100 Common Non-Conformities in ISO 31000:2018 Risk Management

A Practical Guide to Identifying, Preventing, and Fixing the Most Frequent ISO 31000 Audit Gaps Across Enterprise Risk Frameworks

Objectives of This Guide

Implementing a robust risk management framework aligned with **ISO 31000:2018** helps organizations proactively address uncertainty, enhance decision-making, and protect stakeholder value.

However, many risk programs fall short of full alignment — often due to repeatable, preventable oversights that weaken effectiveness and increase exposure during audits or internal reviews.

This guide highlights **100 of the most common non-conformities** observed across industries during **ISO 31000 audits** and maturity assessments. Each item is paired with actionable solutions to help you build a stronger, more integrated risk management system.

✓ Identify and resolve the most frequent ISO 31000:2018 non-conformities before your next audit or review
✓ Translate ISO 31000 principles into real-world controls and documentation practices
✓ Align risk ownership, appetite, treatment, and monitoring across your organization
✓ Support effective implementation of the **ISO 31000 framework 2018** across departments and leadership levels
✓ Build a repeatable, auditable risk process that enhances operational resilience and strategic agility

This guide is ideal for:

• Risk managers, CROs, and compliance officers preparing for audits or board reviews
• Internal auditors aligning enterprise risk programs to ISO 31000 standards
• Executives aiming to strengthen risk-informed decision-making
• Consultants and governance professionals supporting **ISO 31000 certification** alignment

1. No Formal Risk Management Policy

📌 Clause: 5.2 – Leadership & Commitment

What's going wrong:
Many organizations practice some form of risk management, but it's often ad hoc, undocumented, or confined to isolated departments. There's no formal risk policy outlining the organization's commitment, purpose, scope, or guiding principles.

Why it matters:
Without a documented risk management policy, the organization lacks a foundation for aligning its risk activities with ISO 31000. Auditors will view this as a failure in leadership accountability and governance structure.

How to fix it:
✓ Develop a formal risk management policy endorsed by senior leadership
✓ Define the policy's scope, objectives, alignment with ISO 31000, and integration into the organization
✓ Communicate the policy across the organization and review it annually

2. Risk Management Not Integrated into Business Processes

📌 Clause: 5.3 – Integration

What's going wrong:
Risk management operates in a silo, separate from core business activities. It is not embedded into strategy, procurement, operations, HR, or decision-making processes.

Why it matters:
ISO 31000 emphasizes integration. If risk management doesn't influence

how decisions are made, the framework is disconnected from actual business outcomes — and audit findings will reflect that gap.

How to fix it:

✓ Map how risk influences all key business processes (e.g., strategy, planning, budgeting, procurement)

✓ Include risk reviews in project approvals and change initiatives

✓ Train managers to apply risk tools and criteria when making decisions

3. No Defined Risk Criteria or Evaluation Methodology

📌 **Clause: 6.3.1 – Risk Assessment: Establishing the Context**

What's going wrong:

Teams assess risk using their own methods, leading to inconsistent ratings and prioritization. There's no shared framework to assess likelihood, impact, or overall risk level.

Why it matters:

Consistent, objective risk evaluation is central to the ISO 31000 framework. Without defined risk criteria, organizations can't prioritize risks effectively or justify treatment decisions.

How to fix it:

✓ Create and document a standardized risk matrix

✓ Define scoring systems for likelihood and impact

✓ Train stakeholders to apply it uniformly across departments

4. Risk Registers Are Outdated or Incomplete

📌 Clause: 6.4 – Risk Identification

What's going wrong:
Risk registers are developed once and then forgotten. Many contain outdated risks, missing owners, or lack mitigation statuses.

Why it matters:
A risk register is a core document during an ISO 31000 audit. If it's incomplete or irrelevant, it reflects poorly on your ability to monitor, prioritize, and manage risks effectively.

How to fix it:
✓ Review and update your risk register at least quarterly
✓ Ensure each risk includes: description, category, rating, owner, treatment plan, and status
✓ Archive retired risks and highlight emerging risks separately

5. No Documented Risk Appetite or Tolerance Statement

📌 Clause: 5.4 – Alignment with Organizational Objectives

What's going wrong:
Risk decisions are made without a clear understanding of what levels of risk are acceptable. Teams may over-control or under-react to threats.

Why it matters:
Auditors want to see evidence that the organization has defined its risk appetite and that this guidance influences risk responses and escalation paths.

How to fix it:

✓ Facilitate a leadership workshop to define risk appetite and tolerance thresholds

✓ Document risk appetite by category (financial, reputational, compliance, etc.)

✓ Include it in your risk policy and communicate it across teams

6. Risk Owners Not Clearly Assigned

📌 **Clause: 5.3 – Roles and Responsibilities**

What's going wrong:

Risks are logged, but there's no designated person responsible for managing them. Ownership is vague or left to risk managers alone.

Why it matters:

ISO 31000 requires risk accountability. A lack of ownership leads to inaction, unresolved risks, and confusion during audits.

How to fix it:

✓ Assign a responsible individual or team for each risk

✓ Define their responsibilities in the risk register and job descriptions

✓ Review ownership quarterly and update as needed

7. No Mechanism for Identifying Emerging Risks

📌 Clause: 6.3.2 – Risk Identification

What's going wrong:
The organization focuses only on known or historical risks, ignoring new and evolving threats (e.g., AI ethics, climate change, geopolitical instability).

Why it matters:
An effective risk framework must look forward. ISO 31000 auditors will expect your system to account for both current and potential future risks.

How to fix it:

✓ Establish a recurring "emerging risk" review

✓ Use tools like PESTLE, SWOT, or scenario analysis

✓ Add an "Emerging Risk" category to your register with ongoing monitoring

8. No Monitoring of Risk Treatment Effectiveness

📌 Clause: 6.6 – Monitoring and Review

What's going wrong:
Mitigation plans are created but not followed up. There's no tracking of whether controls are implemented or if they're working.

Why it matters:
ISO 31000 emphasizes the importance of evaluating treatment effectiveness. Failure to monitor creates audit gaps and unresolved exposure.

How to fix it:

✓ Define KPIs or control objectives for each treatment action

✓ Assign deadlines and accountability

✓ Use dashboards or tracking sheets to monitor progress and flag delays

9. Inconsistent Risk Terminology Across the Organization

📌 **Clause: 6.1 – Communication and Consultation**

What's going wrong:
Terms like "residual risk," "inherent risk," and "risk control" are used differently by different teams, leading to confusion in reporting and action.

Why it matters:
A shared understanding of risk language is essential for effective communication, training, and reporting.

How to fix it:

✓ Develop a risk glossary aligned with ISO 31000 definitions

✓ Include the glossary in training and awareness materials

✓ Require standard terminology in risk reports, templates, and audit logs

10. No Structured Review of the Risk Management Framework

📌 **Clause: 5.6 – Continual Improvement**

What's going wrong:
The overall risk framework (policy, roles, tools, etc.) hasn't been formally evaluated or updated in years.

