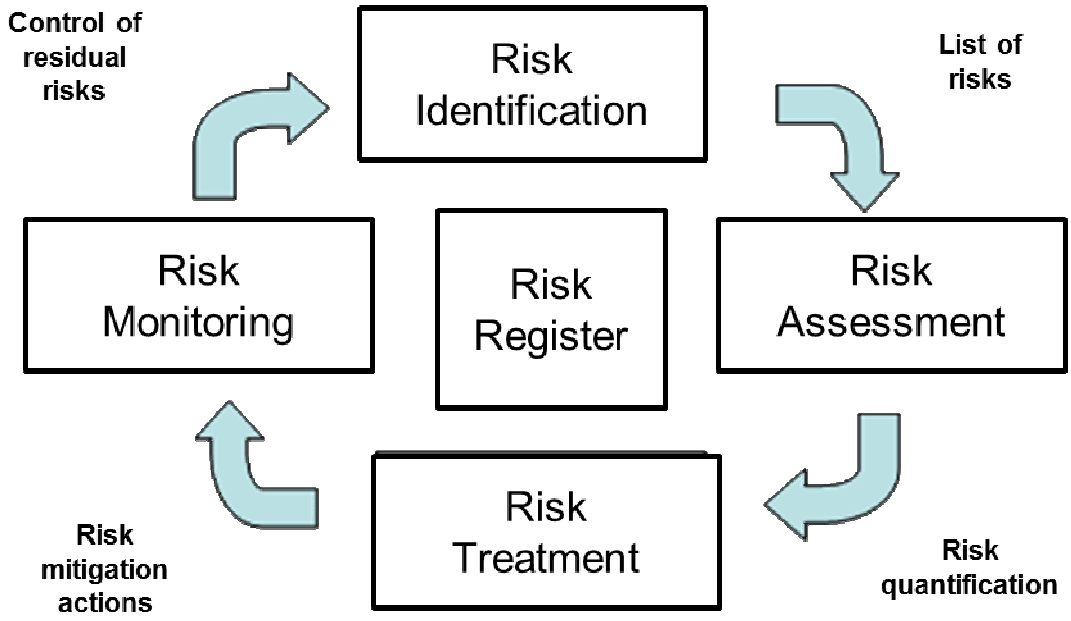
(a) free access to all information considered important for the fulfilment of his/her tasks, both in the company and in any companies in the group the company leads;
(b) participation in the meetings of the Board of Directors which discuss the matters for which he/she is responsible;
(c) faculty to dialogue with all administrative and control bodies in the company and in the subsidiaries;
(d) faculty to approve the company procedures, where these impact the balance sheets, consolidated financial statements and other documents subject to certification;
(e) participation in the design of information systems which impact the economic, financial and asset situation of the company;

(f) possibility to use the information systems.

To allow the Board of Directors to correctly exercise its supervisory powers, the Manager in Charge shall also report at least on a quarterly basis to the Board on the activities carried out, as well as any problems that have emerged.

2.7.2 Risk Management

Avio S.p.A. has a transversal structure dedicated specifically to managing the general internal risks of the Group, and this process is established in the procedures of the certified Quality Management System UNI EN ISO 9001:2008 and UNI EN 9100:2009.
The aforementioned procedure defines the methods and responsibilities for the identification, evaluation, mitigation and control of general internal risks at all levels of the Avio company structure, taking as a reference the structure of company processes defined in the Quality Management System in force.
In relation to the management of specific risks, the other Company Management Systems (Significant Accidents, Health and Safety, Environment) have their own specific procedures for the management of these specific risks, responding to precise legal requirements and/or systems.
The implemented management process can be summarised in four macro-phases, as represented in the figure below, with a final operational output represented by the "Risk Register" which lists and classifies all the identified risks (those managed and those being handled) and which may potentially occur and compromise the company objectives.



The main company figures responsible for the risk management process are:

- **Risk Manager**: the figure responsible for the coordination and management of the whole process. He/she reports directly to the Appointed SCIGR Director and ensures the correct application of the company risk management methods and, where necessary, requests appropriate reserves and insurance cover. This figure is generally the Head of Quality function or the Head of Legal Affairs function of Avio S.p.A.
- **Risk Owners**: the Managers covering all areas of potential company risk, and are therefore the first levels of the General Management.
- **Risk Specialists**: in their own field of competence, these figures are those who know the risk management methods, know how to analyse and evaluate the impacts and are able to propose and implement appropriate mitigation actions.

