UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
MANAGE COMPLIANCE (GOVERNANCE)

Risk and controls matrix (compliance)

Overview

Companies confront a magnitude of risks in compliance operations, the sources of which are varied and companywide. Leading companies implement control measures to manage those risks and to lessen the potential for noncompliance, which could have serious consequences, including regulatory fines, business interruption, and even loss of reputation.

The risk and controls matrix below identify many of the risks inherent in compliance functions as well as the sources of those risks, their possible consequences, and control measures to help manage them.

Please note that this information is at the generic business process level and that many companies will need to go beyond generic models to address the specific business processes that support the financial and nonfinancial disclosures being made. You can combine the insight of this business risk and control information with your industry-specific knowledge and understanding of your company's environment when conducting internal control assessments and designing and implementing recommendations.

UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
MANAGE COMPLIANCE (GOVERNANCE)

Key risks and controls

Business risk	Source of risk	Consequences of risk	Control measures
Company provides inadequate, inaccurate, or untimely regulatory and financial information.	• Ignorance or complexity of requirements, regulations, and filing deadlines • Lack of formal reporting policies, procedures, roles and responsibilities • Inadequate communication of reporting policies to all business units and subsidiaries • Lack of technology integration • Reporting silos • Disengaged board or senior leadership • Lack of employee training • Criminal intent	• Noncompliance • Greater vulnerability to fines, sanctions, litigation, and regulatory oversight • Erroneous disclosures • Hampered internal and external decision-making • Damage to reputation and brand value • Share price volatility • Undercapitalization • Inability to secure license to operate in new markets • Lower employee morale	• Integrate IT reporting systems • Identify key stakeholders and their information needs • Document and communicate reporting policies, disclosure schedules, and filing deadlines to all business units • Define reporting roles and responsibilities at all levels • Assign senior-level and board responsibility for timely, accurate disclosure • Provide compliance training • Establish and maintain relationships with regulators • Solicit an independent review of reporting policies and procedures • Leverage real-time reporting technologies
Business risk	Source of risk	Consequences of risk	Control measures

UNIVERSITY OF TOLEDO INTERNAL AUDIT DEPARTMENT
MANAGE COMPLIANCE (GOVERNANCE)

Compliance efforts are duplicated across the organization	• Lack of clear-cut compliance roles and responsibilities • Lack of regular communication between board and senior management • Ineffective oral and written communication between business unit leaders and between employees • Existence of information silos	• Unnecessary expenditure of time and capital • Inconsistent disclosure • Inconsistent execution of compliance activities • Greater confusion as to compliance goals and individual responsibilities	• Define clear roles and responsibilities • Monitor compliance management centrally • Ensure regular communication between compliance officer and business unit leaders • Communicate regularly with all employees • Establish a uniform set of internal compliance measures • Integrate technology systems
Business risk	Source of risk	Consequences of risk	Control measures
Company lacks	• Leadership and	• Low employee morale	• Convey a top-down

strong compliance leadership, or "tone at the top," at the executive level	board are indifferent or impervious to compliance responsibilities • Lack of focus on the importance of ethical conduct • Lack of education at the executive and board levels about compliance responsibilities • Criminal intent • Abuse of executive stock options incentives • Short-term value management	• High employee turnover • Reputational damage • Fines and sanctions • Greater regulatory scrutiny • Inability to achieve business objectives • Revenue losses • Legal costs • Loss of profitability	compliance mind-set from the senior leadership level • Establish an independent board • Require greater board involvement • Penalize executives for improper or unethical conduct • Separate the CEO and Chair positions • Restructure stock-option policies • Require management to sign certification of compliance • Monitor the company culture • Include ethics and integrity as categories for leadership performance reviews • Provide ethics training • Nurture a culture that values compliance
Business risk	Source of risk	Consequences of risk	Control measures
Company suffers brand or	• Unwillingness or inability to	• Higher cost of capital • Erosion of customer	• Create and promote a transparency

