ISO CD1 37301 BENCHMARKING WITH U.S. DoJ - EVALUATION OF CORPORATE COMPLIANCE PROGRAMS

by

Ariosto Farias Jr

Brazilian Expert on ISO TC 309/WG4-Compliance Management Systems

May 2019 – Rev:0

PURPOSE OF THIS DOCUMENT

The purpose of this document is to provide contributions for the improvement of **ISO CD 1 37301: Compliance management systems - Requirements with guidance for use** by adopting as a **benchmark** the updated Guidance Document: **U.S. Department of Justice-Evaluation of Corporate Compliance Programs (April 2019)**, taking into account that many of the topics of the U.S. DoJ Guidance Document also appear in the **following internationally recognized Compliance Instruments:**

Internationally recognized Compliance Instruments

1) Anti-Corruption Ethics and Compliance Handbook for Business ("OECD Handbook") published in 2013 by OECD, United Nations Office on Drugs and Crime, and the World Bank;

2)Good Practice Guidance on Internal Controls, Ethics, and Compliance adopted by the Organization for Economic Co-operation and Development.

U.S. DoJ Guidance Document References

U.S. References:

- JM 9-28.000 Principles of Federal Prosecution of Business Organizations, Justice Manual
- JM 9-47.120 FCPA Corporate Enforcement Policy
- Chapter 8 – Sentencing of Organizations - United States Sentencing Guidelines
- Memorandum entitled “Selection of Monitors in Criminal Division Matter Criminal Division corporate resolution agreements
- A Resource Guide to the U.S. Foreign Corrupt Practices Act (“FCPA Guide”)

The U.S. DoJ Guidance Document is based on three “fundamental questions”

1. “Is the corporation’s compliance program well designed?“

2. “Is the program being applied earnestly and in good faith?“ In other words, is the program being implemented effectively?

3. “Does the corporation’s compliance program work“ in practice?

Contents of this document

1. IS THE CORPORATION'S COMPLIANCE PROGRAM WELL DESIGNED?

1A) RISK ASSESSMENT

1A1 Risk Management Process

1A2 Risk-Tailored Resource Allocation

1A3 Updates and Revisions

1B) POLICIES AND PROCEDURES

1B1 Design

1B2 Comprehensiveness

1B3 Accessibility

1B4 Responsibility for Operational Integration

1B5 Gatekeepers

1C)TRAINING AND COMMUNICATIONS

1C1 Risk-Based Training

1C2 Form/Content/Effectiveness of Training

1C3 Communications about Misconduct

1C4 Availability of Guidance

Contents of this document

Contents of this document

2.IS THE CORPORATION'S COMPLIANCE PROGRAM BEING IMPLEMENTED EFFECTIVELY?

Contents of this document

3.DOES THE CORPORATION'S COMPLIANCE PROGRAM WORK IN PRACTICE?

Legend:

1)The texts in brown type at the column “Proposal” are suggestions to the improvement of ISO CD1 37301.

2)The texts in **bold black** type at the column “ISO CD1 37301” are the ISO 37301 requirements to meet the DoJ questions.

3)The texts with “----------” mean that it were not taken into consideration.

1. IS THE CORPORATION'S COMPLIANCE PROGRAM WELL DESIGNED?

U.S. Department of Justice Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1A1 Risk Management Process 1A1.1What methodology has the company used to identify, analyze, and address the particular risks it faces?	**4.6 Compliance risk assessment** The organization shall **identify, analyse and evaluate its compliance risks based upon a formal compliance risk assessment**.	
1A1.2What information or metrics has the company collected and used to help detect the type of misconduct in question?	9 Performance evaluation **9.1 Monitoring, measurement, analysis and evaluation** **9.1.2 Sources of feedback on compliance performance** 9.1.3 Development of indicators **9.1.4 Compliance reporting**	
1A1.3How have the information or metrics informed the company's compliance program?	**9.3 Management review** g) information on the compliance performance, including trends in: **2) monitoring and measurement results.**	To add: A.4.6 Compliance risk assessment:The organization should devote a reasonable and proportionate amount of time to policing high compliance risk areas, such as questionable payments to business associates consultants, suspicious trading activity, or excessive discounts to resellers and distributors.

U.S. Department of Justice Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1A2 Risk-Tailored Resource Allocation 1A2.1Does the company devote a disproportionate amount of time to policing low-risk areas instead of high-risk areas, such as questionable payments to third-party consultants, suspicious trading activity, or excessive discounts to resellers and distributors?		To add :A.4.6 Compliance risk assessment: The organization should devote a reasonable and proportionate amount of time to policing high compliance risk areas, such as questionable payments to business associates consultants, suspicious trading activity, or excessive discounts to resellers and distributors.
1A2.2Does the company give greater scrutiny, as warranted, to high-risk transactions (for instance, a large-dollar contract with a government agency in a high-risk country) than more modest and routine hospitality and entertainment?		To add :A.4.6 Compliance risk assessment: The organization should give greater scrutiny, as warranted, to high compliance risk transactions (for instance, a large-dollar contract with a government agency in a high-risk country) than more modest and routine hospitality and entertainment.
1A3 Updates and Revisions 1A3.1Is the risk assessment current and subject to periodic review?	4.6Compliance risk assessment **The compliance risks shall be assessed periodically and whenever there are material changes in circumstances.**	

U.S.Department of Justice-Criminal Division Evaluation of Corporate Compliance Program	ISO CD1 37301 (March 2019)	Proposal
1A3.2Have there been any updates to policies and procedures in light of lessons learned?	7.5 Documented information 7.5.2 Creating and **updating** When creating and **updating** documented information the organization shall ensure appropriate: **-review** and approval for suitability and adequacy.	To add :A.7.5.2 Creating and updating:The organization should identify the root cause of not following the policy and or procedure, that contributed to the misconduct, and update the policy and procedure based on the lessons learned.
1A3.3Do these updates account for risks discovered through misconduct or other problems with the compliance program?		To add: A.7.5.2 Creating and updating: The updates should take into account the risks discovered through misconduct or other problems with the compliance program.