In particular, it is the task of the Risk Manager:

- to ensure the definition of the methods and functional tools for the Group risk management process, to identify, measure, represent and monitor the key risks and relative management plans;
- ensure the risk assessment and monitoring of the key risks in the Group, supporting the management in the identification, evaluation and management of risks and, where possible and appropriate, in the definition of the relative indicators and the performance of qualitative and quantitative analyses and investigations;
- draft the work plan and the periodic reporting to the Appointed ICRMS Director and the Control and Risks Committee in relation to the risk assessment and monitoring activities at Group level, producing the documents drafted for the management committees and administration and control bodies.

The Risk Manager drafts a summary of the activities carried out and the main company risks identified, evaluated and monitored (Risk Report). The results of these reports are presented, at defined frequencies, to the Appointed ICRMS Director, the Managing Director, the Control and Risks Committee, the Board of Statutory Auditors and the Board of Directors.

2.7.3 Company committees

Within the governance mechanisms and relative operating methods, the Avio Group has established specific committees, composed by the company management, to perform consultative and proactive concerning specific risk issues.

2.7.4 Other second level control structures

At Avio S.p.A. there are other second level control bodies, which work on these activities but not exclusively.
These structures monitor specific corporate risks (for example, those linked to the management of health and safety in the work place under Italian Legislative Decree no. 81/2008, security, environmental aspects, fraud, IT security, etc.), proposing guidelines for the relative control systems and checking their suitability, ensuring the efficiency and effectiveness of operations, appropriate risk controls, reliability of information, conformity to laws, regulations and internal procedures.

These second level control functions liaise with the company Risk Management function according to specific operating methods and exchanges of information.

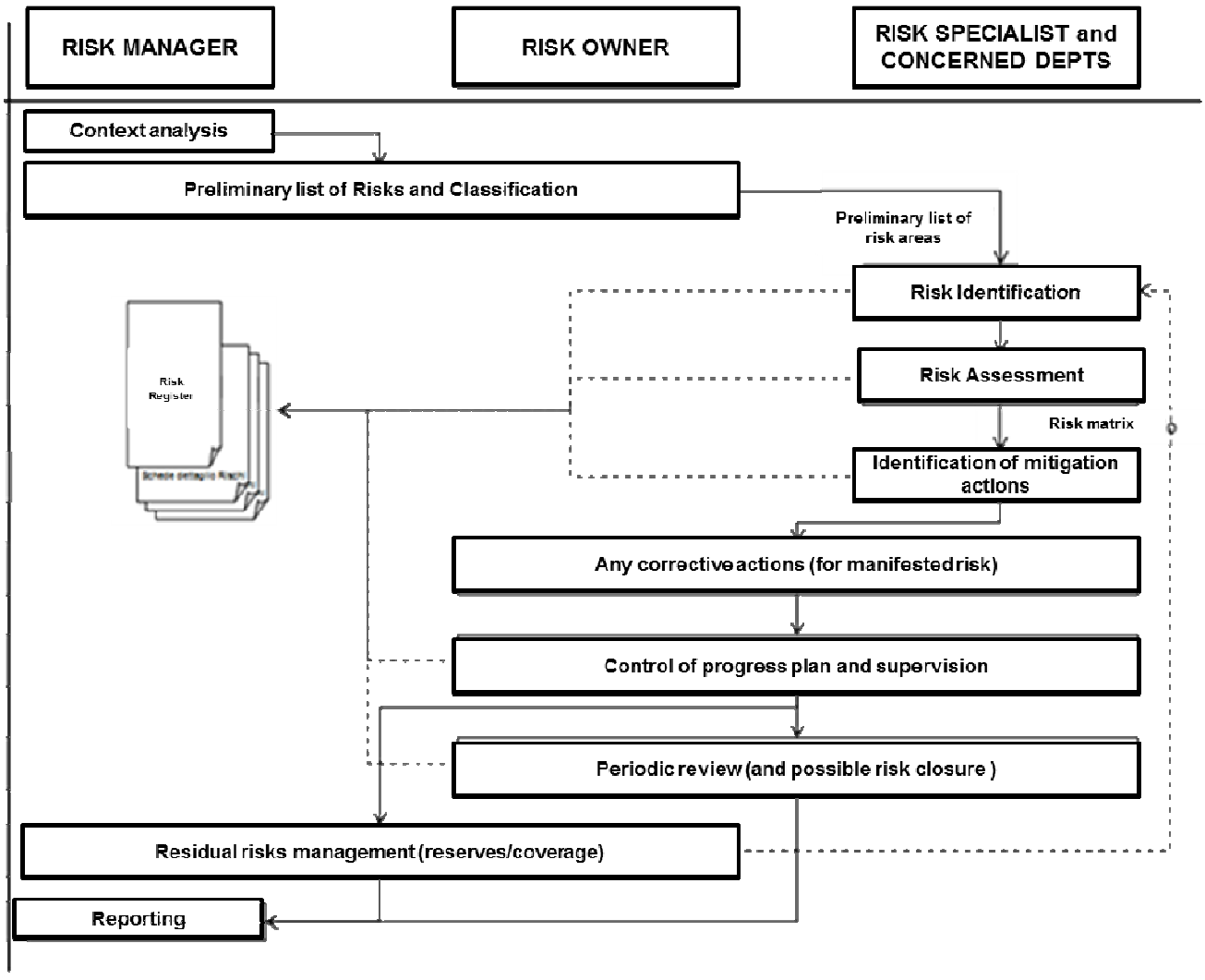
2.8 Third level control body: Internal Audit