Why it matters:
ISO 31000 calls for regular review of the entire risk management system. A static framework limits relevance, adaptation, and improvement.

How to fix it:

✓ Conduct annual reviews of your risk framework with key stakeholders

✓ Use lessons learned, audit findings, and incident analysis to identify improvements

✓ Document changes and communicate them across teams

11. Risk Treatment Plans Lack Specificity

📌 **Clause: 6.5 – Risk Treatment**

What's going wrong:

Mitigation plans are vague (e.g., "monitor this risk" or "improve controls") with no timeline, KPIs, or accountability. As a result, treatment efforts lack urgency and focus.

Why it matters:

ISO 31000 requires well-defined and actionable treatment plans. Vague or generic actions are seen as weak governance and signal a lack of commitment to risk reduction.

How to fix it:

✓ Make all treatment actions SMART (Specific, Measurable, Achievable, Relevant, Time-bound)

✓ Assign owners and deadlines

✓ Link treatments to risk severity and appetite thresholds

12. No Formal Stakeholder Engagement in Risk Identification

📌 Clause: 6.2 – Communication and Consultation

What's going wrong:
Risk identification happens in a top-down fashion, without input from operational, regional, or external stakeholders who may have direct exposure or insight.

Why it matters:
ISO 31000 emphasizes inclusive risk consultation. Without stakeholder input, critical risks may go unidentified or underestimated.

How to fix it:
✓ Conduct risk workshops or surveys with key departments
✓ Include external parties (suppliers, partners, regulators) where appropriate
✓ Document stakeholder involvement in the risk context section

13. Risk Reporting is Irregular or Inconsistent

📌 Clause: 6.6 – Monitoring and Review

What's going wrong:
Risk reports are generated ad hoc, inconsistently across units, or not presented to leadership in a timely manner.

Why it matters:
Without structured, scheduled reporting, leadership lacks visibility — and auditors question oversight effectiveness.

How to fix it:
✓ Implement a quarterly or monthly risk reporting cycle

✓ Standardize formats across business units

✓ Include summaries in board-level reporting packs

14. Controls Are Not Mapped to Risks

📌 **Clause: 6.5 – Risk Treatment**

What's going wrong:
Risk registers list mitigation actions, but there's no link to specific internal controls, making it hard to evaluate effectiveness.

Why it matters:
Control mapping helps ensure that risk treatment is robust, auditable, and measurable.

How to fix it:

✓ For each risk, identify one or more control activities

✓ Use control IDs if part of a broader GRC or internal controls system

✓ Test control effectiveness during internal audits

15. No Use of Risk Categories or Taxonomy

📌 **Clause: 6.3 – Risk Identification and Context**

What's going wrong:
Risks are recorded without classification (e.g., strategic, operational, financial, legal), making them difficult to prioritize, analyze, or communicate.

Why it matters:
Taxonomies help in heatmap creation, reporting, escalation, and departmental alignment.

How to fix it:
✓ Establish risk categories based on ISO 31000 or organizational structure
✓ Require classification for all risks in the register
✓ Use categories to align reporting and dashboards

16. No Process for Escalating High-Risk Items to Leadership

📌 **Clause: 5.3 – Roles and Responsibilities**

What's going wrong:
Significant risks are stuck at the departmental level. There's no structured mechanism to escalate them to executives or risk committees.

Why it matters:
Critical risks must be reviewed at the appropriate level. Delayed escalation can result in missed warnings or poor response.

How to fix it:
✓ Define thresholds that require escalation (e.g., high severity, multiple departments impacted)
✓ Include escalation protocols in your risk policy
✓ Use workflow tools or risk dashboards with alerts

17. Risk Culture Not Actively Promoted

📌 **Clause: 5.1 – Principles & Culture**

What's going wrong:
Risk is seen as a back-office function. Employees aren't encouraged or rewarded for identifying risks or reporting near misses.

Why it matters:
ISO 31000 emphasizes a strong risk culture as the foundation of effective management. A disengaged workforce creates blind spots.

How to fix it:
✓ Promote risk awareness through training and internal campaigns
✓ Recognize staff who proactively manage or report risks
✓ Include risk behavior in performance reviews

18. Risk Tools Are Inadequate or Overly Complex

📌 **Clause: 5.5 – Resources and Infrastructure**

What's going wrong:
Spreadsheets are outdated or not accessible, or GRC tools are too technical, deterring regular use.

Why it matters:
Risk tools should enable—not hinder—risk visibility, reporting, and engagement.

How to fix it:
✓ Assess current tool usability and adoption

✓ Provide training or switch to intuitive risk platforms

✓ Ensure tools are integrated with reporting and audit workflows

19. No Link Between Risk and Strategic Objectives

📌 **Clause: 6.3.1 – Establishing the Context**

What's going wrong:
Risks are documented in isolation, without showing how they impact business goals or strategy execution.

Why it matters:
ISO 31000 requires alignment of risk management with organizational objectives. This is a key measure of maturity during audits.

How to fix it:

✓ Connect each risk to a strategic pillar or objective

✓ Highlight risks that may block or accelerate business goals

✓ Use this alignment in reporting to senior leadership

20. No Process to Retire or Archive Resolved Risks

📌 **Clause: 6.6 – Monitoring and Review**

What's going wrong:
The risk register is cluttered with outdated or fully mitigated risks. There's no formal way to close or retire them.

Why it matters:
A cluttered register confuses auditors and decision-makers, and may falsely inflate risk exposure.

How to fix it:

✓ Define a process for risk closure and archiving

✓ Move retired risks to a separate tab or archive log

✓ Maintain closure rationale for audit traceability

21. No Clear Link Between Risks and Opportunities

📌 **Clause: 6.3.1 – Establishing the Context**

What's going wrong:

Risks are framed solely as threats. Opportunities (e.g. entering new markets, adopting emerging tech) aren't captured or assessed.

Why it matters:

ISO 31000 views risk as the effect of uncertainty on objectives — positive or negative. Ignoring upside risks limits strategic agility.

How to fix it:

✓ Include opportunity assessments in your risk framework

✓ Use a dual-impact scale (positive/negative) where relevant

✓ Track both threats and opportunities in your risk register

22. No Defined Review Frequency for Risk Registers

📌 **Clause: 6.6 – Monitoring and Review**

What's going wrong:

Risk reviews happen irregularly or only around audits. This leads to stale data and outdated mitigation plans.

Why it matters:
ISO 31000 expects ongoing monitoring. Lack of structure here is a red flag for auditors.

How to fix it:
✓ Define a risk review cycle (monthly, quarterly, or by risk level)
✓ Automate reminders for risk owners
✓ Document all review dates and update history

23. No Evidence of Lessons Learned from Risk Events

📌 **Clause: 6.6 – Monitoring and Review**

What's going wrong:
Incidents or near misses are resolved, but their causes and lessons aren't captured for future mitigation.

Why it matters:
A mature risk framework includes feedback loops. ISO 31000 values continual improvement.