U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1B1 Design 1B1.1What is the company's process for designing and implementing new policies and procedures, and has that process changed over time?	**7.5.2 Creating and updating**	
1B1.2Who has been involved in the design of policies and procedures?		To add: A.7.5.2 Creating and updating: The organization should be aware that the owner of the processes/areas related to compliance matters (e.g; financial, HR, legal, procurement, sales, marketing), should be involved in the design of its own policies and procedures.
1B1.3Have business units been consulted prior to rolling them out?		To add: A.7.5.2 Creating and updating: The organization should be aware that its business units (if any) should be consulted in the designed compliance program prior to rolling them out.

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1B2 Comprehensiveness 1B2.1What efforts has the company made to monitor and implement policies and procedures that reflect and deal with the spectrum of risks it faces, including changes to the legal and regulatory landscape?	9.2Internal audit 9.2.1 The organization shall conduct internal audits at planned intervals to provide information on whether the compliance management system: a) conforms to: **1) the organization's own requirements for its compliance management system**	
1B3 Accessibility 1B3.1How has the company communicated its policies and procedures to all employees and relevant third parties?	7.4Communication **7.4.2 Internal communication** **7.4.3 External communication**	
1B3.2If the company has foreign subsidiaries, are there linguistic or other barriers to foreign employees' access?	**7.4Communication**	To add 7.4.1 General : e)who will communicate; f)the language in which to communicate
1B4 Responsibility for Operational Integration 1B4.1Who has been responsible for integrating policies and procedures?	5.3.3 Compliance function The compliance function shall be responsible for: **b) ensuring that compliance obligations are integrated into existing policies, procedures and processes;** **k) providing personnel with access to resources on compliance procedures and references.**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1B4.2Have they been rolled out in a way that ensures employees' understanding of the policies?	**7.2.2 Employment process** In relation to all its personnel, the organization shall implement procedures such that: b) within a reasonable period of their employment commencing**, personnel receive a copy of, or are provided with access to, the compliance policy and training in relation to that policy.**	
1B4.3In what specific ways are compliance policies and procedures reinforced through the company's internal control systems?	7.2.2 Employment process In relation to all its personnel, the organization shall implement procedures such that: a) conditions of employment **require personnel to comply with the compliance policy and compliance management system**, and give the organization the right to disciplinary measures in the event of non-compliance; b) within a reasonable period of their employment commencing, **personnel receive a copy of, or are provided with access to, the compliance policy and training in relation to that policy.**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1B5 Gatekeepers 1B5.1What, if any, guidance and training has been provided to key gatekeepers in the control processes (e.g., those with approval authority or certification responsibilities)?	----------	
1B5.2Do they know what misconduct to look for? 1B5.3Do they know when and how to escalate concerns?	----------	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1C1.Risk-Based Training 1C1.1 What training have employees in relevant control functions received?	**a) appropriate to the roles of personnel and the compliance risks to which personnel is exposed to;** b) assessed for effectiveness; c) reviewed regularly. Training records shall be retained as documented information.	
1C1.2 Has the company provided tailored training for high-risk and control employees, including training that addresses risks in the area where the misconduct occurred?		To add:A.7.2.3Traning: The organization should provide training for high risks, including training that addresses risks in the area where the misconduct has occurred.
1C1.3Have supervisory employees received different or supplementary training?		To add:A.7.2.3Traning: For supervisory personnel, the organization should provide different or supplementary training.
1C1.4What analysis has the company undertaken to determine who should be trained and on what subjects?		To add:A.7.2.3Traning: The organization should determine on its procedure who should be trained and on what subjects.



U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1C2 Form/Content/Effectiveness of Training 1C2.1Has the training been offered in the form and language appropriate for the audience?		To add:A.7.2.3Traning: Education and training should be: b) sufficiently flexible to account for a range of techniques to accommodate the differing needs of organizations and ~~employees~~ personnel, in the form and language appropriate for the audience.
1C2.2Is the training provided online or in-person (or both), and what is the company's rationale for its choice?	A.7.2.3 Training **Interactive training might be the best form of training,** if noncompliance could result in serious consequences.	
1C2.3 Has the training addressed lessons learned from prior compliance incidents?	A.7.2.3 Training Compliance retraining should be considered whenever there is: -issues arising from monitoring, auditing, reviews, **complaints and noncompliance,** including interested party feedback.	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1C2.4 How has the company measured the effectiveness of the training?	A.9 Performance evaluation A.9.1 Monitoring, measurement, analysis and evaluation A.9.1.1 General Monitoring of the compliance management system typically includes: — **effectiveness of training**	
1C2.5Have employees been tested on what they have learned?		To add:7.2.3Traning: Personnel shall be provided with training on a regular basis, from the time of commencement and at planned intervals determined by the organization and shall be tested on what they have learned.
1C2.6How has the company addressed employees who fail all or a portion of the testing?		To add:7.2.3Traning: For the personnel who fail all or partially of the testing, the organization shall submit those personnel to another testing.