Internal Audit is responsible for third level control activities and therefore has a recognised key position in the ICRMS. As a third level control function, it has the task of providing independent assurance on the ICRMS, aiming to improve the efficiency and effectiveness of the organisation.
Internal Audit is in charge of checking that the ICRMS is functional and suited to the size and operations of the Group, checking, in particular, that the Management has identified the key risks, that these have been evaluated using uniform methods and that the appropriate mitigation actions have been defined and implemented. It also checks that the risks are managed consistently with the resolutions of the Board of Directors, external regulations and internal rules of the Group.
The Chief Audit Officer is not responsible for any operational area, has direct access to all useful information for performing his/her tasks, reports directly to the Board of Directors and ensures that the Control and Risks Committee and the Board of Statutory Auditors receive all due information.
The annual Internal Audit work plan ("Audit Plan"), based on a structured process of analysis and prioritisation of the key risks, similarly to what laid down for the budget, is subject to the approval of the Board of Directors, having received the opinion of the Control and Risks Committee, the Board of Statutory Auditors and the Appointed SCIGR Director.
The Audit Plan lists the activities through which Internal Audit checks, both continuously and in relation to specific needs and in compliance with international standards, the operations and suitability of the ICRMS. Moreover Internal Audit checks, within the Audit Plan, the reliability of the information systems, including the accounting systems.
The Chairmen of the Board of Directors, Board of Statutory Auditors and Control and Risks Committee, as well as the Appointed SCIGR Director, are recipients of the information flows, both periodic and in relation to events of particular importance, generated by the Internal Audit function in methods that guarantee the simultaneous involvement of these bodies.

3. Implementation of the Internal Control and Risk Management System

3.1 Risk Management

Taken from the aforementioned procedure, the model below shows an example of the activity/responsibility flows involved in the risk management process, with a macro-description.



Phase 1: Identification of Risk Areas

Context analysis

The Risk Manager, with the support of the first management levels, (Risk Owners), defines a preliminary list of risk areas which may be found in the company and which will be continuously updated in subsequent phases.
The identification of the key risk areas is based on a systematic and continuous analysis of all company processes and the context in which the company is called on to operate (top-down). In the initial phase and the periodic updating phases, these analyses are carried out in brainstorming sessions promoted and managed by the Risk Manager with the managers of the main company functions (first management levels); the approach must

be that of analysing all the factors which may compromise the achievement of the company objectives.
Integrating the above, each manager, starting from the activities that must be done in his/her own function, analyses all the elements which may have negative business impacts (bottom-up).

Preliminary list of Risks and Classification

All identified risk areas must be classified (see the examples of risk management categories and subcategories shown below); this classification not only allows the grouping by type, but also to order them according to their priority to define a preliminary intervention list. For each risk area, with the support of the most involved first level management, the most suitable person for performing the analysis on the basis of specific knowledge held must be identified (Risk Specialist).
The preliminary list of risk areas must be continuously updated by the Risk Manager and constitutes a dynamic risk reduction work plan.