How to fix it:
✓ Conduct post-event reviews and document findings
✓ Log "lessons learned" in your risk records
✓ Adjust controls or training based on findings

24. Risk Management Not Included in Training Programs

📌 **Clause: 7 – Recording and Reporting (Implied via awareness)**

What's going wrong:
Only the risk or compliance team understands the framework. Operational teams are unaware of roles or tools.

Why it matters:
ISO 31000 assumes organization-wide engagement. Audit success depends on frontline involvement.

How to fix it:
✓ Integrate risk awareness into onboarding and role-based training
✓ Provide refresher sessions annually
✓ Include basic training on risk identification, escalation, and ownership

25. Inadequate Documentation of Risk Context

📌 **Clause: 6.3 – Risk Assessment: Establishing Context**

What's going wrong:
Risks are logged without describing their organizational, regulatory, or operational context. This limits understanding.

Why it matters:
Context is crucial for evaluating risk impact and relevance. Auditors need to see why a risk matters.

How to fix it:
✓ Include a brief "risk context" field for each register entry

✓ Link risks to projects, processes, or external drivers

✓ Use context to justify scoring and treatment

26. No Use of Risk Heatmaps or Visual Reporting Tools

📌 **Clause: 6.4 – Risk Analysis and Communication**

What's going wrong:
Risk data is maintained in dense spreadsheets that leadership finds hard to digest.

Why it matters:
Effective communication is part of the ISO 31000 risk process. Visual tools aid decision-making and demonstrate maturity.

How to fix it:

✓ Generate heatmaps or dashboards showing likelihood vs. impact

✓ Use color coding and categories to enhance clarity

✓ Present summaries in leadership or board reports

27. Duplicate or Overlapping Risks in Register

📌 **Clause: 6.4 – Risk Identification**

What's going wrong:
Different departments record similar risks under different names, creating redundancy and confusion.

Why it matters:
Duplicates distort reporting and dilute accountability. Auditors see this as a sign of poor register governance.

How to fix it:

✓ Periodically review the register for duplicates

✓ Consolidate similar risks and clarify descriptions

✓ Assign ownership to the most relevant function

28. No Process for Validating Control Effectiveness

📌 **Clause: 6.5 – Risk Treatment**

What's going wrong:

Controls are listed in treatment plans, but there's no follow-up testing or evidence that they work.

Why it matters:

ISO 31000 expects a results-based approach. It's not enough to assign controls — you must test them.

How to fix it:

✓ Define performance indicators for each control

✓ Schedule periodic control testing or assurance activities

✓ Document test results and improvements made

29. External Risks Are Not Considered

📌 **Clause: 6.3 – Establishing Context**

What's going wrong:

Focus remains on internal risks (e.g., process failures), while external ones (e.g., regulatory changes, supplier instability, pandemics) are neglected.

Why it matters:
ISO 31000 encourages scanning of external environments. Ignoring them can lead to blind spots.

How to fix it:
✓ Include external risk drivers in context analysis
✓ Use tools like PESTLE to identify them
✓ Engage external experts or sources for insight

30. No Version Control for Risk Framework Documents

📌 **Clause: 5.2 & 5.6 – Policy and Improvement**

What's going wrong:
Policy documents, registers, and templates exist in multiple, inconsistent versions with no change history.

Why it matters:
Lack of version control undermines audit readiness and weakens confidence in governance.

How to fix it:
✓ Implement version numbers, update logs, and ownership fields
✓ Store risk documents in a central, controlled location
✓ Communicate updates to all relevant stakeholders

31. No Process for Linking Risks to Business Continuity Plans (BCP)

📌 Clause: 6.3 – Risk Context and Understanding Organizational Needs

What's going wrong:
The business continuity team operates separately from risk management, resulting in gaps when real-world disruptions occur.

Why it matters:
ISO 31000 emphasizes a unified, organization-wide view of risk. If risks aren't reflected in BCPs, recovery efforts may be ineffective.

How to fix it:
✓ Map high-priority risks to corresponding business continuity plans
✓ Involve the risk team in BCP development and drills
✓ Track continuity response effectiveness as part of your risk review cycle

32. Lack of Defined Criteria for Residual Risk Acceptance

📌 Clause: 6.5 – Risk Treatment

What's going wrong:
Residual risk is vaguely documented with no standard to determine whether it's acceptable, often leading to under-treated threats.

Why it matters:
Auditors want to see how organizations determine when a risk is sufficiently mitigated, and whether that decision aligns with risk appetite.

How to fix it:
✓ Define acceptable residual risk levels by category

✓ Require review and approval of residual risks before closure

✓ Reassess if organizational priorities or external conditions change

33. No Centralized Repository for Risk Documents and Logs

📌 **Clause: 7.5 – Documented Information**

What's going wrong:
Risk assessments, registers, treatment plans, and audit trails are scattered across spreadsheets and emails, with no centralized control.

Why it matters:
ISO-aligned frameworks require accessible, secure, and version-controlled documentation. Poor documentation is a red flag during audits.

How to fix it:

✓ Implement a centralized risk documentation platform (e.g., SharePoint, GRC tool)

✓ Assign documentation custodians

✓ Regularly audit access, updates, and data integrity

34. Lack of Regular Internal Audits on Risk Framework Effectiveness

📌 **Clause: 6.6 – Monitoring and Review**

What's going wrong:
Internal audit does not evaluate the risk management framework as part of its audit plan. Gaps go unnoticed until external reviews.

Why it matters:
Internal audits are a core component of continual improvement under ISO 31000.

How to fix it:
✓ Add risk management audits to your annual audit plan
✓ Include reviews of risk identification, treatment, ownership, and documentation
✓ Share findings with executive leadership for improvement actions

35. No Defined Process for Updating Risk Framework After Major Incidents

📌 **Clause: 5.6 – Continual Improvement**

What's going wrong:
When a critical incident occurs (e.g., cyberattack, legal dispute), lessons are learned but not used to update the framework.

Why it matters:
ISO 31000 expects organizational learning and framework refinement after real-life disruptions.

How to fix it:
✓ Conduct post-incident reviews for all major events
✓ Identify root causes and missed risks
✓ Update risk register, controls, and training based on findings

36. Risk Treatment Does Not Consider Cost-Benefit Analysis

📌 **Clause: 6.5 – Selecting Risk Treatment Options**

What's going wrong:
Controls are implemented without evaluating whether the cost of mitigation outweighs the benefit or whether better alternatives exist.

Why it matters:
Risk treatment should be proportionate and value-driven. ISO 31000 encourages resource efficiency alongside effectiveness.

How to fix it:
✓ Include cost-benefit analysis as a required field in treatment planning
✓ Compare alternative treatments with estimated effectiveness
✓ Consult finance or procurement teams during implementation

37. Over-Reliance on Risk Matrices Without Qualitative Context

📌 **Clause: 6.3.3 – Risk Analysis**

What's going wrong:
Risks are scored and placed on a matrix, but without narrative descriptions, causes, or scenarios to bring clarity or support decisions.

Why it matters:
ISO 31000 promotes both quantitative and qualitative understanding. Numbers without context limit strategic relevance.