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1C3 Communications about Misconduct 1C3.1What has senior management done to let employees know the company's position concerning misconduct?	5.2 Compliance policy The governing body and **top management** shall establish and approve a compliance policy that: f) **outlines the consequences** of not complying with the compliance policies and procedures.	
1C3.2What communications have there been generally when an employee is terminated or otherwise disciplined for failure to comply with the company's policies, procedures, and controls (e.g., anonymized descriptions of the type of misconduct that leads to discipline)?		To add: 7.2.2 Employment process: When personnel are terminated or disciplined for failure to comply with the organization´s policies and procedures, the organization shall take the necessary steps in order to identify the root cause for such failure.



U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1C4 Availability of Guidance 1C4.1What resources have been available to employees to provide guidance relating to compliance policies?	7.5.3 Control of documented information Documented information recommended by the compliance management system and by this document shall be controlled to ensure: a) **it is available, accessible and suitable for use**, where and when it is needed.	
1C4.2How has the company assessed whether its employees know when to seek advice and whether they would be willing to do so?	8.4 Raising concerns The organization shall implement procedures which: **e) enable personnel to receive advice** **The organization shall ensure that all personnel are aware of the reporting procedures, their rights and protections and are able to use them.**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1D1.Effectiveness of the Reporting Mechanism 1D1.1Does the company have an anonymous reporting mechanism, and, if not, why not?	8.4 Raising concerns The organization shall implement procedures which: a) encourage and enable persons to report in good faith attempted, suspected or actual violations of the compliance policy or the compliance management system; b) treat reports confidentially; **c) accept anonymous reports.**	
1D1.2 How is the reporting mechanism publicized to the company's employees?	8.4 Raising concerns **The organization shall ensure that all personnel are aware of the reporting procedures, their rights and protections and are able to use them.**	
1D1.3 Has it been used?	----------	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1D1.4 How has the company assessed the seriousness of the allegations it received?	8.5 Investigation processes The organization shall establish processes **to assess**, evaluate, investigate and close reports on **suspected violations of compliance obligations**. These processes shall be governed by the principles of protection, fairness and impartiality.	
1D1.5Has the compliance function had full access to reporting and investigative information?	5.3.3 Compliance function **i) establishing a system for reporting concerns**; **l) providing advice to the organization on compliance-related matter.**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1D2 Properly Scoped Investigations by Qualified Personnel 1D2.1How does the company determine which complaints or red flags merit further investigation? 1D2.2 How does the company ensure that investigations are properly scoped?	8.5 Investigation processes **The organization shall establish processes** to assess, evaluate, investigate and close reports on suspected violations of compliance obligations. **These processes shall be governed by the principles of protection, fairness and impartiality.**	
1D2.3 What steps does the company take to ensure investigations are independent, objective, appropriately conducted, and properly documented?	The investigation processes shall be carried on **by independent and competent personnel**. The organization shall retain **documented information** on the investigation process.	
1D2.4How does the company determine who should conduct an investigation, and who makes that determination?	The investigation processes shall be carried on **by independent and competent personnel**.	



U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1D3Investigation Response 1D3.1 Does the company apply timing metrics to ensure responsiveness?		To add :A.9.1.3 Development of indicators Indicators can include: -the time taken to ensure responsiveness in an investigation process
1D3.2Does the company have a process for monitoring the outcome of investigations and ensuring accountability for the response to any findings or recommendations?		To add :A.9.1.3 Development of indicators Reactive indicators can include: -outcome of the investigation process
1D4Resources and Tracking of Results 1D4.1Are the reporting and investigating mechanisms sufficiently funded?		To add :8.5 Investigation processes These processes shall be governed by the principles of protection, fairness and impartiality, and shall be sufficiently funded.
1D4.2How has the company collected, tracked, analyzed, and used information from its reporting mechanisms?	9.1 Monitoring, measurement, analysis and evaluation	To add :9.3 Management review: 9.3Governing body and top management review The governing body (if any) and top management shall review the organization's compliance management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.



U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1D4.3Does the company periodically analyze the reports or investigation findings for patterns of misconduct or other red flags for compliance weaknesses?		To add 9.3:Management review: 9.3Governing body and top management review The governing body (if any) and top management shall review the organization's compliance management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of: 5)Investigations report.



A WELL-DESIGNED COMPLIANCE PROGRAM SHOULD APPLY RISK-BASED DUE DILIGENCE TO ITS THIRD PARTY RELATIONSHIPS.

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1E1. Risk-Based and Integrated Processes 1E1.1 How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company?	8.3 Outsourced processes **The organization shall consider compliance risks related to ~~third-party~~ business associates processes** relating to the supply of products and services and distribution of products, and put controls in place, as necessary.	To add :3 Terms and definitions: 3.x **third party** person or body that is independent of the *organization* (3.x) Note 1 to entry: All *business associates* (3.x) are third parties, but not all third parties are business associates 3.x business associate external party or person with whom the *organization* (3.1) has, or plans to establish, some form of business relationship. Note 1 to entry: Business associate includes but is not limited to clients, customers, joint ventures, joint venture partners, consortium partners, outsourcing providers, contractors, consultants, sub-contractors, suppliers, vendors, advisors, agents, distributors, representatives, intermediaries and investors. This definition is deliberately broad and should be interpreted in line with the compliance risk profile of the organization to apply to business associates which can reasonably expose the organization to compliance risks.

