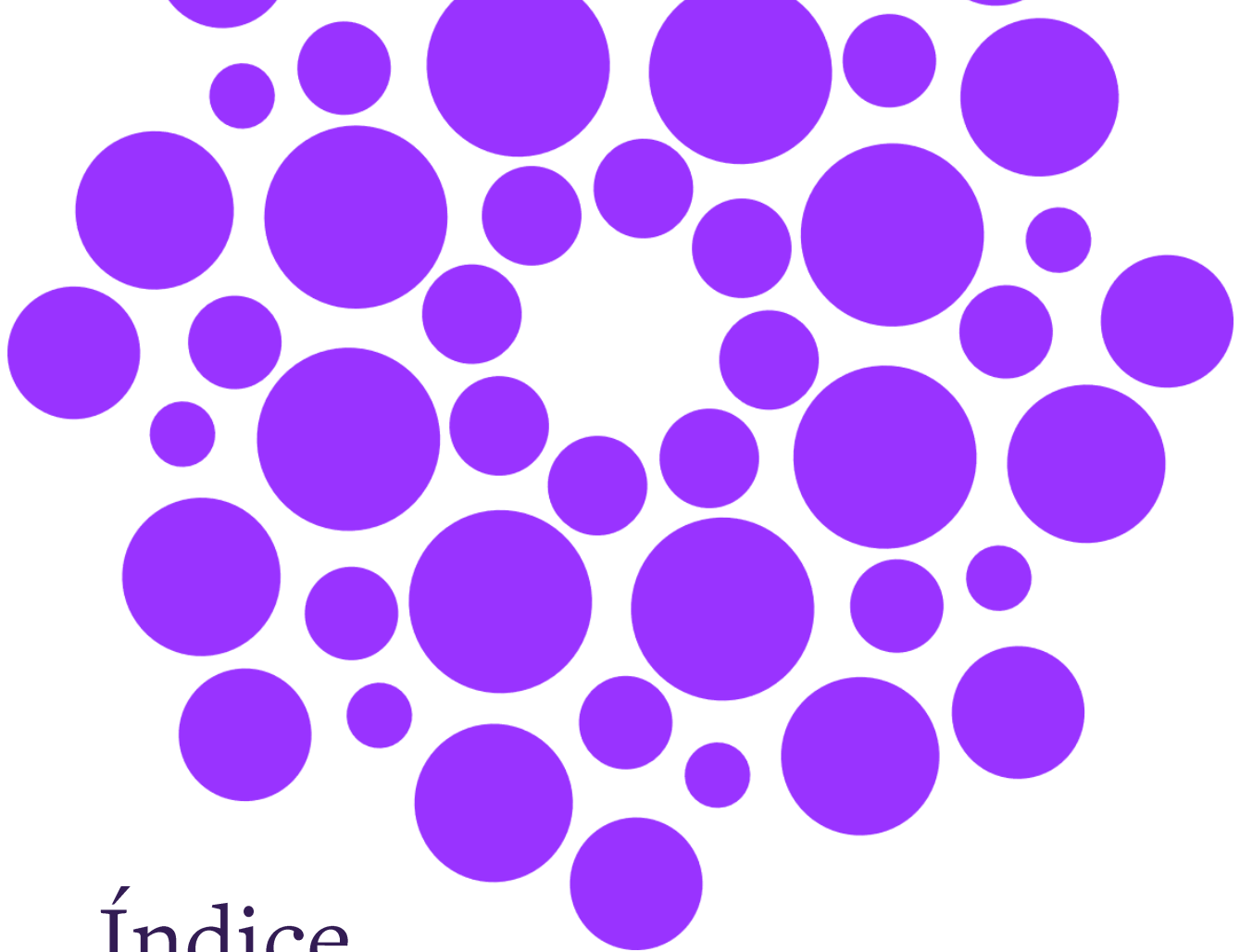


Risk Prevention Plan for Corruption and Related Offenses

2025 - 2028



Índice

Context.....	4
Presentation of the Entity.....	4
History.....	4
Mission and Values.....	5
Organization Structure	5
Risk Prevention Plan for Corruption and Related Offenses	8
Scope of Application.....	8
Concept of Corruption and Related Offenses.....	8
Compliance Officer	8
Methology for risk identification, assessment, and classification.....	9
Evaluation of preventive and corrective measures	11
Risk and control matrix	12
Monitoring, review and disclosure.....	13
Anexo I.....	14

Anexo II 16

Annex III.....33

Context

In the context of increasing legal and regulatory demands concerning the prevention of corruption and related offenses, Decree-Law No. 109-E/2021, of December 9, was published, which established the National Anti-Corruption Mechanism (“**MENAC**”) and set forth the General Corruption Prevention Regime (“**RGPC**”).

The RGPC requires entities within its scope to adopt and implement a Compliance Program (hereinafter referred to as the “**PCN**” or “**Program**”), which must include the following elements:

- Risk Prevention Plan for Corruption and Related Offenses;
- Code of Conduct;
- Whistleblowing Channel; and
- Training Program.

Based on the principles and values that inspired its creation, the Fundação GIMM - Gulbenkian Institute for Molecular Medicine (hereinafter “**GIMM**” or “**Entity**”) has progressively implemented internal mechanisms to ensure ethics and integrity in its activities, including measures for the prevention and mitigation of corruption and related offenses.

In this context, the present Risk Prevention Plan for Corruption and Related Offenses (“**RPP**”) outlines the corruption and related risks identified within GIMM’s operational scope, indicates the current and future prevention and mitigation measures to be implemented by the Entity, and describes the applicable methodology for risk classification and grading, along with the responsible parties for its application and monitoring.

Presentation of the Entity

History

Founded in 2023, GIMM is a private Portuguese foundation created by a group of public and private institutions. It is a non-profit entity with public utility status, dedicated to promoting scientific research and technological development in the field of life sciences and health.

It emerged from the combination of two research institutions of excellence in Portugal:

- The Gulbenkian Institute of Science (**IGC**), founded in 1961, became a renowned European center for international collaboration and scientific excellence in Portugal. With around 300 researchers from 45 nationalities across 27 research groups, the IGC attracted global talent to Portugal. Its pioneering PhD programs stimulated critical thinking and nurtured talent, inspiring the next generation of scientific leaders; and
- The João Lobo Antunes Institute of Molecular Medicine (**iMM**), founded in 2002, quickly established itself as a dynamic force in biomedical research, hosting around 485 researchers from 25 nationalities across 30 research groups. Strategically located near major Portuguese educational institutions, the iMM fostered strong links to clinical

sciences and played a key role in shaping national science policy and responding to global challenges.

The creation of GIMM resulted from a shared desire to establish a world-class research institute that pushes the boundaries of scientific knowledge, addresses fundamental biological questions, and improves human health and global well-being.

Today, GIMM brings together approximately 700 researchers, 38 research groups, 8 spin-offs, and 18 support infrastructures.

Mission and Values

GIMM's mission is anchored in scientific excellence and social impact, structured around five key pillars:

- **Challenging frontier science:** promoting curiosity-driven research and interdisciplinary collaboration using cutting-edge technologies;
- **Advancing health outcomes:** combining discovery and application through translational and clinical research to develop innovative, data-driven, equitable health solutions;
- **Fostering innovation and translation:** prioritizing the practical application of scientific discoveries for the prevention, diagnosis, and treatment of disease;
- **Empowering the next generation:** supporting innovative training programs and career development opportunities for researchers from diverse backgrounds to thrive in cross-disciplinary science;
- **Beyond GIMM's walls:** shaping the national and European R&D ecosystem through collaboration, research and training excellence, and societal engagement.

GIMM promotes and upholds the values of Diversity, Equity, and Inclusion, both in its research mission and internal organizational culture.

