

BDO LUXEMBOURG

HEALTH CHECK GOVERNANCE



PROTECT YOUR ORGANISATION IN AN INCREASINGLY COMPLEX ENVIRONMENT

Organisations are navigating an increasingly complex environment, characterised by a growing number of regulations and risks. Compliance, governance, and risk management have become essential, as any vulnerability can impact the organisation's sustainability. Undetected errors or fraud can also harm the reputation of leaders and damage the company's image.

Our "Governance Healthcheck" provides a targeted assessment to identify risks and vulnerabilities across 6 key areas: financial transfers, supplier management, governance bodies, alert mechanisms, fraud detection (forensic), and IT security. This approach enables you to strengthen your control systems and minimise threats to your operations.

Our experts support you in identifying vulnerabilities, implementing tailored solutions, and establishing regular reporting mechanisms, thereby ensuring a more secure and efficient management of your organisation.





1. ANALYSIS OF PROCESSES RELATED TO FINANCIAL TRANSACTIONS

i. Role Separation in Payments

Verification of the segregation of duties (preparation, validation, payment, reconciliation) to minimise the risks of errors and fraud.

ii. Approval and Authorisation Controls

Assessment of procedures to ensure that appropriate authorisations are in place prior to any payment, contract, or invoice.

iii. Reviewing the maturity of financial processes

Comprehensive review of payment processes, discussion of best practices and development of recommendations.

iv. Allocation and Use of Funds

2. SUPPLIER MANAGEMENT

i. Procurement Process

Assessment of the transparency and adequacy of procurement policies, including tendering, supplier selection, obtaining rebates and managing conflicts of interest.

ii. Supplier Management

Review of contracting and payment processes, with validation of services prior to settlement.

iii. Contract Tracking

Ensuring rigorous follow-up of contracts and authorisations for any contract changes.

3. GOVERNANCE BODIES

i. Documentary Compliance

Verification that official documents (statutes, meeting minutes, etc.) related to governance are present and complete and comply with the legal requirements in force, including their regular update.

ii. Roles and Responsibilities

Review of the clarity and completeness of the roles and responsibilities of governance bodies (board, office, executive committee, management), ensuring a transparent and balanced distribution of responsibilities and management of conflicts of interest.

iii. Steering and Reporting

Evaluation of the steering system, including monitoring and reporting mechanisms, to ensure effective governance, with decision-making based on reliable information and relevant indicators.



4. ALERT MECHANISMS

i. Ethical Commitment and Governance Culture

Assessment of governance's commitment to promoting honesty, integrity and ethical behaviour, highlighting a "Tone at the top" culture within the organisation.

ii. Whistleblowing Mechanism

Analysis of the effectiveness and confidentiality of the whistleblowing system, allowing employees to report financial misconduct and unethical behaviour without fear of reprisal. Verification of the accessibility and communication of the mechanism.

iii. Investigation Process

Review of procedures for investigating reported incidents, ensuring transparency and accountability. Evaluation of the implementation of corrective measures and follow-up, with appropriate reporting to governance bodies.

5. FRAUD DETECTION

i. Identification of Fraud Schemes

Spot common fraud patterns that can affect your organisation, such as fictitious suppliers, double payments, inflated invoices, employee personal purchases, and kickbacks.

ii. Fraud Risk Assessment

Analysis of specific fraud risks in the disbursement process and identification of potential vulnerabilities.

iii. Review of Fraud Incidents

Study of internal and external fraud incidents in similar organisations to learn from them.

iv. Integrity Test

Carrying out specific forensic tests, such as journal entry testing, in order to verify the probity and quality of transactions and operations.

6. CYBERSECURITY

i. Evaluation of Prevention Mechanisms

Review of processes to protect the organisation from cyberattacks and fraud, including regular penetration testing and protocols to prevent social manipulation and phishing.

ii. Access Management Assessment

Analysis of access management policies, focusing on privileged access to payment systems and the principle of least privilege. Review of ERP systems and access controls, as well as evaluation of current IAM systems, including role-based access control (RBAC). Identification of gaps compared to NIST and ISO 27001 standards to assess potential risks.

iii. Awareness and Training

Evaluation of awareness and training programs for staff.



INTERESTED?

Get in touch with our experts:



Jan Brosius
Partner - Local Market
+352 45 123 430
jan.brosius@bdo.lu



Patrick Terazzi
Partner - Internal audit
+352 45 123 299
patrick.terazzi@bdo.lu



Benoit Wtterwulghe
Partner - Consulting
+352 45 123 795
benoit.wtterwulghe@bdo.lu

Next steps:

- ▶ **A qualification meeting:** We offer you an initial appointment with our experts to understand your priorities and qualify your specific needs. This in-depth discussion will allow us to identify the key issues facing your organisation and better understand your expectations.
- ▶ **A tailored offer:** At the end of this meeting, you will receive a personalized proposal, adapted to your needs in terms of the topics discussed and the depth of the analysis

Target Sectors:

- ▶ Operating entities
- ▶ Public and parapublic sector
- ▶ Associative and cultural sector
- ▶ International organisations

We are talking:

- ▶ English 
- ▶ French 
- ▶ German 
- ▶ Luxembourgish 

BDO in Luxembourg

▼
Audit & Assurance

▼
Consulting

▼
Business Services & Outsourcing

▼
Taxation



This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad guidance only.

This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication herein without obtaining specific professional advice.

Please contact the appropriate BDO Member Firm to discuss these matters in the context of your particular circumstances.

No entity of the BDO network, nor the BDO Member Firms or their partners, employees or agents accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO is an international network of public accounting firms, the BDO Member Firms, which perform professional services under the name of BDO. Each BDO Member Firm is a member of BDO International Limited, a UK company limited by guarantee that is the governing entity of the international BDO network.

Service provision within the BDO network is coordinated by Brussels Worldwide Services BVBA, a limited liability company incorporated in Belgium with its statutory seat in Brussels.

Each of BDO International Limited (the governing entity of the BDO network), Brussels Worldwide Services BVBA and the member firms of the BDO network is a separate legal entity and has no liability for another such entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BVBA and/or the member firms of the BDO network.

BDO is the brand name for the BDO network and for each of the BDO Member Firms.

© 2025 BDO Advisory

All rights reserved.

www.bdo.lu