How to fix it:
✓ Require narrative descriptions for each risk, not just scores

✓ Include root cause, scenario examples, and potential consequences
✓ Ensure context supports prioritization and treatment decisions

38. No Use of Heatmaps or Risk Dashboards for Reporting

📌 **Clause: 6.6 – Communication and Review**

What's going wrong:
Risk data is stored in tables or spreadsheets that are not visually digestible, slowing down decision-making at the leadership level.

Why it matters:
Visual tools improve communication, clarity, and engagement, especially at the executive and board level.

How to fix it:
✓ Implement heatmaps, bubble charts, or dashboards for top risks
✓ Use visual cues (color, size, trend) to signal severity and urgency
✓ Update visuals regularly for leadership reviews

39. No Evidence of Stakeholder Consultation in Setting Risk Context

📌 **Clause: 6.3.1 – Establishing the Context**

What's going wrong:
The organizational context is defined without consulting departments, customers, or other relevant stakeholders.

Why it matters:
ISO 31000 emphasizes external and internal stakeholder engagement in establishing the environment in which risks arise.

How to fix it:

✓ Conduct interviews or surveys when defining or updating context

✓ Involve representatives from operations, legal, compliance, and external partners

✓ Document contributions in the context-setting process

40. Controls Are Not Reviewed for Ongoing Relevance

📌 **Clause: 6.6 – Monitoring and Review**

What's going wrong:

Once implemented, risk controls are not periodically reviewed. They may become outdated due to tech changes, process shifts, or new threats.

Why it matters:

Static controls are ineffective over time. ISO 31000 promotes active monitoring and review.

How to fix it:

✓ Define review intervals for all key controls

✓ Reassess control effectiveness based on performance, incidents, and environment

✓ Retire or replace obsolete measures and update documentation

41. No Mechanism to Track Risk Interdependencies

📌 **Clause: 6.3 – Risk Identification and Context**

What's going wrong:

Risks are recorded as isolated entries. Dependencies between risks (e.g.,

how a supplier risk affects reputational risk) are not documented or analyzed.

Why it matters:
ISO 31000 encourages holistic risk awareness. Overlooking interdependencies can lead to cascade failures.

How to fix it:
✓ Include a "related risks" field in the risk register
✓ Use mapping tools or network diagrams to show connections
✓ Evaluate how one risk can amplify or trigger others during assessment

42. No Structured Risk Prioritization Process

📌 **Clause: 6.4 – Risk Evaluation**

What's going wrong:
Once risks are rated, there's no consistent method to prioritize which ones need immediate attention or additional resources.

Why it matters:
Prioritization enables efficient treatment and aligns efforts with strategy and risk appetite.

How to fix it:
✓ Rank risks based on their overall score and strategic impact
✓ Highlight top risks in executive summaries and dashboards
✓ Align priorities with leadership input and resource capacity

43. Inconsistent Use of Residual vs. Inherent Risk

📌 **Clause: 6.3.3 – Risk Analysis**

What's going wrong:
Some risks are rated without clarifying whether the rating reflects inherent risk (before controls) or residual risk (after controls).

Why it matters:
Lack of clarity confuses reporting and decision-making. Auditors may question accuracy and risk visibility.

How to fix it:
✓ Define and train teams on inherent vs. residual risk
✓ Require both to be recorded in the register
✓ Use side-by-side comparisons to show treatment effectiveness

44. No Review of Risk Relevance After Organizational Changes

📌 **Clause: 6.6 – Monitoring and Review**

What's going wrong:
New product lines, market entries, leadership changes, or tech upgrades occur without triggering a formal reassessment of existing risks.

Why it matters:
ISO 31000 expects the risk framework to adapt to change. Static registers reflect poor governance.

How to fix it:
✓ Define triggers that require risk review (e.g., M&A, new regulations)

✓ Add change impact reviews into project governance

✓ Reassess both new and existing risks after major shifts

45. No Involvement of the Board or Executive Committee in Risk Oversight

📌 **Clause: 5.1 – Leadership Commitment**

What's going wrong:
Risk reports are shared only at the operational level. There is limited or no engagement from top leadership or the board.

Why it matters:
Strategic risks require strategic oversight. ISO 31000 demands active leadership involvement.

How to fix it:

✓ Present top risks at quarterly board or executive meetings

✓ Include risk as a standing agenda item

✓ Use board-level risk dashboards and summaries

46. Risk Controls Are Not Aligned with Risk Severity

📌 **Clause: 6.5 – Risk Treatment**

What's going wrong:
Low-level risks receive heavy control investment, while high-level risks may be under-treated.

Why it matters:
Misaligned resources reduce cost-efficiency and expose the organization to unmanaged threats.

How to fix it:
✓ Link control strength to risk rating and risk appetite
✓ Rebalance mitigation efforts in periodic control reviews
✓ Reallocate budgets based on updated priorities

47. Lack of Version Control for Risk Documents

📌 **Clause: 7.5 – Documented Information**

What's going wrong:
Multiple versions of the risk register or policy exist across teams. There's confusion about which is current or official.

Why it matters:
Auditors expect documented traceability. Inconsistent records reduce trust and auditability.

How to fix it:
✓ Use version-controlled templates or document management tools
✓ Mark each update with date, editor, and change log
✓ Limit edit access to authorized roles

48. No Differentiation Between Strategic and Operational Risks

📌 **Clause: 6.3.1 – Establishing Context**

What's going wrong:
All risks are lumped together, blurring the line between daily operational issues and long-term strategic threats.

Why it matters:
ISO 31000 encourages context-based risk assessment. Without categorization, leadership can't focus on what truly matters.

How to fix it:

✓ Tag risks as strategic, operational, financial, compliance, etc.

✓ Segment reporting views accordingly

✓ Use different escalation paths based on type and impact

49. No Mechanism to Reassess Risks After Incidents or Near Misses

📌 **Clause: 6.6 – Monitoring and Review**

What's going wrong:
Incidents are investigated, but there's no feedback loop into the risk register to reflect changes in likelihood or impact.

Why it matters:
ISO 31000 emphasizes adaptability and learning. Ignoring incidents limits growth and weakens controls.

How to fix it:

✓ Review related risks after every incident or near miss

✓ Adjust scores, treatment plans, or ownership as needed

✓ Document lessons learned and communicate to stakeholders

50. Risk Roles Are Not Defined in Job Descriptions

📌 **Clause: 5.3 – Roles and Responsibilities**

What's going wrong:
Staff are assigned as "risk owners" but have no clarity on what that role entails, nor is it reflected in their formal responsibilities.

Why it matters:
ISO 31000 expects clear accountability structures. Undefined roles lead to passive risk management.

How to fix it:

✓ Include risk responsibilities in job descriptions and performance goals

✓ Define what ownership entails (e.g., monitoring, reporting, treatment updates)

✓ Provide role-based training and guidance materials

51. No Integration Between Risk Management and Internal Audit Planning

📌 **Clause: 5.3 – Integration into the Organization**

What's going wrong:
Risk management and internal audit operate separately. Audit planning is not informed by the risk register or strategic risk profile.