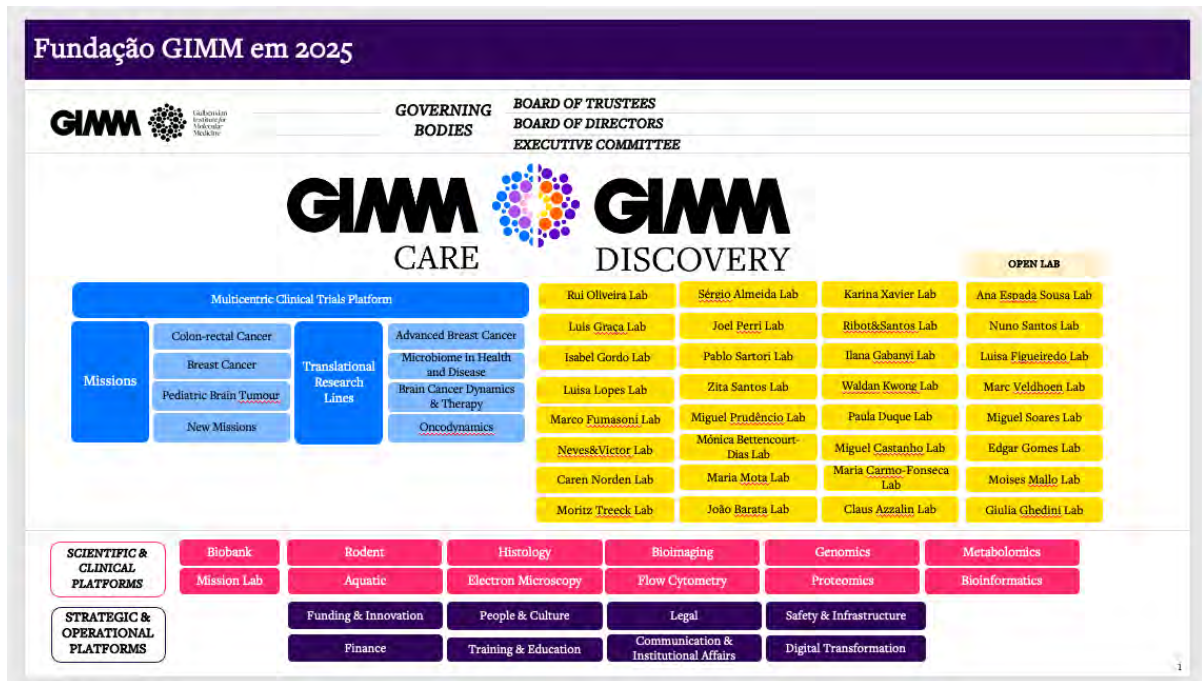
Organization Structure

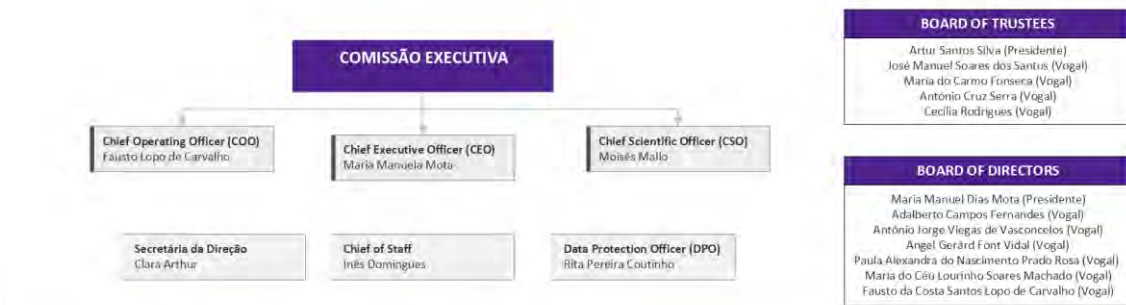
The GIMM is organized into an internal structure divided between GIMM Discovery and GIMM CARE. GIMM Discovery consists of 38 laboratories whose main mission is the practice of discovery science. GIMM CARE focuses on scientific research applied to the improvement of healthcare and quality of life. It is divided into three axes: Multicentric Clinical Trials Platforms; Missions (3); and Translational Research Lines (4).

GIMM Discovery and GIMM CARE are supported by Platforms. There are two types of platforms: Strategic and Operational Platforms, and Scientific and Clinical Platforms, which differ in the purpose of their activities (management and research, respectively).

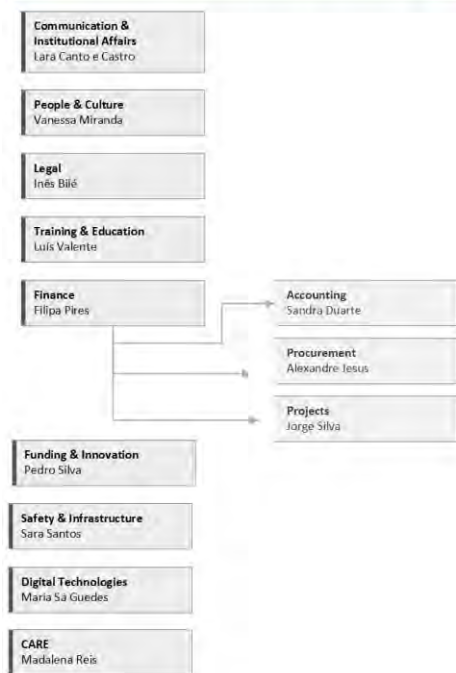
At the level of corporate governance, GIMM has an Executive Committee composed of three members, in addition to a Board of Trustees and a Board of Directors, whose functions, terms of office, and appointment procedures are duly stipulated in the foundation's statutes.

In this context, the organizational chart below illustrates the relevant internal areas of GIMM, indicating their respective leaders:

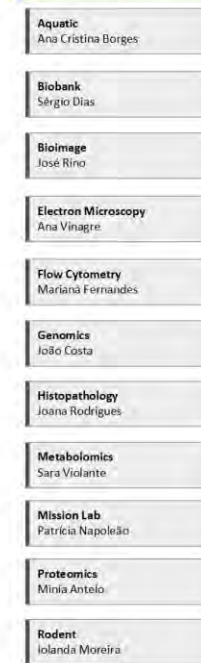




PLATAFORMAS ESTRATÉGICAS E OPERACIONAIS



PLATAFORMAS CIENTÍFICAS E CLÍNICAS



Risk Prevention Plan for Corruption and Related Offenses

Scope of Application

This document aims to meet the requirements established in the RGPC, specifically in Article 6, paragraph 1, which states:

Covered entities shall adopt and implement a Risk Prevention Plan for Corruption and Related Offenses that encompasses the entirety of their organization and activity, including administrative, management, operational, and support areas, and which must include:

- a) The identification, analysis, and classification of risks and situations that may expose the entity to acts of corruption and related offenses, including those associated with the exercise of functions by members of the management and executive bodies, considering the reality of the sector and the geographical areas in which the entity operates;*
- b) Preventive and corrective measures that reduce the likelihood of occurrence and the impact of the identified risks and situations.*

As a legal entity headquartered in Portugal that currently employs 50 or more individuals, GIMM qualifies as a “covered entity” under the terms of Article 2, paragraph 1 of the RGPC.

This RPP covers the entire structure and activity of GIMM. It applies to all its employees and researchers, regardless of their legal relationship with the Entity, as well as to all areas of operation, including management, administrative, operational, and support functions.

Concept of Corruption and Related Offenses

According to Article 3 of the RGPC, for the purposes of the Compliance Program (PCN), the term “corruption and related offenses” includes the crimes of corruption, undue receipt or offer of advantage, embezzlement, economic participation in business, extortion, abuse of power, misconduct in public office, influence peddling, money laundering, or fraud in obtaining or diverting subsidies, grants, or credit, as set forth in the Portuguese Penal Code (Decree-Law No. 48/95, of March 15, as amended).

Additional offenses associated with corrupt practices, which are also detrimental to the proper functioning of organizations, can be found in separate criminal legislation.

Annex I of this RPP provides a non-exhaustive list of corruption and related offenses for which private sector legal entities may be held liable under Article 11 of the Penal Code.

Compliance Officer

GIMM’s Legal Department is responsible for monitoring the implementation of this RPP and ensuring compliance with the requirements set out in the RGPC. The department reports directly to the Entity’s executive and top management bodies.

