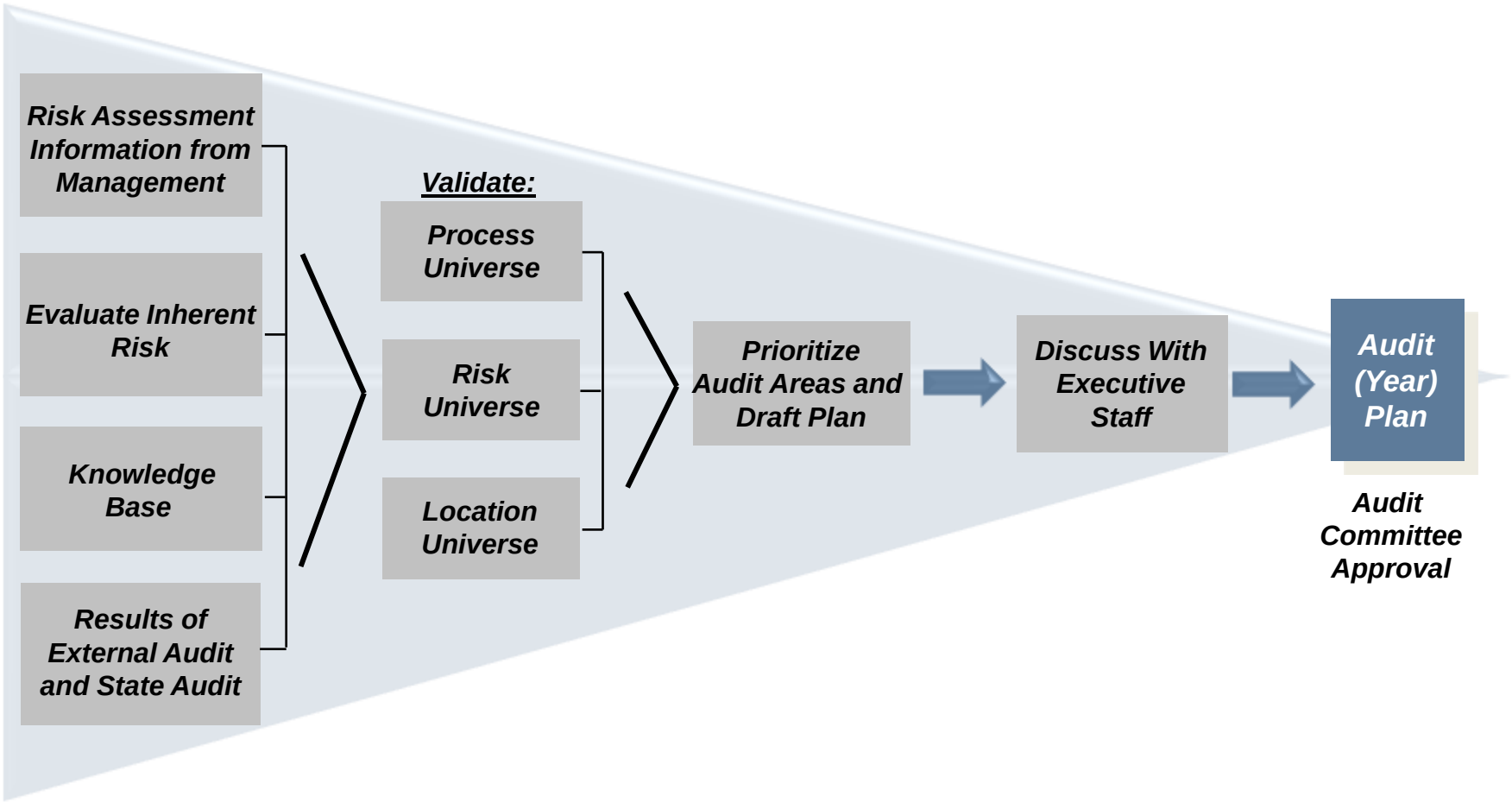
Internal Audit

Risk Assessment Report

Risk Assessment Process Overview

Internal Audit Plan Development Process



INPUT → ***Planning Process*** → ***OUTPUT***

Source: www.summitcl.com

Risk Assessment Process Overview

A risk assessment was conducted with the assistance of Company X management to identify perceived areas of risk and potential internal audit projects. The following procedures were performed:

- Conducted interviews with members of Company X management to identify and gain an understanding of areas of perceived risk.
- Identified and defined risks/areas of concern potentially preventing Company X from achieving its business objectives and strategic vision.
- Used risk model to evaluate inherent risk applicability and significance to Company X .
- Leveraged knowledge obtained from other engagements.
- Considered results of the report from the Office of the State Auditor and the (Year) external auditor management letter.
- Created an Auditable Process Universe that identifies the primary business processes within the company.
- Surveyed management regarding # business processes/risk areas where potential risks were identified during the interviews. Management numerically ranked the top # processes, providing an explanation for the top # processes.
- Analyzed information obtained through the risk assessment process to create a Company X Risk Prioritization Map.
- Validated the Prioritization Map with key senior management members.
- Collaborated with senior management to define the (Year) internal audit plan based on the risk assessment process.

The following pages contain the Interviewee List, Auditable Process Universe, Risk Areas for the Company and the Risk Prioritization Map.

Source: www.summitcl.com

Risk Assessment Information Source

The following is a list of the members of management who were interviewed and/or who were asked to complete the risk assessment survey:

- Audit Committee Chair
- President and Chief Executive Officer
- Chief Financial Officer
- Sr VP, Strategic Planning
- Acting VP, Human Resources
- Chief Investment Officer
- Interim VP Development, (Location)
- Associate VP and General Counsel
- VP, Controller
- President and CEO, (Location)
- VP, Human Resources
- VP, Campaigns
- VP, Development Services
- Associate VP Development, (Location)
- VP Development, (Location)
- Portfolio Managers (2)
- Director Project Management
- Director of Development
- Manager, Donor Relations
- Assistant Controller and Controller (Location)

Source: www.summitcl.com

Auditable Process Universe

The following Auditable Processes Universe for Company X was determined based on discussions with management and industry-specific guidance (may not be all-inclusive):

Executive Management	Development	Investments
• Organizational strategy • Strategic planning • Major campaign • Mission/vision/values • Organizational structure	• Prospect cultivation • Donor relations • Annual fundraising • Gift planning	• Investment due diligence and selection • Asset allocation • Investment valuation • Portfolio management and performance monitoring • Investment transactions and settlement
Development Services	**Management Information Systems**	**Alumni Association**
• Gift/records processing • Donor prospect identification and research • Donor relations (service after the sale) • Project management • Technical training	• Information technology strategy/planning • Systems implementation • IT project management • Systems maintenance • Business continuity/disaster recovery planning • IT asset management • Network administration security/privacy	• Membership • Travel program • Event planning and administration

Source: www.summitcl.com

Auditable Process Universe (Continued)

Finance and Accounting	Human Resources and Payroll	Legal
• Accounts receivable • Accounts payable • Financial close • Financial statement preparation and reporting • 501(c)(3) requirements • Fixed asset/lease accounting • Loans • Facilities management • Travel and expense reporting • Treasury/cash management	• Recruiting/hiring • Compensation and benefits • Performance reviews • Employee relations • Termination • File retention • Orientation/training and development • Time entry • Payroll processing (outsourced) • Policies and procedures	• Contract and lease administration • Litigation management • Corporate compliance • Insurance/risk management • Gift acceptance/due diligence • Development services agreement/operating agreement compliance

The Auditable Process Universe was categorized into general and specific risk areas, as defined and illustrated on the following pages.