Why it matters:
ISO 31000 promotes integration across governance functions. Internal audit should test the effectiveness of risk treatments.

How to fix it:
✓ Involve risk managers in audit scoping sessions
✓ Prioritize audit areas based on the organization's top risks
✓ Share risk updates with audit committees regularly

52. Lack of Defined Triggers for Reassessing Risks

📌 **Clause: 6.6 – Monitoring and Review**

What's going wrong:
Risks are reassessed irregularly, with no policy outlining what types of changes should prompt an immediate review.

Why it matters:
Timely risk reassessment ensures continued accuracy and relevance in decision-making.

How to fix it:
✓ Create a trigger list (e.g., market entry, regulatory change, incident)
✓ Add it to your risk management policy
✓ Train risk owners to report when triggers occur

53. No Formal Risk Escalation Matrix or Process

📌 **Clause: 5.3 – Roles and Responsibilities**

What's going wrong:
Teams aren't sure when or how to escalate risks. Some issues are handled at the wrong level, resulting in delay or exposure.

Why it matters:
Escalation ensures that risks are addressed by the appropriate authority based on impact and urgency.

How to fix it:
✓ Develop an escalation matrix based on risk severity
✓ Define timeframes and responsible roles for each level
✓ Incorporate escalation guidance into training and governance documents

54. Inadequate Risk Assessments During Project Planning

📌 **Clause: 6.3 – Risk Assessment and Context**

What's going wrong:
Projects proceed without structured risk assessments or are reviewed too late (e.g., during execution).

Why it matters:
ISO 31000 encourages embedding risk assessment into decision-making — especially for change initiatives.

How to fix it:
✓ Require a risk impact summary in every project proposal

✓ Include project risks in the central risk register

✓ Reassess risks at each project stage or gate review

55. No Risk-Based Criteria for Vendor or Third-Party Selection

📌 **Clause: 6.3 – External Risk Context**

What's going wrong:
Vendor selection focuses on cost and capability, but not risk exposure (e.g., data handling, geopolitical ties, financial health).

Why it matters:
Third-party risk is a major source of operational disruption and reputational harm. ISO 31000 encourages external context analysis.

How to fix it:

✓ Add a risk scoring section to vendor evaluation templates

✓ Include compliance, cybersecurity, and resilience criteria

✓ Periodically reassess critical vendors

56. Risk Committee Does Not Include Cross-Functional Representation

📌 **Clause: 5.3 – Roles and Engagement**

What's going wrong:
Risk governance is centralized in one team (e.g., finance or compliance), leaving key departments underrepresented.

Why it matters:
ISO 31000 encourages broad participation and context awareness from across the organization.

How to fix it:

✓ Include representatives from operations, HR, IT, legal, and strategy

✓ Rotate participation to maintain relevance and buy-in

✓ Empower members to bring forward emerging risks from their domains

57. No Process to Evaluate Reputational Impact of Risks

📌 **Clause: 6.3.1 – Establishing Risk Criteria**

What's going wrong:

Risks are scored based on financial or operational impact only. Reputational damage is overlooked or downplayed.

Why it matters:

Reputational risks can have far-reaching and long-lasting effects. ISO 31000 supports holistic, stakeholder-focused assessments.

How to fix it:

✓ Include reputation in your risk impact matrix

✓ Use stakeholder mapping to anticipate consequences

✓ Work with communications or PR teams during assessments

58. Risk Assessments Do Not Account for Cumulative Risk Exposure

📌 **Clause: 6.3.3 – Risk Analysis**

What's going wrong:

Individual risks are assessed in isolation, ignoring the compounding effect of multiple concurrent risks.

Why it matters:
ISO 31000 promotes systemic thinking. Compound risk exposure can increase vulnerability.

How to fix it:
✓ Review high-risk clusters and combined risk scenarios
✓ Use scenario modeling for simultaneous events (e.g., supply chain + cyber)
✓ Reevaluate treatment strategies accordingly

59. No Process for Reviewing Risk Management Training Effectiveness

📌 **Clause: 7.2 – Competence and Awareness**

What's going wrong:
Training is delivered, but there's no assessment of whether it actually improves awareness, knowledge, or behavior.

Why it matters:
Effectiveness reviews support ISO 31000's principle of continual improvement and competence development.

How to fix it:
✓ Include quizzes or case-based assessments post-training
✓ Survey participants on confidence and clarity
✓ Adjust future sessions based on feedback and observed performance gaps

60. Risk Reporting Is Too Technical for Executive Leadership

📌 **Clause: 6.2 – Communication and Consultation**

What's going wrong:
Risk reports are data-heavy and filled with jargon, making them inaccessible to senior leaders and board members.

Why it matters:
ISO 31000 encourages tailored communication. Reports should be clear, actionable, and strategic at the leadership level.

How to fix it:
✓ Use visual dashboards and executive summaries
✓ Highlight key messages: top 5 risks, trends, treatment status
✓ Avoid technical language; use business-impact framing

61. No Risk Ownership at the Executive Level

📌 **Clause: 5.1 – Leadership Commitment**

What's going wrong:
Executives approve risk reports but don't personally own or monitor specific strategic risks.

Why it matters:
ISO 31000 emphasizes leadership accountability. Lack of executive ownership results in limited engagement and slow mitigation.

How to fix it:
✓ Assign top strategic risks to individual executives
✓ Include risk performance in leadership scorecards
✓ Discuss updates in monthly or quarterly exec reviews

62. Lessons Learned from Incidents Are Not Fed Back into the Risk Framework

📌 Clause: 5.6 – Continual Improvement

What's going wrong:
After-action reviews happen, but they're disconnected from risk registers, control improvements, or training adjustments.

Why it matters:
ISO 31000 supports learning and continuous improvement. Failing to act on lessons leads to recurring failures.

How to fix it:
✓ Make post-incident reviews a formal input to the risk review process
✓ Document lessons in the risk register
✓ Use trends to update training, controls, and treatment plans

63. No Alignment Between Risk Treatment Plans and Budgeting

📌 Clause: 6.5 – Risk Treatment

What's going wrong:
Risk mitigation actions are approved but unfunded, causing delays or shortcuts.

Why it matters:
Without funding, treatment plans remain theoretical. Auditors often flag this as a disconnect between risk intent and execution.

How to fix it:
✓ Involve finance in risk treatment planning
✓ Estimate treatment costs and include them in the annual budget
✓ Prioritize funding based on risk ratings and urgency

64. No Consideration of ESG Risks in the Risk Management Framework

📌 Clause: 6.3 – Establishing Context

What's going wrong:
Environmental, social, and governance (ESG) risks are not formally assessed, despite increasing regulatory and stakeholder pressure.

Why it matters:
ISO 31000 calls for full-spectrum risk identification. ESG is now a material concern across industries.

How to fix it:
✓ Add ESG categories to your risk taxonomy
✓ Use stakeholder impact analysis during assessments
✓ Involve sustainability teams in the risk process

65. Lack of a Defined Risk Communication Strategy

📌 Clause: 6.2 – Communication and Consultation

What's going wrong:
Risk communication is inconsistent, informal, or left to individual departments.