reputational damage	communicate company news in a candid, timely fashion, regardless of the circumstances	base • Erosion of investor base • Lower analyst ratings • Diminished brand value • Vulnerability to fines, sanctions, litigation, and greater regulatory oversight	framework • Communicate all news in a prompt, candid manner, regardless of the consequences • Implement a crisis communication plan • Establish and maintain strong relationships with analysts, regulators, investors, employees, and other key stakeholders
Business risk	Source of risk	Consequences of risk	Control measures
Employees are noncompliant	• Lack of cohesive compliance policy • Absence of	• Sanctions and fines • Damaged reputation and brand value	• Document and communicate compliance policies

	sustainable remediation procedures • Criminal intent • Uncertainty about compliance requirements • Lack of senior leadership commitment to compliance • Absence of board oversight • Lack of communication between senior leadership and the workforce about the importance of ethical behavior • Fear of reprisals if a misdeed is reported • Lack of internal controls • Inconsistent enforcement of disciplinary policies • Unethical board or senior leadership	• Low investor confidence • Increased regulatory scrutiny • Lost revenue • Low employee morale • Greater employee turnover • Increased litigation costs	and procedures • Provide confidential hotlines or other channels to report noncompliance • Offer incentives for compliance • Train employees to detect and report noncompliance • Implement sustainable remediation procedures • Provide ethics training
Business risk	Source of risk	Consequences of risk	Control measures
Company lacks clearly defined goals and aspirations for a	• Absence of compliance policies and procedures • Failure to designate	• Noncompliance • Vulnerability to fines and sanctions • Higher consulting costs	• Establish compliance policies and procedures • Designate an

compliant organization	an individual to administer compliance functions and monitor related laws and regulations • Inability to align necessary employee competencies with company goals • Lack of awareness of current compliance laws and regulations • Inadequate resource allocation for compliance	• Failure to meet performance potential • Greater vulnerability to risk scenarios Inability to respond to regulatory pressures • Greater confusion as to compliance goals and individuals' responsibilities	individual to manage the compliance process • Provide compliance training to employees companywide • Involve key employees and functional units in developing compliance procedures • Ensure top-down support and ongoing communication about compliance policies • Leverage online dashboards to gain a broader view of the organization's compliance performance
Business risk	Source of risk	Consequences of risk	Control measures
Company allocates inadequate resources for compliance risk management	• Indifferent or inattentive board and senior leadership • Poorly coordinated reporting and	• Reporting gaps • Problems are not resolved or remedied • Lack of an evolving compliance culture and	• Scrutinize compliance risk procedures to find gaps, redundancies, and unfulfilled tasks

	compliance efforts • Lack of compliance-related awareness • Budget constraints • Failure to identify key compliance responsibilities in each job • Alternative senior management priorities	mindset • Miscommunication to the marketplace • Negative perception among customers and investors • Emerging compliance issues and changes will not be recognized or addressed	• Centrally coordinate all compliance activities • Seek guidance from external regulators to improve efforts • Increase ethics and compliance training for all employees and board members • Benchmark against companies with strong compliance and reporting processes
Company's compliance functions are stagnant or ineffective	• Failure to regularly assess and refine compliance activities • Poor monitoring of emerging compliance issues • Complacency due to prolonged period without problems or new developments • Lack of emphasis on compliance from senior management • Turnover among key compliance personnel	• Not prepared to address new regulatory or reporting requirements • Surprised by a significant compliance lapse • Damage to reputation and stock price • Legal action against senior management • Declining employee morale	• Regularly assess and refine compliance activities • Monitor the regulatory and reporting environment on an ongoing basis • Establish and maintain relationships with regulators, lobbyists, and investigators • Provide ongoing training as needed • Capture the knowledge and best practices of key compliance staff
Business risk	Source of risk	Consequences of risk	Control measures
Compliance roles and responsibilities are not defined for employees at all levels of the	• Failure to create an organizational chart that clearly defines compliance roles and responsibilities	• Duplication of compliance efforts throughout the organization • Greater risk of	• Define and communicate compliance roles and responsibilities for

organization	• Lack of emphasis on compliance activities from senior leadership • Lower-level employees are not recognized for their critical role in the compliance equation	noncompliance • Low employee morale • Loss of reputation • Financial penalties	all employees • Convey a compliance mind-set at the senior leadership level • Ensure lower-level employee involvement in key compliance functions

Supporting material

A selection of governance, risk, and compliance best practices provide further insight into initiatives that can improve compliance and help companies manage risk.