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1E1.2 How has this process been integrated into the relevant procurement and vendor management processes?		To add :A.8.3 Due diligence The organization should take into account the business associate process into the relevant procurement and vendor management process.
1E2 Appropriate Controls 1E2.1 How does the company ensure there is an appropriate business rationale for the use of third parties?		To add :**8.3Due diligence** Where the organization's compliance risk assessment, as conducted in 4.6, has assessed a compliance risk in relation to: a)specific categories of transactions, projects or activities, b)planned or on-going relationships with specific categories of business associates, or c)specific categories of personnel in certain positions (see 7.2.2), the organization shall assess the nature and extent of the compliance risk in relation to specific transactions, projects, activities, business associates and personnel falling within those categories.

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1E2 Appropriate Controls 1E2.1 How does the company ensure there is an appropriate business rationale for the use of third parties?		To add :**8.3Due diligence** This assessment shall include any due diligence necessary to obtain sufficient information to assess the compliance risk. The due diligence shall be updated at a defined frequency, so that changes and new information can be properly taken into account. NOTE 1The organization can conclude that it is unnecessary, unreasonable or disproportionate to undertake due diligence on certain categories of personnel and business associate. NOTE 2The factors listed in a), b) and c) above are not exhaustive.
1E2.2 If third parties were involved in the underlying misconduct, what was the business rationale for using those third parties?		A.8.3 Due Diligence In the case that the businesses associates were involved in the underlying misconduct, the organization should confirm the rationale for using those businesses associates.

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1E2.3 What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered? **1E3 Management of Relationships** 1E3.1 How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks? 1E3.2 How does the company monitor its third parties?		To add: A.8.3 Due Diligence: The organization should implement controls to ensure that the procurement, operational, commercial and other non-financial aspects of its activities are being properly managed. Depending on the size of the organization and transaction, the procurement, operational, commercial and other non-financial controls implemented by an organization which can reduce compliance risks could include, for example, the following controls: a)using approved contractors, sub-contractors, suppliers and consultants that have undergone a pre-qualification process under which the likelihood of their participating in a noncompliance issues, such as bribery, is assessed; this process is likely to include a due diligence. b)assessing: 1)the necessity and legitimacy of the services to be provided by a business associate (excluding clients or customers) to the organization, 2)whether the services were properly carried out;



U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1E2.3 What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered? **1E3 Management of Relationships** 1E3.1 How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks? 1E3.2 How does the company monitor its third parties?		3)whether any payments to be made to the business associate are reasonable and proportionate with regard to those services. This is particularly important in order to avoid the risk that the business associate uses part of the payment made to it by the organization to pay a bribe on behalf of or for the benefit of the organization. For example, if an agent has been appointed by the organization to assist with sales and is to be paid a commission or a contingency fee on award of a contract to the organization, the organization needs to be reasonably satisfied that the commission payment is reasonable and proportionate with regard to the legitimate services actually carried out by the agent, taking into account the risk assumed by the agent in case the contract is not awarded. If a disproportionately large commission or contingency fee is paid, there is an increased risk that part of it could be improperly used by the agent to induce a public official or an employee of the organization's client to award the contract to the organization. The organization may also request that its business associates provide.
1E3.3 Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past?		To add: A.8.3 Due Diligence The organization should have audit rights to analyze the books and accounts of business associates.

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1E2.3 What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered? **1E3 Management of Relationships** 1E3.1 How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks? 1E3.2 How does the company monitor its third parties?		documentation that demonstrates that the services have been provided; c)awarding contracts, where possible and reasonable, only after a fair and, where appropriate, transparent competitive tender process between at least three competitors has taken place; d)requiring at least two persons to evaluate the tenders and approve the award of a contract; e)implementing a separation of duties, so that personnel who approve the placement of a contract are different from those requesting the placement of the contract and are from a different department or function from those who manage the contract or approve work done under the contract; f)requiring the signatures of at least two persons on contracts, and on documents which change the terms of a contract or which approve work undertaken or supplies provided under the contract; g)placing a higher level of management oversight on potentially high risk transactions;

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1E2.3 What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered? **1E3 Management of Relationships** 1E3.1 How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks? 1E3.2 How does the company monitor its third parties?		h)protecting the integrity of tenders and other price-sensitive information by restricting access to appropriate people; i)providing appropriate tools and templates to assist personnel (e.g. practical guidance, do's and don'ts, approval ladders, checklists, forms, IT workflows).
1E3.3 Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past?		To add: A.8.3 Due Diligence The organization should have audit rights to analyze the books and accounts of business associates.

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1E3.4 How does the company train its third party relationship managers about compliance risks and how to manage them?		To add after line 526 (7.3 Awareness) Taking into account the compliance risks identified (see 4.6), the organization shall also implement procedures addressing compliance awareness and training for business associates acting on its behalf or for its benefit, and which could pose a compliance risk to the organization. These procedures shall identify the business associates for which such awareness and training is necessary, its content, and the means by which the training shall be provided. The organization shall retain documented information on the training procedures, the content of the training, and when and to whom it was provided.
1E3.5 How does the company incentivize compliance and ethical behavior by third parties?		(8.4 Outsourced processes) The organization shall incentivize compliance and ethical behavior by business associates.