For the purposes of Article 5, paragraphs 2 and 4 of the RGPC, Inês Bilé is designated as the Compliance Officer (“RCN”), currently serving as Head of Legal at GIMM.

The appointed Compliance Officer performs her duties independently, on a permanent basis, and with decision-making autonomy. She has access to internal information and the necessary human and technical resources to effectively fulfill her responsibilities.

The responsibilities of the Compliance Officer include, among others:

- Coordinating the collection and systematization of the Entity’s ethical values and principles of conduct, as well as defining appropriate behavioral guidelines to ensure compliance. This includes promoting and ensuring the participation of all members, particularly top management and middle management, in the processes of drafting and updating the Code of Ethics and Conduct.
- Coordinating the identification and risk analysis of corruption and related offenses, along with the definition of preventive measures. This involves ensuring the engagement and collaboration of the Entity’s hierarchical structure in preparing and updating the Risk Prevention Plan (RPP), as well as in evaluating its implementation.
- Ensuring compliance with deadlines for communication, disclosure, and public availability of the Code of Ethics and Conduct, the RPP, and the related performance assessment reports.
- Monitoring and verifying compliance with the operational requirements of the internal whistleblowing channel to be implemented within the Entity. This includes ensuring the protection of whistleblowers, confidentiality and discretion, meeting deadlines, and preventing conflicts of interest.
- Collecting and organizing information related to training needs in the areas of ethics, integrity, and the prevention of corruption and related offenses. The Officer is also involved in developing training programs and monitoring their completion.
- Assessing the need to update various instruments of the Compliance Program (PCN).

Methodology for risk identification, assessment, and classification

The methodology used in the development of this RPP involved identifying and assessing risks, reviewing the preventive and corrective measures currently in place at the Entity, and planning and recommending additional measures to be implemented in due course to strengthen existing controls.

To that end, a thorough and detailed analysis of GIMM’s key internal areas was carried out. This allowed for a comprehensive understanding of its operations and procedures (formalized or in the process of formalization), in order to identify the activities and responsibilities that could pose significant risks of corruption and related offenses.

Nevertheless, the risk identification, assessment, and classification process took into account the fact that the Entity was recently established and is still in a transitional phase, particularly regarding procedures inherited from the former IMM and IGC.

The risks listed in this RPP are assessed in terms of their probability of occurrence according to the following scale:

Probability of occurrence	Very remote	Remote	Likely	Very likely	Almost certain
	1	2	3	4	5

	It is likely never to happen or happen again.	We do not expect it to happen or happen again, but it is possible.	It may happen or happen again occasionally.	It will probably happen or happen again, but not systematically.	It will undoubtedly happen or happen again, and possibly frequently.
--	---	--	---	--	--

Each risk may affect more than one pillar simultaneously. The overall assessment of each risk follows the formula:

Risk impact	Very low	Low	Medium	High	Critical
Score	1	2	3	4	5
	<ul style="list-style-type: none"> - Minor impact on public image - Minor cost and schedule deviations - Occasional failures in non-critical services - Minimal impact on safety, health, or the quality of the Entity's activities <p>Require simple corrective actions.</p>	<ul style="list-style-type: none"> - Minor budget deviations - Occasional delays - Minor health and safety issues - Brief service interruptions - Formal complaints from staff, sponsors, researchers, funders, clients and/or suppliers - Decline in the quality of the Entity's activities <p>Require improvement actions</p>	<ul style="list-style-type: none"> - Unbudgeted expenses - Significant delays - Health and safety impacts - Moderate environmental and reputational implications - Unauthorized disclosure of confidential business information - Local-level operational failures - Dissatisfaction among staff, sponsors, researchers, funders, clients and/or suppliers 	<ul style="list-style-type: none"> - Significant operational and financial failures - Legal and regulatory non-compliance - Clear negative impact on the quality of the Entity's activities - Harm to the Entity's credibility with the public and scientific community <p>Require urgent corrective actions.</p>	<ul style="list-style-type: none"> - Disastrous consequences for the organization - Total loss of trust from public and scientific community - Severe damage to brand image and credibility - Major impact on health, safety, and activity quality - Serious legal and regulatory violations - Catastrophic financial, operational, and reputational damage

			Require improvement actions.		Require urgent corrective actions.
--	--	--	------------------------------	--	------------------------------------

The inherent risk classification is calculated using the formula mentioned earlier: **Risk Rating = Probability × Impact**. This is applied using a predefined matrix:

Probability	Impact				
	Very low (1)	Low (2)	Medium (3)	High (4)	Critical (5)
Almost certain (5)	Moderate (5)	High (10)	Critical (15)	Critical (20)	Critical (25)
Very likely (4)	Moderate (4)	High (8)	High (12)	Critical (16)	Critical (20)
Likely (3)	Low (3)	Moderate (6)	High (9)	High (12)	Critical (15)
Remote (2)	Low (2)	Moderate (4)	Moderate (6)	High (8)	High (10)
Very remote (1)	Low (1)	Low (2)	Low (3)	Moderate (4)	Moderate (6)

Evaluation of preventive and corrective measures

GIMM has a set of preventive and corrective measures in place to address the risks of corruption and related offenses to which it may be exposed. These measures vary in nature and may consist of general principles, procedures and policies, physical or digital controls, among others.

Nevertheless, upon completing its current transition phase, GIMM also plans to implement additional risk mitigation measures. These may include practices already adopted by the former iMM and IGC, as well as new actions tailored to the specific characteristics and needs of the Entity. Such measures will be subject to future discussion and approval.

In addition to other existing or planned actions, the following measures are currently in place:

- Creation of a Code of Ethics and Conduct applicable to all GIMM employees and researchers, including top management;
- Implementation of a General Privacy and Data Protection Policy;
- Implementation of a Gender Equality Policy;
- Implementation of a Workplace Safety Management Manual;

- Adoption of international guidelines and best practices related to the ethical, legal, and social implications (ELSI) of scientific research;
- Development of a structured procurement procedure, in accordance with the internal Approval/Authorization Matrix;
- Stratification of decision-making processes among the Executive Committee, Board of Directors, and Board of Trustees, based on predefined rules in the Foundation’s bylaws; and
- Initial and ongoing training of employees and researchers, including topics on ethics, integrity, and workplace safety.

These measures are evaluated for their effectiveness in reducing the likelihood and/or impact of associated risks, as per the following logic:

Evaluation of preventive and corrective measures	
Not effective	It has no impact on the identified risk.
	The preventive and corrective measures are not fully effective given the nature and characteristics of the risk, thus the probability of occurrence remains unchanged.
Partially effective	Reduces the probability level by 1.
	The preventive and corrective measures are partially effective given the nature and characteristics of the risk, reducing its probability of occurrence to lower levels.
Effective	Reduces the probability level to 1 and decreases the impact level by 1.
	The preventive and corrective measures are effective given the nature and characteristics of the risk, reducing its probability of occurrence to minimal levels.

Some specific preventive or corrective measures may have a greater effect than indicated in the standard matrix, acting both on the likelihood and impact dimensions simultaneously.

Risk and control matrix

Annex II lists the identified risks of corruption and related offenses, organized by the operational areas of the Entity, indicating the relevant platform (Strategic/Operational or Scientific/Clinical) and the internal department concerned. Additionally, transversal risks — those not limited to a single platform or area — have been identified.

Each of these risks was assessed in terms of its probability of occurrence and potential impact. Corresponding mitigation controls were also identified, including relevant principles, policies, regulations, and other applicable prevention documents, as well as existing operational mitigation measures.

Once the **Inherent Risk** has been assessed — classifying risks by their likelihood and impact — a risk score and corresponding risk level are obtained.

The Control Effectiveness Level (categorized as Not Effective, Partially Effective, or Effective) is then evaluated. This level reflects the preventive and mitigation measures implemented and applicable to the specific risk, and determines their effect in reducing the likelihood and/or impact of its occurrence.

By applying the existing measures and calculating their impact on the risk score (Probability × Impact), the **Residual Risk** is determined — that is, the remaining risk after implementing said measures. Depending on the effectiveness level of the control, the residual risk may remain the same as the inherent risk or may be reduced.