1 – Business & Strategy	2 – Design / Construction / Maintenance	3 – Supply Chain / Procurement
International crises / reduced volumes	Client product performance not achieved	Risks linked to Joint-ventures with suppliers
Import / Export constraints	Times / Costs of Production > target	Supplier at risk of bankruptcy
	Problems linked to client escapes	Unsuitable supplier (timing and quality)

4 – Equipment / Assets	5 – Human Factors	6 - Finance
Loss of assets due to floods, earthquakes,…	Lack of resources / skills	Incorrect financial projections
Lack of services (electricity, water,…)	Strikes/contract renewals	Interest rate risk
	Poor motivation/resignation	Exchange rate risk

7 – IT / Information and Security	8 – Environment / Health and Safety	9 – Governance/Compliance/Ethics
lack of IT service	Binding environmental requirements not met	Compliance with binding legal requirements
Lack of protection of sensitive data	Work hazardous to human health	Non-compliance with Code of Ethics
Hacking	Fire-fighting safety	Fraud against the company

Examples of categories and subcategories in risk management

Phase 2: Risk Assessment

Risk identification

For each risk area, the Risk Specialist, directly or with the support of the experts from the involved departments, performs a systematic analysis of the activities, identifying all the potential events which could have a negative impact on the company objectives, assessing their consequences and causes. This phase may be based on: previous experience, brainstorming, cause-effect diagrams, benchmarking.
The risks must be identified in the form of "IF" (hypothesis) "THEN" (effect), as this organisation helps to accurately define the risk and facilitate the subsequent evaluation.
Verifying the existence of a concrete risk must lead to the recording of an item in the Risk Register (see example below); for each risk the Risk Owner must always be identified.

Risk Assessment

The risk assessment is done according to a matrix that cross-references the probability of occurrence (scale 1-5) and impact (scale 1-4), obtaining a Risk Index (RI - scale 1-20) determining the level of attention to be paid to the risk and the priority of intervention.
To standardise the evaluation of all risk elements and reduce the subjectivity of the evaluation, tables have been defined indicating the criteria for probability of occurrence (5 levels) and impact (4 levels), as well as the relative numerical indices. An example of these tables is given below.

Probability	Description	Index
High	**Probability that the risk occurs >70%** **Risk reduction plan not available / not possible**	**5**
Significant	**Probability that the risk occurs between 50% and 70%** **Risk reduction plan possible**	**4**
Moderate	**Probability that the risk occurs between 20% and 50%** **Risk reduction plan exists**	**3**
Minor	**Probability that the risk occurs between 5% and 20%** **Existing and approved risk reduction plan**	**2**
Low	**Probability that the risk occurs <5%** **Risk reduction plan exists and already tested in previous experience**	**1**

Example of criteria according to probability of occurrence (Probability index)

Impact	DESCRIPTION			Index
	SERVICES (not linked to times or costs)	TIMES (compared to the duration of the supply)	COSTS	
Critical	Serious impact; failure to achieve the performance with significant damage to Clients, Shareholders or Persons	Average delay in activities > 20%: delay in key contractual milestones with significant impact on deliveries to the Client	Cost increases > 10% Or cost delta > 3 million €	4
High	Consistent effect; insufficient performance with possibility of extension into other areas, minor damage to Clients, Shareholders or Persons	Average delay in activities > 10% but < 20%: delay in some critical milestones involving the Client but without contractual impacts	Cost increases > 5% Or cost delta > 1 but < 3 million €	3
Average	Minor effect; partial shortcomings in performance in some areas, no risk of spreading, in any case visible to Clients, Shareholders or Persons	Average delay in activities > 5% but < 10%: delay in some non-critical milestones but visible to the Client	Cost increases > 2% Or cost delta > 0.3 but < 1 million €	2
Low	Minimal or negligible effect on a single area, does not affect Clients, Shareholders or Persons	Average delay in activities < 5%: replanning required but not of interest to the Client	Cost increases < 2% Or cost delta < 0.3 million €	1

Example of criteria for impact (Impact Index)

Cross-referencing the two indices PI and II it is possible to calculate the Risk Index (RI – scale 1-20) from the Risk Matrix valid for any risk evaluated in Avio.