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1E4 Real Actions and Consequences 1E4.1 Does the company track red flags that are identified from due diligence of third parties and how those red flags are addressed?		(8.3Due Diligence) Where the due diligence (see 8.3) conducted on a specific transaction, project, activity or relationship with a business associate establishes that the relevant compliance risks cannot be managed by the existing controls, and the organization cannot or does not wish to implement additional or enhanced compliance controls or take other appropriate steps (such as changing the nature of the transaction, project, activity or relationship) to enable the organization to manage the relevant compliance risks, the organization shall: a)in the case of an existing transaction, project, activity or relationship, take steps appropriate to the compliance risks and the nature of the transaction, project, activity or relationship to terminate, discontinue, suspend or withdraw from it as soon as practicable; b)in the case of a proposed new transaction, project, activity or relationship, postpone or decline to continue with it.
1E4.2 Does the company keep track of third parties that do not pass the company's due diligence or that are terminated, and does the company take steps to ensure that those third parties are not hired or re-hired at a later date?		To add after line 1067 (A.8.3 Due Diligence): The organization should keep track of business associates that do not pass the organization's due diligence or that are terminated, in order to ensure that those business associates are not hired or re-hired at a later date.

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
1E4.3 If third parties were involved in the misconduct at issue in the investigation, were red flags identified from the due diligence or after hiring the third party, and how were they resolved?	8.5 Investigation processes The organization shall establish processes **to assess, evaluate, investigate and close reports on suspected violations of compliance obligations**.	
E4.4 Has a similar third party been suspended, terminated, or audited as a result of compliance issues?	----------	
F1 Due Diligence Process F1.1 Was the misconduct or the risk of misconduct identified during due diligence? F1.2 Who conducted the risk review for the acquired/merged entities and how was it done? F1.3 What is the M&A due diligence process generally? **F2 Integration in the M&A Process** F2.1 – How has the compliance function been integrated into the merger, acquisition, and integration process? **F3 Process Connecting Due Diligence to Implementation** F3.1 What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process?		To add: A.11 Mergers and Acquisitions (M&A) : The organization should implement a due diligence and identify, analyse and evaluate a compliance risk, based on a formal compliance risk assessment, for the acquired/merged entities.

2.IS THE CORPORATION'S COMPLIANCE PROGRAM BEING IMPLEMENTED EFFECTIVELY?


U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2A.1Conduct at the Top 2A1.1 How have senior leaders, through their words and actions, encouraged or discouraged compliance, including the type of misconduct involved in the investigation?	5.1.3 Governing body and top management b) **developing, leading and promoting a compliance culture** in the organization that supports the intended outcomes of the compliance management system; g) communicating the importance of effective compliance management **and the importance of conforming to the compliance management system requirements;** m) ensuring that the commitment to compliance is maintained **and that noncompliance and noncompliant behavior are dealt with appropriately**;	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2A.1Conduct at the Top 2A1.1 How have senior leaders, through their words and actions, encouraged or discouraged compliance, including the type of misconduct involved in the investigation?	5.2 Compliance policy The governing body and top management shall establish and approve a compliance policy that: **f) outlines the consequences of not complying with the compliance policies and procedures**	
2A1.2What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts?	5.1.3 Governing body and top management The governing body and top management **shall demonstrate leadership and commitment with respect to the compliance management system by:** b) developing, leading and promoting a compliance culture in the organization that supports the intended outcomes of the compliance management system;	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2A.1.2What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts?	c) ensuring that the compliance policy and **compliance objectives are established and are compatible with the values, objectives and strategic direction of the organization**; d) ensuring that policies, procedures and processes are developed and implemented to achieve compliance objectives;	
2A1.3 How have they modelled proper behavior to subordinates?	7.3.2 Behaviour **Top management shall encourage behaviour that creates and supports compliance and shall not tolerate behaviour that compromises compliance.**	To add: 7.3.2Behaviour: Everyone is responsible for conducting themselves in an ethical and compliant manner, including conforming to the requirements of the organization's compliance management system and compliance laws. It is particularly important that management take the leadership role in achieving compliance in the parts of the organization for which they have responsibility.
2A1.4Have managers tolerated greater compliance risks in pursuit of new business or greater revenues?	5.3.4 Management Management shall be responsible **for compliance within its area of responsibility by**: **b) complying with policies, procedures and processes**;	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2A.1.2What concrete actions have they taken to demonstrate leadership in the company's compliance and remediation efforts?	**c) identifying and communicating compliance risks in their operations;** d) **integrating compliance obligations into existing business practices** and procedures in their areas of responsibility;	
2A1.5 Have managers encouraged employees to act unethically to achieve a business objective, or impeded compliance personnel from effectively implementing their duties?	5.3.4 Management Management shall be responsible for compliance within its area of responsibility by: a) cooperating with and supporting the compliance function and **encouraging personnel to do the same;**	
2A.2Shared Commitment 2A.2.1What actions have senior leaders and middle-management stakeholders (e.g., business and operational managers, finance, procurement, legal, human resources) taken to demonstrate their commitment to compliance or compliance personnel, including their remediation efforts?	5.3.2 Top management Top management shall: e) ensure alignment between **operational targets and compliance obligations;** f) establish and maintain accountability mechanisms **including disciplinary actions and consequences**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2A.2.2Have they persisted in that commitment in the face of competing interests or business objectives?	5.3.2 Top management Top management shall: e) ensure alignment between **operational targets and compliance obligations;** 5.3.4 Management Management shall be responsible **for compliance within its area of responsibility by:** **d) integrating compliance obligations into existing business practices and procedures in their areas of responsibility;**	
2A.3Oversight 2A.3.1What compliance expertise has been available on the board of directors?	5.1.2 Governance The governing body shall ensure: — **direct access of the compliance function to the governing body or the highest level of authority** in the absence of a governing body	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2A3.2Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions?	5.1.3 Governing body and top management The governing body and top management shall demonstrate leadership and commitment with respect to the compliance management system by: l**) ensuring that they are informed in a timely manner on compliance matters**, including on instances of noncompliance 5.3.1 Governing body The governing body and top management shall assign the responsibility and authority to the compliance function for: **b) reporting on the performance of the compliance management system to the governing body and top management.**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2A.3.3 What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?		To add:9.3 Management review: 9.3Governing body and top management review The governing body (if any) and top management shall review the organization's compliance management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of: 5)Investigations report
2B.1 Structure 2B.1.1Where within the company is the compliance function housed (e.g., within the legal department, under a business function, or as an independent function reporting to the CEO and/or board)? 2B1.2 To whom does the compliance function report?	5.1.2 Governance 322 The governing body shall ensure: - **direct access of the compliance function to the governing body** or the highest level of authority in the absence of a governing body; - **independence of the compliance function**;	