Why it matters:
ISO 31000 promotes structured, inclusive communication to create alignment and awareness.

How to fix it:
✓ Create a communication plan outlining channels, audiences, and frequency
✓ Define how risk updates are shared across levels
✓ Incorporate feedback loops to capture concerns from all stakeholders

66. No Integration of Cybersecurity Risks into Enterprise Risk Register

📌 Clause: 6.3 – Risk Identification and Analysis

What's going wrong:
Cyber risks are handled by IT or InfoSec in isolation — with no integration into the wider enterprise risk picture.

Why it matters:
Cyber risks affect reputation, operations, and compliance. ISO 31000 supports an enterprise-wide approach.

How to fix it:
✓ Integrate key cyber risks into the main risk register
✓ Map their cross-functional impact (finance, HR, legal)
✓ Include IT in strategic risk reviews

67. Inadequate Use of Quantitative Risk Analysis Methods

📌 Clause: 6.3.3 – Risk Analysis

What's going wrong:
All risks are scored qualitatively (e.g., high/medium/low), even when data exists to quantify impact or probability.

Why it matters:
ISO 31000 encourages both qualitative and quantitative techniques. Lack of quantification weakens prioritization.

How to fix it:
✓ Apply Monte Carlo simulations, expected loss models, or cost-impact estimates for high-value risks
✓ Train risk analysts in basic quantitative methods
✓ Use both types of analysis where possible

68. No Documentation of Risk Context Updates Over Time

📌 **Clause: 6.3.1 – Establishing the Context**

What's going wrong:
Risk context (e.g., internal structure, external environment) is not formally reviewed or updated, even when business conditions change.

Why it matters:
Context influences how risks are perceived and managed. ISO 31000 requires context to be clear and current.

How to fix it:
✓ Review internal and external context annually or after major changes
✓ Document and track changes (e.g., via version-controlled records)
✓ Align context updates with risk criteria and assessment processes

69. No Engagement with External Stakeholders During Risk Assessment

📌 **Clause: 6.2 – Communication and Consultation**

What's going wrong:
Customers, partners, investors, or regulators are not consulted when assessing risks that affect them directly.

Why it matters:
ISO 31000 promotes stakeholder-driven risk awareness. Overlooking them may result in blind spots or reputational risk.

How to fix it:
✓ Identify key external stakeholders for each major risk area
✓ Conduct interviews, surveys, or advisory forums
✓ Include stakeholder perspectives in risk narratives

70. Risk Framework Not Aligned with Other Management Systems (e.g., ISO 9001, ISO 27001)

📌 **Clause: 5.3 – Integration**

What's going wrong:
The risk framework operates separately from quality, information security, or environmental management systems, leading to duplication or inconsistency.

Why it matters:
ISO 31000 supports integration with other standards. Misalignment weakens both efficiency and audit readiness.

How to fix it:
✓ Map overlapping clauses and processes across standards
✓ Create a shared risk register or cross-reference matrix
✓ Coordinate risk treatment efforts across functions

71. Risk Framework Does Not Reflect Regulatory Requirements

📌 **Clause: 6.3 – Understanding External Context**

What's going wrong:
Compliance obligations (e.g. GDPR, SOX, environmental laws) are handled separately from risk management, resulting in siloed awareness and exposure gaps.

Why it matters:
ISO 31000 calls for external context awareness. Ignoring regulatory risk weakens compliance, oversight, and audit performance.

How to fix it:
✓ Integrate legal, regulatory, and compliance teams into risk reviews

✓ Add “regulatory exposure” as a column in your risk register
✓ Link risks to legal requirements and obligations

72. Inconsistent Use of Risk Categories Across Departments

📌 **Clause: 6.3.2 – Risk Identification**

What’s going wrong:
Different teams use different definitions or categories for risks (e.g., HR calls it “talent risk,” while operations logs it under “staffing”).

Why it matters:
A shared taxonomy is critical for clarity, reporting, and aggregation across business units.

How to fix it:
✓ Standardize a risk category framework aligned with ISO 31000
✓ Include definitions in a glossary and risk templates
✓ Provide cross-functional training on risk classification

73. No Documentation of Assumptions Behind Risk Assessments

📌 **Clause: 6.3.1 – Establishing Context**

What’s going wrong:
Risk ratings are assigned, but the rationale and assumptions behind impact and likelihood scores are not documented.

Why it matters:
ISO 31000 supports transparency. Without context, scores can’t be challenged, updated, or justified to auditors or leadership.

How to fix it:
✓ Require a “rationale” or “assumptions” field in your risk register

✓ Document scenarios, data sources, and any uncertainty
✓ Review and update assumptions regularly

74. No Consideration of Positive Risk (Opportunities)

📌 **Clause: 6.3 – Risk Identification**

What's going wrong:
Risk is only seen as a threat, not as uncertainty that could lead to upside (e.g., market entry, innovation, tech advantage).

Why it matters:
ISO 31000 defines risk as *effect of uncertainty on objectives*, which includes both threats and opportunities.

How to fix it:
✓ Add "opportunity risks" to the register where relevant
✓ Evaluate upside scenarios in strategic planning
✓ Encourage business units to identify innovation-based risks

75. No Risk-Based Criteria for Investment or CapEx Decisions

📌 **Clause: 5.3 – Integration into Decision-Making**

What's going wrong:
Major investments are evaluated on ROI and payback alone, with no consideration of associated risks.

Why it matters:
Risk-informed capital planning ensures smarter investments and resource allocation.

How to fix it:
✓ Require a formal risk section in investment/business case templates

✓ Include risk-adjusted return calculations where applicable
✓ Review top risks in CapEx committee discussions

76. No Clear Risk Reporting Line to the Board or Audit Committee

📌 **Clause: 5.1 – Leadership Oversight**

What's going wrong:
Risk reporting stops at mid-management. The board lacks regular, structured updates on top risks.

Why it matters:
ISO 31000 requires leadership oversight. Board engagement is critical for strategic risk governance.

How to fix it:
✓ Set a quarterly board risk reporting cadence
✓ Use dashboards and executive summaries
✓ Align reporting with board priorities and risk appetite

77. No Framework for Measuring Risk Management Maturity

📌 **Clause: 5.6 – Continual Improvement**

What's going wrong:
There is no method to evaluate the maturity, effectiveness, or evolution of the risk management framework itself.

Why it matters:
ISO 31000 supports iterative improvement. Without maturity assessments, organizations can't track progress.

How to fix it:
✓ Use a risk maturity model (e.g., 5-level scoring for culture, integration,

tools, etc.)

✓ Assess annually and benchmark over time

✓ Use results to plan capability-building efforts

78. Lack of Integration Between Risk and Strategy Teams

📌 **Clause: 5.3 – Integration into Organizational Planning**

What's going wrong:
Strategic planning happens independently of risk teams. Long-term objectives are pursued without structured risk analysis.

Why it matters:
Strategic risks are among the most impactful. ISO 31000 promotes embedding risk into decision-making at all levels.

