

XYZ Company

Sarbanes Oxley 404 Compliance
Risk and Control Matrix

Location: Corporate
Process: Entity Level Assessment
Qualitative Risk Rating: High

Risk #	Risk ("What can go wrong?")	Control Objective	Control Activity	Control Number	Evidence of Control	Key Control	
Control Environment							
1	Employees are unsure of behavior that is expected of them by the company.	A Code of Conduct exists and has been implemented.	XYZ Corporation has a formal Code of Business Conduct policy. The company has adopted a Code of Business Conduct (COBC) Policy which was approved by the Board of Directors on April 7, 2005. Each new employee is provided a hard copy of the COBC and an employee handbook at orientation and must submit written confirmation of receipt.	ELA1	Code of Conduct	X	
3	Management could take an aggressive approach to accounting policies, resulting in inaccurate reporting and potential restatement.	Management exemplifies attitudes and actions reflecting a sound control environment and commitment to ethical values, and adopts accounting policies that best fit the economic realities of the business.	XYZ Corporation Management's financial reporting philosophy is conservative. The CFO has established a conservative approach to recording estimates, accruals and reserves.	ELA2	Accounting Policies	X	
4	Extreme incentives or temptations may exist which unnecessarily and unfairly test employees' adherence to ethical values.	Management strikes the appropriate balance between incentivizing employees and setting unrealistic performance targets.	Company goals are communicated to employees and linked to individual goals.	ELA3	Code of Conduct		
			Senior management compensation is established and monitored by the Board of Directors Compensation Committee. As outlined in XYZ's Compensation Committee Charter, the Compensation Committee, which is composed of three outside directors, is responsible for determining participants, defining the award opportunity, setting targets, and administering and interpreting the executive bonus plan and stock compensation plan.	ELA4	Audit Committee charter		
5	The Audit Committee is ineffective.	Audit Committee members are independent from management, have clearly articulated responsibilities, and understand those responsibilities.	The Audit Committee shall consist of two or more independent members; the Charter articulates specific authority and responsibility for overall governance. The Audit Committee has a charter which addresses the Audit Committee's Financial Reporting responsibilities. The Charter authorizes the Committee to conduct or initiate inquiries as needed. In addition, the Charter authorizes the Committee to retain, at the Company's expense, special legal, accounting or other consultants it deems necessary.	ELA5	Audit Committee charter		
			The Board receives key financial information at least quarterly. The Board receives a draft of the 10-Q and 10-K; its content is discussed and documented via minutes; the Audit Committee authorizes the issuance of the 10-Q/10-K.	ELA6	Board minutes		X
6	Management fails to set an appropriate "tone at the top" emphasizing, communicating, and enforcing a mindset of control consciousness. Management may fail to ensure that valuable assets including intellectual property and information stored both physical	Management, through its philosophy and operating style, promotes and enforces an appropriate level of acceptance of business risks, control consciousness, and safeguarding of assets.	The external auditor reports to the Audit Committee. Per the Audit Committee charter, the external auditor is accountable solely to, and reports directly to, the Audit Committee. The Audit Committee has the sole responsibility for selecting, evaluating	ELA7	Board minutes		
			XYZ has a formal Code of Business Conduct policy. The company has adopted a Code of Business Conduct (COBC) Policy which was approved by the Board of Directors on April 7, 2005, and is available on the company intranet. Each ne	ELA1	Code of Conduct		X
			The COBC policy addresses requirement to report suspected omission, falsification or inaccuracy of accounting and financial entries. The Code of Business Conduct section on Company Books and Records informs employees that they also agree to notify the Legal Department or Audit Committee of any concerns they may have regarding questionable accounting or auditing matters of the Company.	ELA8	Code of Conduct		