U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2B1.3Is the compliance function run by a designated chief compliance officer, or another executive within the company, and does that person have other roles within the company?	----------	
2B1.4Are compliance personnel dedicated to compliance responsibilities, or do they have other, non-compliance responsibilities within the company?	----------	
2B1.5Why has the company chosen the compliance structure it has in place?	----------	
2B2Seniority and Stature 2B2.1How does the compliance function compare with other strategic functions in the company in terms of stature, compensation levels, rank/title, reporting line, resources, and access to key decision-makers?	5.1.2 Governance 322 The governing body shall ensure: - **direct access of the compliance function to the governing body** or the highest level of authority in the absence of a governing body; - independence of the compliance function; - **appropriate authority and adequate resources allocated to the compliance function.**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2B2.2What has been the turnover rate for compliance and relevant control function personnel?	----------	
2B2.3What role has compliance played in the company's strategic and operational decisions?	5.3.3 Compliance function The compliance function shall be responsible for: **b) ensuring that compliance obligations are integrated into existing policies, procedures and processes**	
2B2.4How has the company responded to specific instances where compliance raised concerns?	8.4 Raising concerns The organization shall implement procedures which: **a) encourage and enable persons to report in good faith attempted, suspected or actual violations of the compliance policy or the compliance management system.**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2B2.5Have there been transactions or deals that were stopped, modified, or further scrutinized as a result of compliance concerns?	----------	
2B3Experience and Qualification 2B3.1Do compliance and control personnel have the appropriate experience and qualifications for their roles and responsibilities?	7.2 Competence 7.2.1 General The organization shall: **a) determine the necessary competence of person(s) doing work under its control that affects its compliance performance;** b) ensure that **these persons are competent on the basis of appropriate education, training, or experience;** A.5.3.3 Compliance function In allocating responsibility for compliance management, consideration should be given to ensuring that the compliance function has no conflict of interest and has demonstrated: **-relevant competence.**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2B3.2Has the level of experience and qualifications in these roles changed over time?	----------	
2B3.3Who reviews the performance of the compliance function and what is the review process?		To add:A.5.3.2 Top management Top management should review the performance of the compliance function at planned intervals to ensure that the compliance management systems is achieving its objectives
2B4Funding and Resources 2B4.1 Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts?	5.1.2 Governance The governing body shall ensure: -appropriate authority and **adequate resources allocated to the compliance function.** 5.1.3 Governing body and top management The governing body and top management shall demonstrate leadership and commitment with respect to the compliance management system by:	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2B4Funding and Resources 2B4.1 Has there been sufficient staffing for compliance personnel to effectively audit, document, analyze, and act on the results of the compliance efforts?	**f)ensuring that the resources needed for the compliance management system are available, allocated assigned and documented.**	
2B4.2Has the company allocated sufficient funds for the same? 2B4.3Have there been times when requests for resources by compliance and control functions have been denied, and if so, on what grounds?	----------	
2B5Autonomy 2B5.1Do the compliance and relevant control functions have direct reporting lines to anyone on the board of directors and/or audit committee?	5.1.2 Governance The governing body shall ensure: **- direct access of the compliance function to the governing body or the highest level of authority in the absence of a governing body.**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2B5.2 How often do they meet with directors?	----------	
2B5.3 Are members of the senior management present for these meetings?	----------	
2B5.4How does the company ensure the independence of the compliance and control personnel?	5.1.2 Governance The governing body shall ensure: **-independence of the compliance function.** 5.3.1 Governing body 381 The governing body and top management shall assign the responsibility and authority to the compliance function for: **b) reporting on the performance of the compliance management system to the governing body and top management.**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2B6Outsourced Compliance Functions 2B6.1Has the company outsourced all or parts of its compliance functions to an external firm or consultant?	----------	
2B6.2If so, why, and who is responsible for overseeing or liaising with the external firm or consultant?	----------	
2B6.3What level of access does the external firm or consultant have to company information?	----------	
2B6.4How has the effectiveness of the outsourced process been assessed?	----------	
2C1Human Resources Process 2C1.1Who participates in making disciplinary decisions, including for the type of misconduct at issue?	8.5 Investigation processes The organization shall establish processes to assess, evaluate, investigate and close reports on suspected violations of compliance obligations. These processes shall be governed by the principles of protection, fairness and impartiality.	