How to fix it:

✓ Require risk participation in strategic planning workshops

✓ Evaluate risk exposure of each strategic pillar or initiative

✓ Align KPIs and risk indicators

79. No Defined Risk Criteria for Project Approvals

📌 **Clause: 6.3.1 – Establishing Risk Criteria**

What's going wrong:
Projects are greenlit without a consistent risk threshold or formal evaluation against risk appetite.

Why it matters:
ISO 31000 promotes objective, criteria-based risk analysis. Inconsistency creates misaligned investments and exposure.

How to fix it:

✓ Set thresholds for project risk tolerance (financial, reputational, timeline)

✓ Add risk approval gates into project governance

✓ Document rationale for acceptance or rejection

80. No Use of Technology to Automate Risk Monitoring

📌 **Clause: 6.6 – Monitoring and Review**

What's going wrong:
Risk monitoring relies on manual updates. Changes in exposure (e.g., supply chain, financials, IT performance) are slow to detect.

Why it matters:
ISO 31000 supports active, real-time monitoring where possible. Manual-only systems limit responsiveness.

How to fix it:

✓ Use integrated risk dashboards that pull from live data sources

✓ Automate KRIs where feasible (e.g., threshold alerts, performance drops)

✓ Build escalation triggers into system logic

81. No Clear Method for Aggregating Risk at the Enterprise Level

📌 **Clause: 6.4 – Risk Evaluation**

What's going wrong:
Individual business units manage their risks, but there's no method to consolidate or compare them across the enterprise.

Why it matters:
ISO 31000 promotes a holistic view. Without aggregation, leadership lacks a clear picture of the organization's overall exposure.

How to fix it:

✓ Define a methodology for consolidating risks (e.g., heatmaps, weighted scoring)

✓ Use common metrics and criteria across departments

✓ Present integrated risk views to executives and the board

82. No Consideration of Risk Velocity or Speed of Onset

📌 **Clause: 6.3.3 – Risk Analysis**

What's going wrong:
Risks are ranked by impact and likelihood, but how quickly they could unfold isn't assessed.

Why it matters:
ISO 31000 encourages thorough risk understanding. Fast-moving risks may need more urgent treatment, even if they seem low-impact.

How to fix it:

✓ Add a "velocity" or "speed of onset" field to your risk register

✓ Prioritize quick-impact risks in mitigation planning

✓ Use this as part of escalation criteria

83. No Standard Risk Assessment Template or Tool

📌 **Clause: 7.5 – Documented Information**

What's going wrong:
Different departments use inconsistent formats for identifying and assessing risks, creating confusion and inefficiencies.

Why it matters:
A standardized process enhances transparency, quality, and auditability.

How to fix it:

✓ Create a universal ISO 31000-aligned risk assessment template

✓ Include fields for likelihood, impact, control status, and owner

✓ Make it accessible via your risk management platform or shared folder

84. No Independent Challenge or Review of Risk Assessments

📌 **Clause: 6.6 – Monitoring and Review**

What's going wrong:
Risk ratings are accepted at face value with no peer or second-line challenge function, allowing bias or blind spots to go unchecked.

Why it matters:
Independent review improves accuracy and supports good governance.

How to fix it:

✓ Implement peer reviews or "risk validation" sessions

✓ Involve internal audit or compliance as a challenge function

✓ Use dual-approval for high-impact risk scores

85. Risk Appetite Statement Is Too Vague or Generic

📌 **Clause: 5.4 – Risk Alignment**

What's going wrong:
The risk appetite statement is too broad (e.g., "We have low appetite for operational risk") and doesn't guide decision-making.

Why it matters:
ISO 31000 requires alignment between risk criteria and strategic decisions. Vague appetite offers no actionable boundaries.

How to fix it:

✓ Break down risk appetite by category (e.g., financial, reputational, compliance)

✓ Use clear thresholds (e.g., "Up to $100K in loss is acceptable without escalation")

✓ Regularly review and revise with leadership input

86. No Defined Roles for Second-Line Risk Oversight

📌 **Clause: 5.3 – Roles, Responsibilities, and Accountability**

What's going wrong:

Only first-line staff and the centralized risk function are involved. There's no defined oversight or guidance from a second line (e.g., compliance, legal).

Why it matters:

A three-lines-of-defense model strengthens risk assurance and monitoring.

How to fix it:

✓ Define oversight roles for compliance, legal, and internal audit

✓ Assign second-line responsibilities in governance documents

✓ Create a formal handoff process between first and second lines

87. Risk Mitigation Measures Are Not Linked to KPIs or Business Outcomes

📌 **Clause: 6.5 – Risk Treatment**

What's going wrong:

Controls are implemented, but their effectiveness is not measured in relation to actual performance or business impact.

Why it matters:
ISO 31000 encourages risk-informed performance tracking. Otherwise, risk treatment becomes reactive or symbolic.

How to fix it:
✓ Link mitigation actions to specific KPIs or OKRs
✓ Track both implementation and impact (e.g., reduction in incidents)
✓ Adjust treatments based on data and trend insights

88. Risk Reports Are Not Timely Enough to Support Decision-Making

📌 **Clause: 6.6 – Monitoring and Review**

What's going wrong:
By the time risk data is reported, the business has already made decisions, reducing its relevance and value.

Why it matters:
ISO 31000 promotes actionable and real-time risk awareness, especially in fast-moving environments.

How to fix it:
✓ Shift from static quarterly reports to dynamic dashboards
✓ Use rolling risk reviews and quick-update templates
✓ Align reporting cycles with key decision windows

89. No Defined Process for Retiring or Archiving Obsolete Risks

📌 **Clause: 6.6 – Review and Documentation**

What's going wrong:
Old risks remain in the register even after they've been mitigated, resolved, or become irrelevant — cluttering reports and wasting review time.

Why it matters:
Risk records should reflect current exposure. Outdated entries reduce efficiency and dilute focus.

How to fix it:

✓ Define a risk closure process with review checkpoints

✓ Create an "archived risks" tab in your register

✓ Maintain records for audit traceability with documented closure rationale

90. Lack of a Crisis Communication Plan Tied to High-Risk Scenarios

📌 **Clause: 6.5 – Risk Response and Preparedness**

What's going wrong:
The organization identifies high-severity risks (e.g., data breach, fraud) but doesn't have prepared messaging or escalation protocols.

Why it matters:
When high-impact risks materialize, communication is key to managing reputational fallout and stakeholder trust.

How to fix it:

✓ Develop communication templates for top risks

✓ Define spokespersons, escalation contacts, and stakeholder scripts

✓ Test through tabletop exercises or simulations

91. No Consideration of Long-Term Strategic Risks in Planning Cycles

📌 Clause: 6.3 – Risk Identification

What's going wrong:
Risk focus is short-term — limited to quarterly cycles or operational concerns. Disruptive risks like market shifts, climate change, or geopolitical instability are left out.

Why it matters:
ISO 31000 encourages long-term, forward-looking risk identification to build resilience.