Finally, considering the early stage in which the Entity currently operates, control measures planned for future implementation are also identified (i.e., policies, procedures, and systems under internal discussion/development, not yet fully approved or implemented).

Monitoring, review and disclosure

In line with its goal of continuous improvement, the monitoring of this RPP will involve reviewing and testing the effectiveness of controls, collecting documentation and records as evidence of their implementation, and periodically evaluating potential areas for improvement.

In compliance with Article 6, paragraph 4, subparagraphs a) and b) of the RGPC, the monitoring process shall also include:

- By October of each year, the preparation of an interim evaluation report regarding any situations identified as high or maximum risk;
- By April of the following year, the preparation of an annual evaluation report, including a quantification of the implementation level of the preventive and corrective measures identified, as well as a projection for their full implementation;
- Any other periodic communications required by the competent national authorities, including those stated in recommendations and/or guidance issued by MENAC.

According to Article 6, paragraph 5 of the RGPC, this RPP will be reviewed every three years, or whenever a significant change in the Entity's structure or responsibilities occurs that would warrant a revision.

To ensure general awareness of its content, this RPP and the related evaluation reports will be made available to all GIMM employees/researchers via the intranet, and will be published on the Entity's official website, in accordance with the timeline set out in Article 6, paragraph 6 of the RGPC.

List of Corruption Offenses and Related Violations

Crimes	Relevant violations
<p>Money Laundering</p> <p>Art. 368.º-A Portuguese Penal Code</p>	<p>Anyone who converts, transfers, assists, or facilitates the conversion or transfer of proceeds obtained by themselves or by others, directly or indirectly, with the aim of concealing their illicit origin or preventing the offender or participant from being criminally prosecuted or sanctioned; anyone who conceals or disguises the true nature, origin, location, disposition, movement, or ownership of the proceeds, or the rights thereto; or, not being the author of the predicate offense, acquires, possesses, or uses such proceeds, knowing their illicit nature at the time of acquisition or initial possession/use.</p> <p>Penalty: Imprisonment up to 12 years.</p>
<p>Active Corruption in the Private Sector</p> <p>Art. 9.º, Law 20/2008, 21st of April</p>	<p>Anyone who, by themselves or through another person with their consent or ratification, gives or promises to a private sector employee, or to a third party with their knowledge, an undue material or immaterial advantage for the intended purpose.</p> <p>Penalty: Imprisonment up to 5 years or a fine up to 600 days.</p>
<p>Active Corruption</p> <p>Art. 374.º Portuguese Penal Code</p>	<p>Anyone who, by themselves or through another person with their consent or ratification, gives or promises to a public official, or to a third party indicated by or with the knowledge of the official, an undue material or immaterial advantage for performing or omitting any act contrary to the duties of their position, even if prior to the offer or acceptance.</p> <p>Penalty: Imprisonment from 1 to 5 years.</p>
<p>Corruption Affecting International Trade</p> <p>Art. 7.º, Law 20/2008, Law 21st of April</p>	<p>Anyone who, by themselves or through another person with their consent or ratification, gives or promises to a national, foreign, or international organization official, or to a national or foreign political officeholder, or to a third party with their knowledge, an undue material or immaterial advantage to obtain or retain a business, contract, or other undue advantage in international trade.</p> <p>Penalty: Imprisonment from 1 to 5 years.</p>
<p>Passive Corruption in the Private Sector</p> <p>Art. 8.º Portuguese Penal Code</p>	<p>Anyone who, by themselves or through another person with their consent or ratification, requests or accepts, for themselves or for a third party, an undue material or immaterial advantage or its promise, in exchange for any act or omission that violates their functional duties.</p>

	<p>Penalty: Imprisonment from 1 to 8 years and a fine up to 600 days.</p>
<p>Fraudulent Obtaining of Credit</p> <p>Art. 38.º, DL n.º 28/84, 20th January</p>	<p>Anyone who, when submitting a proposal for granting, maintaining, or modifying credit terms for a business or company:</p> <p>(a) provides inaccurate or incomplete written information intended to support the application or relevant to the decision;</p> <p>(b) uses documents with inaccurate or incomplete financial data, such as balance sheets, income statements, asset descriptions, or expert reports; (c) conceals financial deterioration occurring after the application that is relevant to the decision.</p> <p>Penalty: Imprisonment up to 3 years and a fine up to 150 days.</p>
<p>Misuse of Subsidy, Grant or Credit</p> <p>Art. 37.º, DL 28/84, 20th January</p>	<p>(1) Anyone who uses funds obtained as subsidies or grants for purposes other than those legally intended shall be punished. (2) The same applies to using subsidized credit for purposes not foreseen by the authorized credit line. (3) If the value or damage caused is considerably high, the penalty increases. (4) If repeated in the name and interest of a legal entity without voluntary reparation, the court may order its dissolution. Penalty: Imprisonment up to 2 years or fine of at least 100 days; 6 months to 6 years and fine up to 200 days if values are high</p>
<p>Fraudulent Obtaining of Subsidy or Grant</p> <p>Art. 36.º, DL 28/84, 20th January</p>	<p>Anyone who obtains a subsidy or grant: (a) by providing inaccurate or incomplete information about themselves or third parties relevant to the award; (b) by omitting relevant facts contrary to legal requirements; (c) by using documents obtained through false or incomplete information.</p> <p>Penalty: Imprisonment from 1 to 5 years and fine of 50 to 150 days. In particularly serious cases, imprisonment from 2 to 8 years.</p>
<p>Undue Receiving or Offering of Advantage</p> <p>Art. 372.º Portuguese Penal Code</p>	<p>Anyone who, in the exercise of their duties or because of them, directly or through another person with their consent or ratification, requests or accepts, for themselves or a third party, an undue material or immaterial advantage; or gives or promises such advantage to a public official, or a third party with their knowledge, in connection with their duties.</p> <p>Penalty: Imprisonment up to 3 years or fine up to 360 days.</p>
<p>Influence Peddling</p> <p>Art. 335.º Portuguese Penal Code</p>	<p>Anyone who, by themselves or through another person with their consent or ratification, requests or accepts, for themselves or a third party, an undue material or immaterial advantage or its promise, to abuse their real or supposed influence with any public entity, domestic or foreign.</p> <p>Penalty: Imprisonment from 1 to 5 years.</p>

Anexo II

Risks and controls matrix

Risk classification		Inherent risk					
Risk owner	Risk	Probability	Impact	Inherent Risk	Control Level	Implemented Policies and Controls	Residual Risk
Organization-wide	Approval of scientific projects for internal or external funding without proper verification of their ethical, legal, and social implications (ELSI), with the intention of obtaining/granting advantages or benefits, including the favoring or disfavoring of certain candidates/groups/entities.	Remote	High	High Risk	Partially effective	<p>- Code of Ethics and Conduct</p> <p>- Technical analysis of potential conflict of interest situations by relevant internal departments (e.g., Funding & Innovation and Legal), requiring, if the employee is authorised to remain in their role, the signing of a declaration confirming the obligation to immediately terminate the relationship in question should an eventual incompatibility of functions and/or research objectives arise;</p> <p>- Recusal of employees and/or researchers from decision-making processes that may give rise to conflicts of interest due to other positions or functions they hold.</p>	High risk
Organization-wide	Improper manipulation of scientific research methods and/or results due to pressure, influence, bribery, or promises of benefits from funders/sponsors of the project.	Remote	Critical	High risk	Effective	<p>Code of Ethics and Conduct.</p> <p>Project execution schedule, indicating the types of work to be carried out and specific research objectives, without the possibility of unilateral modification by the funder.</p> <p>Compliance with scientific integrity rules and good research practices by GIMM staff/researchers, under the supervision of the respective leaders of scientific laboratories/platforms.</p> <p>Provision and storage of raw/primary research data to allow verification of processed results during project execution.</p> <p>Electronic lab book for systematic recording of data related to ongoing research in each laboratory.</p> <p>Peer review for validation of research data by other experts in the field prior to publication of results.</p>	Moderate Risk