7	The Company not apply accounting principles correctly and fail to disclose important financial information.	Management has acceptable and clearly communicated policies reflecting their attitudes toward financial reporting. The financial reporting function has controls in place to ensure the appropriate selection of accounting policies.	XYZ's 10-Q and 10-K process includes disclosure of accounting pronouncements. Significant or new accounting statements and pronouncements are identified through the preparation of the 10-Q and 10-K. Outside legal counsel is consulted where appropriate	ELA9	10 K reviews	
			The Company has a formal disclosure committee. The disclosure committee meets in concert with the issuance of the 10-Q and 10-K to identify any reportable events or financial issues; both the VP-Internal Audit and the external auditors participate in th	ELA10	Disclosure committee minutes	
Information & Communication						
8	Management fails to obtain and disseminate relevant external information and internally generated information critical to the achievement of QuantRx Biomedical Corporation objectives. Ineffective communication exists between departments within the organi	The Board of Directors and management receive sufficient and timely information to allow them to fulfill their responsibilities, including operating results against budget.	Operating performance is communicated to Executive management and the Board on a quarterly basis. Internal Plan Variance reports are prepared and distributed quarterly to Executive management and annually to the Board. Variances against plan are identified and explained; key metrics are reported.	ELA11	Management reports	X
9	Material changes in the operations of the company may not be identified / disclosed in a timely manner.	Management has controls in place to monitor the results of the operations of the business units against objectives and expected results.	The CFO and Controller meets during the 10-Q and 10-K preparation process to identify any reportable events or financial issues. The external auditors are included when deemed necessary.	ELA10	Disclosure committee minutes	
Monitoring						
10	Management fails to obtain and disseminate relevant external information and internally generated information critical to the achievement of QuantRx Biomedical Corporation objectives. Ineffective communication exists between departments within the organi	The Board of Directors and management receive sufficient and timely information to allow them to fulfill their responsibilities, including operating results against budget.	Operating performance is communicated to Executive management and the Board on a quarterly basis. Internal Plan Variance reports are prepared and distributed quarterly to Executive management and annually to the Board. Variances against plan are identified and explained; key metrics are reported.	ELA11	Management reports	X
11	Material changes in the operations of the company may not be identified / disclosed in a timely manner.	Management has controls in place to monitor the results of the operations of the business units against objectives and expected results.	The CFO and Controller meets during the 10-Q and 10-K preparation process to identify any reportable events or financial issues. The external auditors are included when deemed necessary.	ELA10	Disclosure committee minutes	
Risk Assessment						
12	Material fraud activities may not be detected, investigated, or resolved timely.	Management has a process in place to identify and evaluate the risk of fraud that could result in significant financial statement misstatement.	Key management is required to sign a sub-certification letter on a quarterly basis. A two page disclosure questionnaire is forwarded to key Corporate and market area management in conjunction with the 10-Q process. The questionnaire requires the signee	ELA12	Quarterly certs	
13	Management may not identify and consider the implications of relevant risks at both entity and activity level and subsequently manage the risks. The risk process may fail to consider external and internal changes that could impact the achievement of fina	Management has an ongoing risk assessment process (formal or informal) that adequately addresses the effects of changing conditions on the organization.	XYZ Corporation Audit Committee Charter addresses the Committee's responsibility for risk management. The Audit Committee Charter requires that the Committee, periodically as deemed appropriate, discuss with management the Company's financial risk exposures and steps management has taken to monitor and control such exposures.	ELA13	Audit Committee charter	
14	Failure to assess both the internal and external business environment could expose the company to unplanned risk.	Management has a process in place to review and update the strategic plan which considers changes in the business, including the industry, competition, regulation and consumers.	XYZ Corporation has a strategic planning process in place. There is a process in place to periodically review and update entity-wide strategic plans. The strategic plan is reviewed and approved by QuantRx Biomedical Corporation Board of Directors.	ELA14	Board minutes	
Control Activities						
15	Inadequate staffing levels and expertise could result in financial statement errors, unauthorized access to financial and reporting systems and unauthorized transactions	Accounting is fully staffed and possesses the required expertise	Periodic reviews are made of Accounting Staffing levels and Accounting personnel have the proper background, expertise, supervision and training	Evidence of Accounting Staffing and Expertise Reviews		X
		Adequate IT Staffing levels and expertise exist	Periodic reviews are made of IT Staffing levels and IT personnel have the proper background, expertise, supervision and training	Evidence of IT Staffing and Expertise Reviews		X
16	Inadequate or non-existent policies and procedures could result in financial statement errors, unauthorized access to financial and reporting systems and unauthorized transactions	Necessary policies and procedures exist with respect to each of the entity's activities, and controls called for by policy are being applied.	Formalized IT Policies and Procedures exist in regard to change management, security and access controls	IT Policies		
			Policies and evidenced procedures in unplanned interruptions, back up procedures and help desk procedures.			
			Company's policies and procedures regarding disaster recovery are complete and up-to-date.			