U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2C1.2 Is the same process followed for each instance of misconduct, and if not, why?	----------	
2C1.3 Are the actual reasons for discipline communicated to employees?	----------	
2C1.4 If not, why not?	----------	
2C1.5Are there legal or investigation-related reasons for restricting information, or have pre-textual reasons been provided to protect the company from whistleblowing or outside scrutiny?	----------	
2C2Consistent Application 2C2.1Have disciplinary actions and incentives been fairly and consistently applied across the organization?	----------	
2C2.2Are there similar instances of misconduct that were treated disparately, and if so, why?	----------	



U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
2C3Incentive System 2C3.1Has the company considered the implications of its incentives and rewards on compliance?	7.2.2 Employment process The organization shall implement a process that provides for a periodic review of performance bonuses, performance targets and other incentivizing elements of remuneration **to verify that there are reasonable safeguards in place to prevent encouraging non-compliance**.	
2C3.2 How does the company incentivize compliance and ethical behavior?	7.3.2 Behaviour **Top management shall encourage behaviour that creates and supports compliance** and shall not tolerate behaviour that compromises compliance.	To add:7.3.2Behaviour Everyone is responsible for conducting themselves in an ethical and compliant manner, including conforming to the requirements of the organization's compliance management system and compliance laws. It is particularly important that management take the leadership role in achieving compliance in the parts of the organization for which they have responsibility.
2C3.3Have there been specific examples of actions taken (e.g., promotions or awards denied) as a result of compliance and ethics considerations? 2C3.4 Who determines the compensation, including bonuses, as well as discipline and promotion of compliance personnel?	----------	



3.DOES THE CORPORATION'S COMPLIANCE PROGRAM WORK IN PRACTICE?

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
3A1Internal Audit 3A1.1What is the process for determining where and how frequently internal audit will undertake an audit, and what is the rationale behind that process? 3A1.2How are audits carried out? 3A1.3 What types of audits would have identified issues relevant to the misconduct?	9.2 Internal audit 9.2.1 The organization shall conduct internal audits at planned intervals to provide information on whether the compliance management system: a) conforms to: **1) the organization's own requirements for its compliance management system;** **2) the requirements of this document;** **b) is effectively implemented and maintained.** 9.2.2 The organization shall: a) plan, establish, implement and maintain an audit programme(s) **including the frequency,** **methods, responsibilities, planning requirements and reporting**, which shall take into consideration the importance of the processes concerned and the results of previous audits;	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
3A1.4Did those audits occur and what were the findings?	9.2Internal audit 9.2.2 **d) ensure that the results of the audits are reported to relevant managers;** e) retain documented information as evidence of the implementation of the audit programme(s) **and the audit results.**	
3A1.5What types of relevant audit findings and remediation progress have been reported to management and the board on a regular basis?		To add :9.2 Internal audit 9.2.2 d)ensure that the results of the audits are reported to relevant managers, to the compliance function, to top management and to the governing body (if any), on a regular basis.
3A1.6 How have management and the board followed up?	9.3Management review The management review shall include consideration of: g) information on the compliance performance, including trends in: **1) nonconformities, corrective actions and timelines for resolution;** **4) audit results.**	To add:9.3Governing body and top management review

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
3A1.7 How often does internal audit conduct assessments in high-risk areas?		To add:A.9.2 Internal audit: The organization should conduct internal audit in high compliance risk areas at least once a year.
3A2Control Testing 3A2.1Has the company reviewed and audited its compliance program in the area relating to the misconduct?	9.2 Internal audit 9.2.1 The organization shall conduct internal audits at planned intervals to provide information on whether the compliance management system: a) conforms to: 1) the organization's own requirements for its compliance management system; 2) the requirements of this document; b) is effectively implemented and maintained.	To add :9.3 Management review: 9.3Governing body and top management review The governing body (if any) and top management shall review the organization's compliance management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of: To add: 5)Investigations report