<p>Organiz ation- wide</p>	<p>Improper interactions with national or European public/private entities in the context of implementing partnership or collaboration agreements, likely to give rise to actual or potential conflicts of interest, with the intent to obtain or grant advantages and/or to influence business decisions.</p>	<p>Likely</p>	<p>High</p>	<p>High risk</p>	<p>Partially effective</p>	<p>Code of Ethics and Conduct. Involvement of multiple representatives from both GIMM and the partner entities in meetings for the negotiation of partnerships and contracts (i.e., communications are not centralised in a single point of contact). Internal allocation of project oversight teams based on the nature of each research activity (i.e., there is no exclusivity in GIMM interlocutors engaging with a specific funder). Stratification of strategic management decision-making, with the participation of the Executive Committee, Board of Directors, and Board of Curators, whose members have predefined mandates, functions, and appointment procedures set out in the statutes. Limitation of voting/decision-making power of representatives from founding/supporting entities that contribute financially to GIMM, including the Calouste Gulbenkian Foundation.</p>	<p>High risk</p>
<p>Organiz ation- wide</p>	<p>Lack of independence and impartiality in the process of identifying and selecting projects/researchers for internal or external funding opportunities, resulting from the existence of conflicts of interest (personal, financial, political, or professional).</p>	<p>Very Remote</p>	<p>Medium</p>	<p>Low risk</p>	<p>Partially effective</p>	<p>Code of Ethics and Conduct. Identification and compilation of major external funding programmes and opportunities by the Pre-Award Department, with general dissemination to all GIMM staff/researchers via a regular newsletter. Internal call to identify and select candidates interested in applying for external funding opportunities that allow only one application per institution, with project proposals submitted for evaluation by the Executive Committee. Project management system including (i) recording of internal evaluations, contacts with funders/investors, supporting documentation for the application process, and task execution status for each party involved; (ii) issuance of a final report indicating the outcome of each case (e.g., whether the technology failed in testing, the patent was rejected, a company was created, a licensing deal was signed, etc.); and (iii) restricted access to project managers linked to each process, with monitoring of all changes made by each user. Internal funding is limited to (i) the availability of budget for this purpose; (ii) the submission of a form by the interested researcher justifying the request and describing the proposed project; and (iii) a technical feasibility analysis by the Chief Scientific Officer, followed by submission to the Executive Committee for approval.</p>	<p>Low risk</p>

<p>Organization-wide</p>	<p>Falha na adoção de critérios equitativos e transparentes na alocação de recursos internos do GIMM (humanos e/ou materiais) em projetos envolvendo parceiros externos (em regime de prestação de serviços e/ou de colaboração), resultando na priorização de interesses de terceiros em detrimento do GIMM, na obtenção/concessão de vantagens indevidas e/ou na criação de conflitos de interesse.</p>	<p>Likely</p>	<p>Medium</p>	<p>High risk</p>	<p>Partially effective</p>	<p>Code of Ethics and Conduct. Predefined pricing table for the use of GIMM facilities and resources, with differentiated rates based on the nature/purpose of the use (i.e., reduced costs for internal laboratories/increased costs for external for-profit entities). Prioritisation of GIMM's internal needs when allocating human and material resources to research projects.</p>	<p>Moderate risk</p>
<p>Organization-wide</p>	<p>Entering into contracts, agreements, and/or partnerships with third-party entities that (i) have poor public image, reputation, or integrity; (ii) are associated with investigations and/or adverse judicial decisions; (iii) are subject to sanctions imposed by the European Union, United Nations, or other States; and/or (iv) have shareholders, directors, beneficial owners, or key representatives who are Politically Exposed Persons (PEPs) or are involved in investigations, adverse judicial decisions, and/or included on sanctions lists.</p>	<p>Remote</p>	<p>Critical</p>	<p>High risk</p>	<p>Partially effective</p>	<p>Code of Ethics and Conduct. Mapping and selection of funding/support opportunities with background checks to verify the technical, financial, and commercial credentials of investors. Legal analysis and assessment of the feasibility of the terms and conditions of material transfer agreements, licensing agreements, collaboration/consortium agreements for joint research, agreements regulating research results ownership, research sponsorship agreements, confidentiality agreements (NDAs), and others by the Legal Department. Support from external legal counsel for the review and validation of contracts involving technical specificities and/or significant associated costs.</p>	<p>Moderate risk</p>

<p>Organization-wide</p>	<p>Involvement in and/or facilitation of money laundering practices due to the absence of control and monitoring mechanisms in the donation receipt process.</p>	<p>Very Remote</p>	<p>High</p>	<p>Moderate risk</p>	<p>Partially effective</p>	<p>Code of Ethics and Conduct. Issuance and registration of invoice-receipts for donations received by GIMM. Pre-verification procedure for any refund requests related to donations made through the electronic platform available on the GIMM website.</p>	<p>Moderate risk</p>
<p>Scientific and Clinical Platforms</p>	<p>Unauthorised access, handling, and/or transfer of personal data, human samples, and/or any sensitive and confidential information originating from databases managed by GIMM in collaboration with external partners.</p>	<p>Very Remote</p>	<p>Critical</p>	<p>Moderate risk</p>	<p>Effective</p>	<p>Code of Ethics and Conduct. General Privacy and Data Protection Policy. Data Classification Policy, with criteria for identifying data processing operations involving higher levels of risk. Cybersecurity training made available to staff through the platform of the National Cybersecurity Centre (CNCS). Strategic Information Risk Management Plan, developed in collaboration with the Digital & Technology Department, including (i) criteria for assessing the sensitivity level of information; (ii) tools to detect vulnerabilities in internal systems; and (iii) mitigation measures for identified risks. Restricted digital access for GIMM staff to only those platforms/systems strictly necessary for the performance of their duties. Prior review of research projects involving access to, use of, or transfer of personal data by the Data Protection Office, to ensure legal and regulatory compliance under the General Data Protection Regulation (GDPR) and other applicable rules. Validation of Data Protection Agreements by the Legal and Data Protection Departments in cases involving highly sensitive data requiring additional security measures. Informed consent form for the donation of samples to the biobank and for participation in research projects, in accordance with the Clinical Research Law and the GDPR. Prior data protection risk impact assessment for materials stored in the biobank, in accordance with GDPR rules. Biobank management regulations, drafted by the Local Health Unit of Hospital Santa Maria and approved by the Portuguese Data Protection Authority, including (i) strict control over the entry and exit of samples; (ii) coding of samples to enable traceability while protecting donor identity; and (iii) oversight of activities by the Ethics Committee of Hospital Santa Maria (external to GIMM). Biobank IT system hosted on an independent network (i.e., not linked to GIMM's internal network) with additional layers of protection.</p>	<p>Moderate risk</p>

Scientific and Clinical Platforms	Acts of plagiarism and/or fraud in the production of scientific work by GIMM researchers, with the intent to obtain undue advantages and/or to appropriate the intellectual or industrial property rights of others.	Likely	High	High risk	Partially effective	Code of Ethics and Conduct. Compliance with scientific integrity rules and good research practices by GIMM staff/researchers, under the supervision of the respective leaders of scientific laboratories/platforms. Provision and storage of raw/primary research data to allow verification of processed results during project execution. Electronic lab book for system-based recording of data related to ongoing research in each laboratory. Peer review for validation of research data by other researchers in the field prior to publication of results. Monitoring of major scientific publication platforms by research group/scientific platform leaders at GIMM to detect and identify potential cases of plagiarism and/or fraud. Patent searches and, where justified, freedom-to-operate analyses to assess potential infringement of third-party IP rights.	High risk
Scientific and Clinical Platforms	Improper and/or fraudulent allocation of ownership of scientific work produced at GIMM, with the intent to obtain benefits of any kind and/or to unjustly favour a particular staff member, research group, or external entity.	Remote	High	High risk	Partially effective	Code of Ethics and Conduct. Email or written protocol record of the terms and conditions of certain scientific collaborations (i.e., in more complex projects, involving sensitive data or where such documentation is required by the funder), defining the parties' commitments and the allocation of potential results arising from the collaboration. Completion of invention disclosure forms by research teams, with detailed recording and description of the inventive activity, the responsible inventors, and the respective contribution percentage of each researcher involved. Clarification of any doubts and/or disputes concerning the ownership of scientific research results by the Tech Transfer Department. Possibility of commissioning an independent expert opinion by professionals specialised in patent registration, in more complex cases. Execution of Intellectual Property Ownership Agreements to formalise the intellectual/industrial	Moderate risk