Probability / **Impact**	High	Significant	Moderate	Minor	Low
Critical	1	2	4	8	12
High	3	5	6	10	15
Average	7	9	11	14	17
Low	13	16	18	19	20

KEY: Probability Index (PI) : range (1 – 5)
Impact Index (II): range (1- 4)
Risk Index (RI): range (1 – 20)

Different Risk Indices identified on the Matrix require different reactions:

- range (1 – 5) is a HIGH RISK class: this demands urgent and immediate risk mitigation actions, the definition of a plan and periodic progress reports managed at the level of Risk Manager;
- range (6 – 11) is a MODERATE RISK class: it requires the definition of actions to be implemented in the medium term, managed and monitored at the level of Risk Owner;
- range (12 – 20) is a LOW RISK class: it does not normally require the definition of action plans but they must be periodically monitored, generally these interventions could be implemented at the first next useful opportunity.

Phase 3: Risk treatment

Identification of mitigation actions

The objective is to identify and implement the actions required to reduce the specific risk and return the RI to the no or LOW risk range.

For each risk, responsibility is assigned to a first managerial level, who shall provide for (or foresee in the Budget) the resources required to support the action plan, and a Risk Specialist is appointed to perform the required analyses and carry out the action plan, with the support of experts in the various functions involved.
In the preventive treatment of the risk, the following types of actions can generally be identified:

- Preventive actions to remove the cause of the risk;
- Mitigation actions to reduce the probability;
- Mitigation actions to reduce the impact (such as shift the risk to different subjects in order to reduce its impact).

The Risk Specialist is in charge of compiling the Risk Detail Sheets (see example below) with all the initial data required and keep it updated, reporting on request to the first level management and the Risk Manager.
Where necessary, a measurable plan of the actions must be associated to the Risk Detail Sheet, with an indication of the persons in charge of the actions and the dates of implementation. The risk management plans must be supported by a cost/benefit analysis to obtain a useful opinion for any allocation of additional funds.

Risk No.:	(1)	**Division / Department:**	(2)	**Risk Owner:**	(3)
Risk category:	(4)	**Category description:**	(5)	**Risk Specialist:**	(6)
DATE of sheet opening	**dd/mm/yy**	DATE Expected Closure	**dd/mm/yy**		

Risk description		**Probability Index**	**Impact Index**	**RISK Index**
(7)	**Initial**	(8)	(9)	10)
	Current	(8)	(9)	(10)
	Target	(8)	(9)	(10)
	Residual	(8)	(9)	(10)

Root Causes
(11)

Risk Mitigation Strategy
(12)

Current State

Action No.	**Description of Action**	**Target Date**	**Actual Date**	**Comments / Notes**
(13)	(14)	**dd/mm/yy**	**dd/mm/yy**	(15)

Example of risk detail sheet

Any Corrective Actions

If the risk has already occurred, intervention is required to implement all corrective actions to limit the consequences and relative economic impact.
The Risk Manager is responsible for immediately convening an operational team, assigning the responsibility to a first level manager and appointing a Risk Specialist to carry out the analysis and define an action plan which must be validated by the Director.

Control of progress and supervision

To guarantee the effectiveness of the Risk Management process, it is important for the first level managers to periodically control the progress and effectiveness of the corrective actions defined or implemented under their responsibility, with the support of the Risk Specialists.

It is also decisive for HIGH risks, that the Risk Manager directly coordinates and carries out these periodic controls to ensure the effective reduction of the level of risk.
The frequency of these checks depends on the risk class (HIGH, MODERATE, LOW) identified, present in the Risk Register and being managed, and is decided by the Risk Manager.

Phase 4: Risk monitoring

Periodic risk review

The factors which may influence the probability and impact of a consequence may change over time, as do the factors which influence the applicability or cost of the various actions identified.
Consequently the Risk Management process must be repeated regularly, re-analysing the contents of the Risk Register and relative Risk Detail Sheets both for risks already managed and risks being mitigated. The Risk Specialists, each one for the activities they are responsible for, must periodically repeat the identification phase to check if new risks, which initially were not identified, may occur.
The closure of a Risk is feasible only when, following the implementation of the mitigation actions, the risk class has become LOW (i.e. with RI>11)
The review must be coordinated by the Risk Manager.
It is reasonable to expect that the periodic risk review be done at least once a year and on that occasion the Risk Manager reports on the results to the General Management.