U.S. Department of Justice-Criminal Division:Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
3A2.2More generally, what testing of controls, collection and analysis of compliance data, and interviews of employees and third parties does the company undertake?		To add: **8.3 Due diligence** Where the organization's compliance risk assessment, as conducted in 4.6, has assessed a compliance risk in relation to: a) specific categories of transactions, projects or activities, b) planned or on-going relationships with specific categories of business associates, or c) specific categories of personnel in certain positions (see 7.2.2), the organization shall assess the nature and extent of the compliance risk in relation to specific transactions, projects, activities, business associates and personnel falling within those categories. This assessment shall include any due diligence necessary to obtain sufficient information to assess the compliance risk. The due diligence shall be updated at a defined frequency, so that changes and new information can be properly taken into account.
3A2.3How are the results reported and action items tracked?	10 Improvement **10.1 Nonconformity and corrective action**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
3A3Envolving Updates 3A3.1How often has the company updated its risk assessments and reviewed its compliance policies, procedures, and practices?	4.6 Compliance risk assessment **The compliance risks shall be assessed periodically** and whenever there are material changes in circumstances. 7.5.2 Creating and updating When creating and updating documented information the organization shall ensure appropriate: **- review and approval for suitability and adequacy.**	
3A3.2Has the company undertaken a gap analysis to determine if particular areas of risk are not sufficiently addressed in its policies, controls, or training? 3A3.3What steps has the company taken to determine whether policies/procedures/practices make sense for particular business segments/subsidiaries?	9.2 Internal audit 9.2.1 The organization shall conduct internal audits at planned intervals to provide information on whether the compliance management system: a) conforms to: **1) the organization's own requirements for its compliance management system.**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
3A4Culture of Compliance 3A4.1How often and how does the company measure its culture of compliance? 3A4.2Does the company seek input from all levels of employees to determine whether they perceive senior and middle management's commitment to compliance? 3A4.3What steps has the company taken in response to its measurement of the compliance culture?	5.1.1 Compliance culture The organization shall develop a compliance culture. This depends on the active, visible, consistent and sustained commitment of the governing body, top management and management towards a common standard of behaviour that is required throughout the organization.	To add :5.1.1Compliance culture The organization shall: a)measure its´s culture of compliance; b)seek input from all the personnel to determine whether they perceive top management and middle management's commitment to compliance; c)establishes actions plans based on the results of the organization´s compliance culture indicators
3B1 Properly Scoped Investigation by Qualified Personnel 3B1.1How has the company ensured that the investigations have been properly scoped, and were independent, objective, appropriately conducted, and properly documented?	8.5 Investigation processes The organization shall establish processes to assess, evaluate, investigate and close reports on suspected violations of compliance obligations. **These processes shall be governed by the principles of protection, fairness and impartiality.** The investigation processes shall be carried on by **independent and competent personnel.** The organization shall **retain documented information** on the investigation process.	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
3B2Response to Investigations 3B2.1Have the company's investigations been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory manager and senior executives? 3B2.2What has been the process for responding to investigative findings?	8.5 Investigation processes The organization shall use the outcome of investigations for the improvement (see 10) of the compliance management systems (if appropriate).	
3B2.3How high up in the company do investigative findings go?		To add:8.5 Investigation processes: These processes shall be governed by the principles of protection, fairness and impartiality, regardless of how high up the investigation shall be conducted.
3C1Root Cause Analysis 3C1.1What is the company's root cause analysis of the misconduct at issue? 3C1.2Were any systemic issues identified? 3C1.3 Who in the company was involved in making the analysis?	10 Improvement **10.1 Nonconformity and corrective action**	



U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
3C2Prior Weaknesses 3C2.1What controls failed? 3C2.2If policies or procedures should have prohibited the misconduct, were they effectively implemented, and have functions that had ownership of these policies and procedures been held accountable?	10 Improvement **10.1 Nonconformity and corrective action**	
3C3Payment Systems 3C3.1How was the misconduct in question funded (e.g., purchase orders, employee reimbursements, discounts, petty cash)? 3C3.2What processes could have prevented or detected improper access to these funds? 3C3.3 Have those processes been improved?	10 Improvement **10.1 Nonconformity and corrective action** **10.2 Continual improvement**	
3C4Vendor Management 3C4.1If vendors were involved in the misconduct, what was the process for vendor selection and did the vendor undergo that process?	10 Improvement 1**0.1 Nonconformity and corrective action** 10.2 Continual improvement	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
3C5Prior Indications 3C5.1Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations? 3C5.2 What is the company's analysis of why such opportunities were missed?	9.2Internal audit 8.4Raising concerns 1**0.1 Nonconformity and corrective action** 9.3 Management review: The management review shall include consideration of: **h) opportunities for continual improvement.**	To add: 9.3 Management review: Governing body and top management review The management review shall include consideration of: **h) opportunities for continual improvement**
3C6Remediation 3C6.1What specific changes has the company made to reduce the risk that the same or similar issues will not occur in the future? 3C6.2What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?	10 Improvement **10.1 Nonconformity and corrective action** **10.2 Continual improvement**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
3C5Prior Indications 3C5.1Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations? 3C5.2 What is the company's analysis of why such opportunities were missed?	9.2Internal audit 8.4Raising concerns **10.1 Nonconformity and corrective action**	To add 9.3 Management review: Governing body and top management review The management review shall include consideration of: **h) opportunities for continual improvement**
3C6Remediation 3C6.1What specific changes has the company made to reduce the risk that the same or similar issues will not occur in the future? 3C6.2What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?	10 Improvement **10.1 Nonconformity and corrective action** **10.2 Continual improvement**	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
3C7Accountability 3C7.1What disciplinary actions did the company take in response to the misconduct and were they timely? 3C7.2Were managers held accountable for misconduct that occurred under their supervision? 3C7.3Did the company consider disciplinary actions for failures in supervision?	7.2.2 Employment process In relation to all its personnel, the organization shall implement procedures such that: a) conditions of employment require personnel to comply with the compliance policy and compliance management system, and **give the organization the right to disciplinary measures in the event of non-compliance**; c) to take appropriate **disciplinary action a**gainst personnel who violate the compliance policy or compliance management system. A.5.1.1Compliance culture -**prompt and proportionate disciplining** in the case of willful or negligent breaches of compliance obligations.	

U.S. Department of Justice-Criminal Division: Evaluation of Corporate Compliance Programs	ISO CD1 37301 (March 2019)	Proposal
3C7.4What is the company's record (e.g., number and types of disciplinary actions) on employee discipline relating to the types of conduct at issue?	----------	
3C7.5Has the company ever terminated or otherwise disciplined anyone (reduced or eliminated bonuses, issued a warning letter, etc.) for the type of misconduct at issue?	----------	

THANK YOU VERY MUCH FOR YOUR ATENTION

Email:ariosto@cqsi.com.br

Mobile:+55 71 9 9982 9001

ALFJ CQSI May 2019 – Rev:0