						property rights resulting from scientific work carried out at GIMM, subject to validation by the Funding & Innovation and Legal Departments.	
Scientific and Clinical Platforms	Approval of scientific projects for internal or external funding without proper verification of their ethical, legal, and social implications (ELSI), with the intent to obtain or grant advantages and/or benefits, including the favouring or disadvantaging of specific candidates, groups, or entities.	Remote	High	High risk	Partially effective	Code of Ethics and Conduct. Prior approval of projects involving human samples by external experts formally appointed to the Ethics Committee of the Lisbon Academic Medical Centre (CAML), with a favourable opinion required to support the project's funding application. Prior approval of projects involving animal welfare by the Directorate-General for Food and Veterinary Affairs (DGAV), with a favourable opinion required to support the project's funding application. Monitoring of funding application processes by the Funding & Innovation Department to ensure compliance with the requirements and conditions set by each funding entity. Verification of research compliance with applicable ethical standards for the publication of results in scientific journals. Peer review for validation of research data by other researchers in the field prior to publication.	Moderate risk
Scientific and Clinical Platforms	Fraud or manipulation in the process of selecting intellectual assets for the creation and development of start-ups supported by GIMM, with the intent to obtain or grant undue advantages and/or to favour specific projects or researchers.	Very remote	High	Moderate risk	Effective	Code of Ethics and Conduct. Specialised internal division (Tech Transfer Department) responsible for mapping and identifying research projects with potential for economic exploitation and patent registration. Preparation of a formal proposal by the GIMM Executive Committee describing the rationale for equity participation in the company, the development stage of the technology, the negotiations conducted during investment rounds, and other aspects related to the economic and commercial viability of the business to be supported. Submission of the proposal for prior approval by the Board of Directors.	Low risk

<p>Scientific and Clinical Platforms</p>	<p>Misappropriation, diversion, and/or improper use of funds, grants, subsidies, or similar support (national and/or European) in the context of funded scientific projects.</p>	<p>Remote</p>	<p>Critical</p>	<p>High risk</p>	<p>Partially effective</p>	<p>Code of Ethics and Conduct. Centralisation of expenses allocated to funded projects in individualised cost centres. Formalisation of Grant Agreements for partnerships involving projects funded by European funds, with detailed definition of the budget, project objectives, activity methodology, allocation of expenses and resources, among other practical aspects. Monitoring of funded project implementation by the designated Project Management Department officer, including (i) review of supporting documents submitted by researchers; (ii) assessment of the eligibility of expenses incurred, in accordance with the scientific and financial framework established in the corresponding project agreement; and (iii) financial reporting to the project's funding body, including justification of ineligible and/or questionable expenses. Periodic financial audits in line with the rules set by each funding entity, with the option to hire an external organisation or independent consultant to assist in the reporting process. Submission of progress reports and performance of interim audits (review meetings by external experts) to monitor the implementation status of projects exceeding certain funding thresholds, when requested by the funder. Post-completion storage of documentation relating to funded projects, allowing for ex post verification upon request by the funder. Signing of attendance sheets and photographic records to substantiate expenses related to researchers' participation in visits/travel/external events. Validation of financial reports by the Finance Department or the Project Management Department prior to submission to funders. Impossibility of deleting accounting records of ineligible expenses that have been reallocated/reclassified as indirect costs, thereby preserving the full accounting history of submitted project expenses. Cross-communication between managers representing the beneficiary and the funder, preferably through the designated electronic platform, with message history accessible to other project stakeholders.</p>	<p>Moderate risk</p>
--	--	---------------	-----------------	------------------	----------------------------	--	----------------------

<p>Scientific and Clinical Platforms</p>	<p>Misappropriation, diversion, or unauthorised transfer of equipment, materials, and other resources available in GIMM's facilities and laboratories by internal or external staff/researchers.</p>	<p>Likely</p>	<p>Medium</p>	<p>High risk</p>	<p>Partially effective</p>	<p>Access control to GIMM facilities through identification cards, with biometric identification mechanisms in place for controlled environments or areas involving high security risks (e.g., imaging laboratories, radioactive materials, animal facilities, among others). 24/7 security services provided by a specialised company at both GIMM locations (Lisbon and Oeiras), including the use of video surveillance tools. Authorisation from the respective laboratory/scientific platform leaders required for the entry of external researchers/visitors into GIMM facilities, with access restricted to the areas related to the scientific project they are involved in or observing. Computerised scheduling system for the use of laboratory equipment, identifying (i) the dates/times of use for each available piece of equipment; (ii) the designated staff responsible for each piece of equipment; and (iii) the usage guidelines and any specific features of the equipment. Equipment sharing/loan subject to (i) order of request in the scheduling system; (ii) the scientific need of the project; and (iii) the technical qualifications of the user to operate the equipment in question. Notification of the Safety & Infrastructure Department and the Chief Scientific Officer required for any change in equipment location, with the update recorded in the internal accounting system.</p>	<p>Moderate risk</p>
<p>Scientific and Clinical Platforms</p>	<p>Excessive renewal or extension of scientific equipment maintenance contracts without reviewing the negotiated terms and conditions, thereby avoiding new market consultations and/or bypassing the appropriate approval workflow.</p>	<p>Remote</p>	<p>Medium</p>	<p>Moderate risk</p>	<p>Partially effective</p>	<p>Code of Ethics and Conduct. Centralised workflow managed by the Procurement Department, including (i) stratification of approval levels based on the value/nature of the product or service being acquired; (ii) definition of specific monetary thresholds to determine the number of quotes to be requested from the market; (iii) recordkeeping of the selected quote/proposal for each purchase; and (iv) requirement for the requested item or service to be budgeted within the scientific platform's or project's cost centre to enable approval. Computerised maintenance management software that (i) centralises information on each equipment's maintenance contracts, preventive maintenance schedules, technical intervention reports, and other supporting documentation; and (ii) generates automatic alerts when scheduled maintenance or repairs are approaching, based on predefined maintenance plans.</p>	<p>Low risk</p>

Scientific and Clinical Platforms	Fraud in the process of obtaining, transferring, and maintaining licences and authorisations issued by the competent regulatory authorities for the operation of laboratories and the conduct of scientific activities subject to oversight.	Remote	Medium	Moderate risk	Effective	Regular inspections of GIMM laboratories/facilities by the competent regulatory authorities (e.g., Portuguese Environment Agency, IGAMAOT, among others), with visits accompanied by the Head of the Safety & Infrastructure Department and the respective managers of the areas under inspection. Issuance of specific licences for the operation of facilities/activities involving increased safety risks (e.g., laboratories using microorganisms and radioactive materials). Annual legal compliance audits in the areas of health and environment, conducted by an independent external entity. Occupational Safety Management Manual made available to all staff and researchers using GIMM facilities/laboratories.	Low risk
Strategic and Operational Platforms	Procurement, by decision of the Executive Committee, of goods and services that do not stem from actual needs of GIMM or whose costs are not reasonable/proportional to the nature/context of the expense, with the intent to benefit personal interests or those of third parties unrelated to GIMM.	Remote	Medium	Moderate risk	Partially effective	Code of Ethics and Conduct. Limited authorisation for the Executive Committee Secretariat to directly procure goods and services (e.g., booking of flights and accommodation in the context of corporate travel by members of the Management Board; contracting of catering, audiovisual and other services for internal events; purchase of low-value office supplies). Completion of internal forms, subject to validation by the Procurement Department, to justify the nature, legitimacy, and purpose of expenses to be reimbursed, particularly those related to travel, accommodation, and similar items. Centralised workflow managed by the Procurement Department, including (i) stratification of approval levels based on the value/nature of the product or service being acquired; (ii) definition of specific monetary thresholds to determine the number of quotes to be requested from the market; (iii) recordkeeping of the selected quote/proposal for each purchase; and (iv) requirement for the requested item or service to be budgeted within the scientific platform's or project's cost centre to enable approval.	Low risk
Strategic and Operational Platforms	Lack of independence, impartiality, autonomy, and/or transparency in decisions made by members of the Executive Committee for personal gain or to benefit third parties, in a manner that undermines or contradicts the	Remote	Critical	High risk	Effective	Code of Ethics and Conduct. Weekly meetings to discuss outstanding matters with the participation of all members of the Executive Committee and the Secretary/Chief of Staff. Consultation and collective decision-making by the Executive Committee members on matters with strategic, financial, and/or operational impact. Recording and archiving of meeting minutes and	Moderate risk