How to fix it:

✓ Conduct annual strategic risk workshops

✓ Use scenario planning and PESTLE analysis for macro-risk awareness

✓ Include long-term risks in board-level risk dashboards

92. No Documentation of Changes Made to Risk Ratings Over Time

📌 Clause: 6.6 – Monitoring and Review

What's going wrong:
Risk scores change between reviews, but the reason for the change isn't recorded, making it hard to track trends or justify decisions.

Why it matters:
Audit trails are essential for transparency and improvement. ISO 31000 supports tracking changes and rationales.

How to fix it:

✓ Add a "revision history" section to your risk register

✓ Log every change with a timestamp and explanation

✓ Review trends in audit or committee meetings

93. No Role-Based Access Control for Risk Data

📌 **Clause: 7.5 – Documented Information (Confidentiality & Integrity)**

What's going wrong:
All users have the same access to risk documents, increasing the chance of unauthorized edits or visibility of sensitive risks.

Why it matters:
ISO 31000 requires secure handling of risk information. Access control protects confidentiality and data integrity.

How to fix it:
✓ Restrict edit/view access based on user role and department
✓ Use GRC platforms or permission-controlled folders
✓ Log all access and changes for traceability

94. No Plan for Risk Framework Review During Mergers or Restructures

📌 **Clause: 5.6 – Continual Improvement**

What's going wrong:
During M&A or internal restructures, the risk framework is not reviewed or updated, despite major changes in context and exposure.

Why it matters:
ISO 31000 emphasizes adaptability. A stagnant framework post-change weakens governance and control.

How to fix it:
✓ Trigger a framework review during organizational changes
✓ Reassess risk roles, appetite, and context
✓ Rebuild your register based on new objectives and structures

95. Overemphasis on Known Risks at the Expense of Emerging Ones

📌 Clause: 6.3.2 – Risk Identification

What's going wrong:
The register is dominated by traditional risks. New or hard-to-quantify risks (e.g., AI ethics, ESG backlash, misinformation) are ignored.

Why it matters:
ISO 31000 requires continual risk scanning. Over-focusing on the past blinds you to the future.

How to fix it:
✓ Create a dedicated "emerging risks" category
✓ Review tech, regulatory, and societal trends quarterly
✓ Engage external experts or futurists in risk planning

96. No Clear Link Between Risk Appetite and Performance Metrics

📌 Clause: 5.4 – Alignment with Organizational Objectives

What's going wrong:
Risk appetite is defined, but KPIs and KRIs are set without alignment, leading to contradictory decisions.

Why it matters:
ISO 31000 calls for coherence between performance and risk culture.

How to fix it:
✓ Cross-reference KPIs and risk appetite during planning
✓ Set KRIs that act as early warning signals
✓ Adjust incentives and goals based on risk tolerance

97. Lack of Defined Risk Taxonomy for Digital Transformation Risks

📌 **Clause: 6.3 – Risk Identification**

What's going wrong:
Digital and innovation-related risks (e.g., AI misuse, algorithmic bias, legacy system risk) are poorly defined or missing.

Why it matters:
ISO 31000 encourages dynamic and current risk identification.

How to fix it:
✓ Update taxonomy to include digital transformation categories
✓ Work with IT, innovation, and product teams to map digital risks
✓ Assess ethical, operational, and technical risk layers

98. Stakeholder Expectations Not Considered in Risk Criteria Development

📌 **Clause: 6.3.1 – Establishing Context and Criteria**

What's going wrong:
Risk criteria are developed internally, with no consultation from investors, customers, regulators, or partners.

Why it matters:
ISO 31000 promotes inclusive consultation. Overlooking external viewpoints may lead to blind spots.

How to fix it:
✓ Survey or consult key stakeholders annually
✓ Include stakeholder impact as a scoring dimension
✓ Use insights to refine impact definitions and prioritization

99. No Contingency Planning for High Residual Risks

📌 **Clause: 6.5 – Risk Treatment**

What's going wrong:
Some residual risks remain high after treatment — but there's no "Plan B" if controls fail or issues escalate.

Why it matters:
ISO 31000 encourages preparedness and realism. High residual risks must have response plans.

How to fix it:
✓ Identify risks that exceed tolerance after mitigation
✓ Create contingency or crisis response plans
✓ Test and communicate them to relevant teams

100. Risk Management Is Not Integrated Into Organizational Culture

📌 **Clause: 5.1 – Principles and Risk-Aware Culture**

What's going wrong:
Risk is seen as a compliance function, not a shared value. Employees don't feel empowered to report concerns or propose improvements.

Why it matters:
ISO 31000's success depends on embedding risk into behaviors, mindsets, and values.

How to fix it:
✓ Promote risk awareness through campaigns, training, and leadership messaging
✓ Recognize employees who proactively manage or report risks
✓ Include risk competency in performance evaluations

Strengthening Your ISO 31000 Risk Management Framework

Effective risk management is more than a box to check — it's a long-term investment in resilience, decision-making, and stakeholder trust. ISO 31000:2018 provides a powerful, adaptable framework for managing uncertainty, but even the most experienced organizations encounter gaps in execution.

This guide has outlined **100 of the most frequent and costly non-conformities** seen across industries. By proactively addressing these issues, you're not only improving your alignment with ISO 31000 — you're building a foundation for smarter strategy, stronger governance, and more agile performance.

What's Next?

- **Embed Risk Culture Across All Levels**
  Make risk awareness part of your organization's DNA — from leadership to the front line.
- **Keep the Framework Alive**
  ISO 31000 is dynamic. Regular reviews, stakeholder engagement, and emerging risk scans keep it relevant and future-ready.
- **Link Risk to Strategy and Performance**
  Align your risk appetite with business goals, KPIs, and investment decisions to turn governance into growth.
- **Use This Guide as a Continuous Improvement Tool**
  Revisit it during audits, training, or annual reviews to close new gaps, evolve your program, and stay ahead of regulatory or market change.

Whether you're preparing for an audit, designing your risk architecture, or maturing an existing framework, this checklist is your companion for navigating complexity with confidence.

GSDC
Global Skill Development Council

CERTIFIED ISO 31000:2018 RISK MANAGER

ISO 31000 Certification is based on Risk Management Standards.

ABOUT GSDC CERTIFICATION

LIFETIME VALIDITY

GSDC Certification is an globally accreditted certification with lifetime validity.

EBOOK

Extensive and exclusive Ebook created by world's experts to help you with understanding core concepts.

CREATED BY EXPERTS

GSDC certifications are created and authored by world's leading experts in the field.

LEARNING MATERIALS

Get access to learning materials such as videos, ebooks, templates, and practice exams, which will help you clear the certification exam.

LEARNING OBJECTIVE

- **Ensure understanding of risk management frameworks aligned with ISO 31000.**
- **Demonstrate ability to develop and implement effective risk management strategies.**
- **Enhance career prospects in industries prioritizing robust risk management.**
- **Provide globally recognized certification in ISO 31000 risk management.**

Enroll now with the code **LEARN20** To avail **20%** discount

Enroll Now

www.gsdcouncil.org