Management of Residual Risks

Each risk identified and present in the Risk Register must be evaluated by the Risk Specialist with the support of the first level manager in terms of the costs the company would incur if the risk occurred.
The potential economic impact which, at the full discretion of the Risk Manager, could be subject to reserves or coverage, can be evaluated as: (Cost of the Risk) x (Probability of occurrence).

Reporting

The Risk Manager is responsible for periodically issuing (at least once a year) a Risk Management report.

3.2 Implementation of the ICRMS in subsidiaries

As part of its management and coordination activities, Avio S.p.A. adopts a single Group internal control and risk management system, ensuring the effective control of both the Group's strategic choices as a whole and the balanced management of the individual components.
To guarantee the appropriate operation of the ICRMS, the subsidiaries must therefore comply with these guidelines in establishing and maintaining their own ICRMS, consistently with the strategies and policies of Avio S.p.A., concerning controls, without prejudice to the compliance with any individually applicable regulations.
Within the ICRMS, Avio S.p.A. defines some corporate instruments, roles, rules and regulations as part of its own management and coordination activities for the subsidiaries. This fosters the pursuit of company objectives using an approach aiming for overall coherence, as well as the enhancement of common characteristics through synergies.
This approach uses common and coordinated actions for the transversal issues affecting the subsidiaries, with appropriate information flow from the subsidiaries to the Parent company, as well as the implementation of appropriate monitoring activities. The monitoring aims to verify the compliance by the subsidiaries with the instructions issued concerning the ICRMS and does not therefore include the checking and responsibilities that the ICRMS of each subsidiary is appropriate and functional as a whole.
Within their own autonomy and independence, the subsidiaries implement the ICRMS guidelines issued by Avio S.p.A. adapting them to their own organizational and operational context and to any specific regulations which may be applicable.
In particular, the BoD, or equivalent body in the subsidiary, is responsible for ensuring an appropriate and effective Internal Control and Risk Management System, ratifying these guidelines and taking on the roles and responsibilities laid down for the corresponding body in Avio S.p.A., limited to what is applicable to its own business and company organisation, without prejudice to the compliance with any specific regulations applicable to individual companies.
The Managing Directors or equivalent figures in the subsidiaries ensure the establishment and maintenance of an appropriate and effective ICRMS by implementing this document.
To allow Avio S.p.A. to perform its function of Group management and coordination to the best of its ability, any need for derogations to these guidelines by the subsidiaries must be notified to the Managing Director of Avio S.p.A.

3.3 Audit and continuous evaluation of the effectiveness of the ICRMS

The periodic audit of the suitability and effective operation, and any review of the ICRMS is an essential part of the structure of the ICRMS, to ensure its full and correct effectiveness.
This periodic audit is performed by the Board of Directors assisted by the Control and Risks Committee and the Appointed ICRMS Director.

In performing this audit, the Board of Directors will not only check the existence and implementation of an ICRMS within the company, but will also periodically proceed with a detailed examination of the structure of the System, its suitability and effective and concrete operation.

For this purpose, the Board of Directors shall receive and examine the reports drafted by the Head of Internal Audit, already examined in advance by the Control and Risks Committee and the Appointed ICRMS Director, to check that the structure of the system implemented in the company is suitable and concretely effective in the pursuit of the objectives and if any reported shortcomings imply the need for an improvement of the System.

Annually, during the meeting convened to approve the financial statements, the Board of Directors is also responsible for:

- examining the significant company risks brought to its attention by the Appointed ICRMS Director and evaluating how these were identified, evaluated and managed. For this purpose, particular attention must be paid to examining the changes taking place in the last financial year, the nature and extent of the risks and the evaluation of the response of the company to such changes;
- assessing the effectiveness of the ICRMS in tackling these risks, paying particular attention to any inefficiencies reported;
- considering which actions were undertaken or which must promptly be undertaken to correct these shortcomings;
- drafting any other policies, processes and rules of conduct which allow the company to react appropriately to new or not sufficiently managed risk situations.