	interests and values of GIMM.					resolutions of the Executive Committee, Board of Directors, and Board of Curators. Formalisation of Executive Committee decisions via email for communication to the respective internal area leads. Stratification of relevant management decision-making among the Executive Committee, Board of Directors, and Board of Curators, whose members have predefined mandates, functions, and appointment procedures set out in the statutes. Limitation of the voting/decision-making power of representatives from the founding/supporting entities that provide financial contributions to GIMM, including the Calouste Gulbenkian Foundation.	
Strategic and Operational Platforms	Placement of electronic signatures on documents submitted for Executive Committee approval without proper review of their full content and/or without the prior consent of their respective holders, with the intent to benefit personal interests or those of third parties unrelated to GIMM.	Very remote	High	Moderate risk	Partially effective	Code of Ethics and Conduct. Centralised process for certified digital signatures under the responsibility of the Executive Committee Secretariat, with an internal workflow requiring (i) an explicit request from the head of the internal department requesting the signature; (ii) validation by the Legal Department for documents involving third-party relations, sensitive matters, and/or issues outside the scope of routine corporate management; and (iii) archiving of the signed documents in a folder maintained by the Executive Committee Secretariat/Chief of Staff, with the final version of the document sent by email to the signatory.	Moderate risk
Strategic and Operational Platforms	Manipulation and/or fraud in the communication and dissemination of data/results from scientific research conducted at GIMM due to pressure or influence from external partners and/or stakeholders, with the intent to obtain financial and/or reputational advantages.	Very Remote	Critical	Moderate risk	Partially effective	Code of Ethics and Conduct. Prior validation by the heads of the relevant scientific platforms/research areas for the dissemination and publication of articles, news, and any materials involving technical and scientific data. Development of marketing campaigns, event promotion, and management of social media and press relations with the support of specialised external agencies.	Moderate risk

Strategic and Operational Platforms	Establishment of partnerships with stakeholders and external entities to obtain non-competitive funding that result in irregular lobbying practices, bribery, and/or abuse of power to gain advantages and benefits.	Very remote	High	Moderate risk	Partially effective	Code of Ethics and Conduct. Fundraising plan, indicating the strategies to be adopted, expected financial impacts, and potential partners/sponsors to be contacted, prepared annually by the Communications Department. Approval of the annual fundraising plan.	Moderate risk
Strategic and Operational Platforms	Receipt of bribes or undue advantages for the selection, contracting, and/or favouring of a specific supplier, client, and/or business partner in the procurement process.	Remote	Medium	Moderate risk	Not effective	Code of Ethics and Conduct. Centralised workflow managed by the Procurement Department, including (i) stratification of approval levels based on the value/nature of the product or service being acquired; (ii) establishment of specific monetary thresholds to determine the number of quotes to be requested from the market; (iii) recordkeeping of copies of the selected proposal/quote for each purchase; and (iv) requirement for the requested item or service to be budgeted within the scientific platform's or project's cost centre to enable approval. Internal Approval Matrix requiring, among other controls, (i) prior analysis and validation by the Finance Department for purchases above EUR 50,000; and (ii) initiation of a public procurement process for purchases above EUR 100,000. Participation of at least two Procurement Department managers in meetings with suppliers reaching a certain annual purchase volume for negotiation of prices and contractual terms. Prohibition of invoicing expenses between members of the same consortium or affiliated entities within projects funded by European resources. Documentation, via email or system record, of requisitions submitted by staff/researchers and communications with suppliers for the submission of proposals/quotes.	Moderate risk
Strategic and Operational Platforms	Acquisition of goods and services not arising from GIMM's genuine needs, aimed at benefiting interests unrelated to the organisation.	Remote	Medium	Moderate risk	Effective	Code of Ethics and Conduct. Centralised workflow managed by the Procurement Department, including (i) stratification of approval levels based on the value/nature of the product or service being acquired; (ii) establishment of specific monetary thresholds to determine the number of quotes to be requested from the market; (iii) recordkeeping of copies of the selected proposal/quote for each purchase; and (iv) requirement for the requested item or service to be budgeted within the scientific platform's or project's cost centre to enable	Low risk

						<p>approval.</p> <p>Internal Approval Matrix requiring, among other controls, (i) prior analysis and validation by the Finance Department for purchases above EUR 50,000; and (ii) initiation of a public procurement process for purchases above EUR 100,000. Predefined catalogue with a minimum variety of prices/suppliers for the purchase of consumables/laboratory materials, applicable to requisitions from scientific platforms. Flexibility in the selection/contracting process of goods/services in the context of scientific research, considering project specificities, urgency of the requisition for research continuity, and market supplier limitations, while reserving the possibility of subsequent control over the legitimacy of expenses submitted by the Project Management Department.</p> <p>Requirement for justification of the requisition by the head of the research group for the purchase of equipment/investments of significant value, subject to prior technical feasibility assessment by the Scientific Directorate and approval by the Executive Committee.</p>	
Strategic and Operational Platforms	Misappropriation of resources and other receivables and/or improper approval of payments to obtain and/or grant advantages.	Remote	High	High risk	Effective	<p>Code of Ethics and Conduct.</p> <p>Segregation of duties and access controls in payment management.</p> <p>Payment procedures carried out in accordance with the Internal Approval Matrix based on the value/nature of the expense to be paid.</p> <p>Stratification of internal levels responsible for the review and approval of bank reconciliations.</p> <p>Controls in the financial and accounting system preventing payment of expenses exceeding the contracted/requested amount.</p> <p>Signature authority for approvals at banking institution level (i.e., Finance and Operations Directorates).</p> <p>Cash handling limited to residual payments below EUR 50.00.</p> <p>Submission of justification, with prior approval from the responsible officer, for urgent and/or exceptional payments (i.e., not included within the scope of overdue invoices relating to monthly suppliers).</p>	Low risk
Strategic and Operational Platforms	Improper and/or unjustified approval of reimbursements requested by staff/researchers for undocumented, non-deductible, and/or disproportionate expenses in terms of value or nature.	Remote	High	High risk	Effective	<p>Code of Ethics and Conduct.</p> <p>Limitation of reimbursements for expenses of certain types (e.g., transportation and meals), with any exceptional expenses subject to evaluation by the project manager and the Procurement Department.</p> <p>Integration of the purchasing and accounting IT systems, enabling data cross-checking for transaction validation.</p> <p>Reimbursement requests subject to completion of a form justifying the legitimacy of the expense,</p>	Low risk

						including IBAN and payment identification details, and submission of supporting documentation in the system for validation by the Finance Department. Reimbursement of expenses within funded projects subject to verification in accordance with the specific rules of each funding entity.	
Strategic and Operational Platforms	Fraud and/or manipulation in the budget preparation and management process with the intent to inflate revenues and/or underestimate expenses.	Remote	High	High risk	Effective	Code of Ethics and Conduct. Detailed procedure for the preparation and execution of the annual budget, which involves: (i) identification, starting from the last quarter of the current year, of the budgetary needs of each internal area/scientific platform based on the results of the previous year, with the respective managers required to list nominally the estimated structural expenses of each unit and justify them according to their activities and projects for the following year; (ii) consolidation and financial analysis of the budgetary needs of each area by the Finance Department, followed by submission for approval by the Executive Committee, Board of Directors, and Board of Curators; (iii) case-by-case monitoring of budget execution by the Procurement Department; and (iv) mandatory approval by the Executive Committee for any budget amendments; Revalidation and justification of the legitimacy of expenses/purchases, even if forecasted and approved in the annual budget.	Low risk
Strategic and Operational Platforms	Adoption of discriminatory and/or unethical practices in the recruitment and selection process of staff/researchers.	Remote	Medium	Moderate risk	Partially effective	Code of Ethics and Conduct. Gender Equality Policy. Interview and candidate selection process conducted by independent members and consisting of multiple stages, involving the heads of the requesting department and the People Department. Selection process aligned with HRS4R best practices, respecting funder requirements and project-specific technicalities, with appointment of an internal panel for selecting staff/researchers for scientific positions. Recruitment of staff for technically complex positions and/or positions of trust with the support of specialised external recruiters, selected through a procedure established by the Procurement Department. Employment contracts subject to (i) signing of a declaration by the employee acknowledging GIMM's confidentiality and intellectual/industrial property rules; and (ii) inclusion of exclusivity clauses to prevent conflicts of interest, incompatibility of income, and/or role. Support from the Chief of Staff in the welcoming and onboarding process of leadership positions, reporting directly to the Executive Committee.	Low risk

						Validation of human resources technical matters related to employment contract terms and conditions, granting of leaves and vacations, conduct of disciplinary processes, payment of benefits and salaries, and others by the Legal Department.	
Strategic and Operational Platforms	Undue favouritism or inappropriate selection of candidates in the recruitment process, potentially leading to conflicts of interest (e.g., recruitment of “family members,” “friends,” individuals linked to PEPs, or persons connected to clients and/or suppliers for the positions in question).	Remote	Medium	Moderate risk	Partially effective	Code of Ethics and Conduct. Gender Equality Policy. Interview and candidate selection process conducted by independent members and composed of multiple stages, with participation of the heads of the requesting area and the People Department. Selection process aligned with HRS4R best practices, respecting funder requirements and project-specific technicalities, with appointment of an internal panel for selecting staff/researchers for scientific positions. Recruitment of staff for positions of greater technical complexity and/or positions of trust with support from specialised external recruiters, selected through a procedure established by the Procurement Department. Execution of employment contracts subject to (i) signing of a declaration by the employee acknowledging GIMM’s confidentiality and intellectual/industrial property rules; and (ii) inclusion of exclusivity clauses to prevent conflicts of interest, income incompatibility, and/or role conflicts. Support from the Chief of Staff in the welcoming and onboarding process of leadership positions, with direct reporting to the Executive Committee. Validation of human resources technical matters related to employment contract terms and conditions, granting of leave and vacations, conduct of disciplinary processes, payment of benefits and remuneration, and others by the Legal Department.	Low risk
Strategic and Operational Platforms	Tampering with information and/or approval of undue payments and/or benefits in the processing of remuneration paid to staff/researchers.	Remote	High	High risk	Partially effective	Code of Ethics and Conduct. Processing and payment of salaries and benefits subject to segregation of duties and different hierarchical levels of approval, including the People, Finance, and Accounting Departments. Restricted access to the payroll processing system/employee data files limited to the People, Finance, and Accounting Departments. Prior authorisation of overtime by the People Department for payment of additional remuneration. Specialised human resources management software with attendance control and tracking of hours worked according to the specificities of each staff member’s/researcher’s scientific	Risco Moderado

						<p>roles/projects.</p> <p>Validation of human resources technical matters related to employment contract terms and conditions, granting of leave and vacations, conduct of disciplinary processes, payment of benefits and remuneration, and other issues by the Legal Department.</p>	
Strategic and Operational Platforms	Awarding of undue and/or unfair prizes, recognitions, and other benefits due to the absence of equitable criteria and/or transparency in the evaluation of staff/researchers.	Remote	Medium	Moderate risk	Partially effective	<p>Code of Ethics and Conduct.</p> <p>Processing and payment of salaries and benefits subject to segregation of duties and multiple hierarchical approval levels, including the People, Finance, and Accounting Departments.</p> <p>Restricted access to the payroll processing system and employee data files limited to the People, Finance, and Accounting Departments.</p> <p>Prior authorisation of overtime payments by the People Department.</p> <p>Specialised human resources management software with attendance and work hours tracking according to the specificities of each staff member's/researcher's scientific roles and projects.</p> <p>Support from the Chief of Staff in the welcoming and onboarding process of leadership positions, reporting directly to the Executive Committee.</p> <p>Validation of human resources technical matters related to employment contract terms and conditions, leave and vacation grants, disciplinary proceedings, payment of benefits and remuneration, and other issues by the Legal Department.</p>	Low risk

<p>Strategic and Operational Platforms</p>	<p>Improper disclosure of GIMM's confidential data and information due to loss, theft, and/or robbery of mobile devices, as well as unauthorised access to and/or manipulation of computer systems by staff and/or third parties.</p>	<p>Remote</p>	<p>Critical</p>	<p>High risk</p>	<p>Partially effective</p>	<p>Code of Ethics and Conduct. Management and storage of documents in shared folders associated with GIMM's central servers, with mobile device access requiring VPN connection.</p> <p>Specialised team in data management and digital transformation aligned with good practices of "open science," in coordination with the Data Protection Office, to support staff/researchers in efficient management and secure sharing of research data.</p> <p>Provision and storage of raw/primary research data to allow verification of processed results during project execution.</p> <p>Electronic lab book for systematic recording of data related to ongoing research in each laboratory.</p> <p>Provision of corporate mobile phones to senior management staff, subject to signing a responsibility agreement by the holder, with restricted access to institutional systems.</p> <p>Provision of Service Desk email and telephone contact, with dedicated extensions for each GIMM operating site, for query resolution and reporting of digital security incidents.</p> <p>Network management control through registration of all laptops in GIMM's domain.</p> <p>Prohibition of users from being administrators of their own machines, except in exceptional cases upon signing a responsibility agreement in which the user justifies the need to install external software for research purposes and confirms understanding of the security rules for PC use.</p> <p>Notification of the Digital & Technology Department in case of dismissal of GIMM staff/researchers for (i) identification of IT resources under the responsibility of the departing person; and (ii) execution of equipment verification, formatting, and cleaning procedures.</p>	<p>Moderate risk</p>
--	---	---------------	-----------------	------------------	----------------------------	---	----------------------

Strategic and Operational Platforms	Misappropriation of computer equipment owned by GIMM for personal use and/or sale to third parties.	Likely	Medium	High risk	Partially effective	Code of Ethics and Conduct. Provision of corporate mobile phones to senior management staff, subject to signing a responsibility agreement by the holder, with restricted access to institutional systems. Provision of Service Desk email and telephone contact, with dedicated extensions for each GIMM operational site, for query resolution and reporting of digital security incidents. Network management control through registration of all laptops in GIMM's domain. Users are generally prohibited from being administrators of their own machines, except in exceptional cases upon signing a responsibility agreement, in which the user justifies the need to install external software for research purposes and confirms awareness of security rules for PC use. Notification of the Digital & Technology Department in the event of dismissal of GIMM staff/researchers for (i) identification of IT resources under the responsibility of the departing person; and (ii) execution of equipment verification, formatting, and cleaning procedures.	Moderate risk
Strategic and Operational Platforms	Failure of staff to participate in training activities relevant to their role, including those related to corporate ethics and integrity, as well as safety in the use of facilities and laboratories.	Remote	Low	Moderate risk	Partially effective	Initial training for new staff on (i) general and laboratory safety; and (ii) ethics and integrity in the workplace. Internal "on the job" training programme for scientific platform staff, including specific training sessions when working with higher-risk tasks and/or following identification of training gaps or isolated incidents. Occupational Safety Management Manual made available to all staff and researchers using GIMM facilities/laboratories.	Low risk

Annex III

Plan approval and communication

The present Plan was:

- **Approved by the Board of Directors** on June 17th 2025 ;
- **Communicated** to all employees, collaborators, and relevant stakeholders;
- **Made available** through internal communication channels and the institutional website.