3.4 Methods of coordination and cooperation among the parties involved in the ICRMS

The correct operation of the internal control and risk management system is based on the profitable interaction between the company control functions in the performance of their tasks.
An integrated system aims to achieve the following objectives:

- elimination of methodological/organisational overlapping among the different control functions;
- agreement on methodologies used by different control functions to perform the evaluations;
- improvement of communication between the control functions and the company bodies;
- reduction of the risk of "partial" or "unaligned" information;
- capitalisation of information and evaluations by different control functions.

The definition of coordination and cooperation methods among the company control functions facilitates the overall operation of the ICRMS and ensures an unambiguous and coherent representation to the top management and company bodies of the risks to which the Company and its subsidiaries are exposed.
For this purpose, among the key moments of coordination and cooperation among the control functions is the annual activity planning phase and the periodic meetings of all parties involved in the ICRMS, supported by the foreseen information flows, in which information is exchanged on the results of each function's activities and the evaluations carried out of any weaknesses in the internal control and risk management system, and defined/suggested remedial actions are agreed on.

3.5 Information flows among the parties involved in the ICRMS

The set of interrelations between the governance bodies, control functions and the management of Avio S.p.A. and its subsidiaries represents one of the fundamental operating mechanisms for the operation of the internal control system and the risk management process.
The definition of a model of interrelations makes it possible to identify the objectives pursued by the various bodies, in terms of concrete control needs linked to the fulfilment of the specifically assigned tasks and, in order to ensure an efficient and appropriate coordination between the players in the ICRMS in terms of contents and timing, requires the clear defining of roles and responsibilities.

For this purpose, the system of interrelations between the bodies and functions involved in the internal control system must be inspired by logics and principles of effectiveness, providing useful information to recipients, of efficiency, guaranteeing the correct weight between information needs and the costs of producing such information, completeness, clarity, accuracy and certainty of the information sent, the promptness of sending and updating key information, easy accessibility of information to authorised users and eventually confidentiality to protect the information.

Information flows to the company bodies of Avio S.p.A.

The information flows towards the company bodies aim to promptly and suitably transmit to these bodies the knowledge of the results of the activities undertaken by the company

control functions and any dysfunctions encountered, in order to be able to rapidly implement the required corrective actions.

The main flows towards the company bodies of Avio S.p.A. are shown below.

INFORMATION FLOW	RESPONSIBLE FUNCTION	RECIPIENTS	FREQUENCY
Three-years and annual Audit Plan	INTERNAL AUDIT	BoD Control and Risks Committee Board of Statutory Auditors Managing Director/ Appointed ICRMS Director COC 231	Annual
Audit Report	INTERNAL AUDIT	Chairman of the BoD Chairman of the Control and Risks Committee Chairman of the Board of Statutory Auditors Managing Director/ Appointed ICRMS Director COC 231 (for aspects under their responsibility)	Per event
Summary report on activities carried out and key findings	INTERNAL AUDIT	BoD Control and Risks Committee Board of Statutory Auditors Managing Director/ Appointed ICRMS Director COC 231	Six-monthly
Report on specific audit activities relating to Italian Legislative Decree no. 231/2001	INTERNAL AUDIT	COC 231, and at their indication, to: Chairman of the BoD Chairman of the Control and Risks Committee Chairman of the Board of Statutory Auditors Managing Director/ Appointed ICRMS Director	Per event
Report on activities carried out	COC according to Italian Legislative Decree no. 231/2001	BoD Chairman of the Control and Risks Committee Chairman of the Board of Statutory Auditors Managing Director/ Appointed ICRMS Director	Six-monthly
Report of the Manager in Charge	Manager in Charge	BoD Control and Risks Committee Board of Statutory Auditors COC 231 Managing Director/ Appointed ICRMS Director	Six-monthly
Risk Assessment Plan and risk monitoring/management	Risk Manager	BoD Chairman of the Control and Risks Committee Chairman of the Board of Statutory Auditors Managing Director/ Appointed ICRMS Director	Annual

INFORMATION FLOW	RESPONSIBLE FUNCTION	RECIPIENTS	FREQUENCY
Risks Report	Risk Manager	Chairman of the Control and Risks Committee Chairman of the Board of Statutory Auditors Managing Director/ Appointed ICRMS Director	Six-monthly
Reports on particularly significant events	INTERNAL AUDIT COC according to Italian Legislative Decree no. 231/2001	BoD Control and Risks Committee Board of Statutory Auditors Managing Director/ Appointed ICRMS Director COC 231	Per event