Source: www.summitcl.com

General Risk Area Definitions

General Risk Areas	*Risk Area Definition*
Reputation/ Perception	*How the company is viewed in the eyes of the general public*
Financial	*Accuracy of financial reporting, financial sustainability and viability of the organization, and safeguarding of financial assets*
Operational	*Effectiveness in achieving organizational goals and objectives; efficiency of operations*
Compliance	*Compliance with internal policies and procedures and external laws/regulations*

Source: www.summitcl.com

General and Specific Risk Areas

General Risk Areas	*Specific Risk Areas* *(Not in any particular order)*	
Reputation/ Perception	• Gift processing/transfer (donor intent) • Reputation/public relations • Tone at the top • Company partnership	
Financial	• Liquidity • Financial close and reporting • Investment measurement • Investment performance • Cash and receivables	• Affiliate loan programs • Accounts payable • Travel and entertainment
Operational	• System access/IT security • Facilities management • Gift acceptance • Legal and risk management • Business continuity • IT system strategy • Configuration	• IT asset management • Planned giving • Major campaigns • Donor relations • Payroll/benefits • Human resources
Compliance	• Operating agreement/development services agreement • External regulatory compliance • Human resources/employment regulations	

Source: www.summitcl.com

Specific Risk Areas/Embedded Risk Definitions

Reputation/Perception Risk Areas	"What Can Go Wrong" (Sample)
Gift Processing/Transfer (Donor Intent)	Inaccurate processing of gifts, leading to donor intent non-compliance, untimely processing of gifts, incorrect allocation of gifts to company, excessive callable funds that aren't used by the company, company expenditure of gifts outside of donor's intent
Reputation and Public Relations	Adverse press or other events leading to a reputation erosion, poor public/donor base perception of the company, inadequate management of company reputation (intentional or unintentional)
Organizational Culture/"Tone at the Top"	Strategic company goals and objectives are undefined or unclear, employee behaviors are not aligned with organizational principles, unclear or undefined delineation of authority, management is not aware of unethical acts by employees.
Company Partnership	The company decides that the foundation's benefit to the company does not justify the cost to the company, lack of trust by the company

Source: www.summitcl.com

Specific Risk Areas/Embedded Risk Definitions

Financial Risk Areas	"What Can Go Wrong" (Sample)
Liquidity	Inability to operate the business due to insufficient funds, inability to convert assets (e.g., investment securities, receivables, inventories) to an equivalent cash value, or to raise unsecured funding in a timely and cost-effective manner
Financial Closing/Reporting	Unauthorized or inaccurate accounting entries are made, inaccurate financial statements, inefficient financial closing process, operational decisions are made based on inaccurate, insufficient or untimely financial information
(Location)	Failure to maintain required debt service ratio leading to potential adverse impact on company's bond rating, excessive use of unrestricted net assets to maintain required ratio, asset impairment/write-down, inaccurate or incomplete decision regarding hold vs. dispose-of property, failure to receive revenue/income due to property management fraud or other mismanagement
Investment Portfolio Measurement and Certification	Incorrect valuation of alternative investments, qualified audit opinion resulting from alternative investment valuation considerations.
Investment Performance	Investment strategy/asset allocation is not congruent with the company's strategy, inadequate investment decision due diligence, failure to adequately monitor investment performance, fraud on the part of investment managers, leakage at points of transfer between company and custodian, decreased funding due to market downturn and reduction in associated fees

Source: www.summitcl.com

Specific Risk Areas/Embedded Risk Definitions

Financial Risk Areas - Continued	"What Can Go Wrong" (Sample)
Cash and Accounts Receivable	Improper processing of checks payable to company, inefficient processing of cash receipts, misappropriation of cash receipts, failure to adequately monitor/follow up on receivables
Affiliate Loan Programs	Non-compliance with existing policies and procedures, credit exposure due to inadequate due diligence prior to extending loans, untimely or inaccurate processing of loan payments, inadequate or missing loan contractual documents
Accounts Payable	Fraudulent disbursements, duplicate payments, payments to inappropriate vendors, timely payment discounts not taken, vendor credits not applied
Travel and Entertainment	Personal/fraudulent expenses are paid by the company, expenses are excessive and not congruent with company philosophies, or otherwise subject the company to adverse perception or embarrassment

Source: www.summitcl.com

Specific Risk Areas/Embedded Risk Definitions

Operational Risk Areas	"What Can Go Wrong" (Sample)
IT Security and System Access	Access to systems may not be restricted or updated appropriately, security of servers may not exist, compromise of data integrity may occur, critical systems are not available due to outage, virus, etc.
Facilities Management	Inefficient use of building facilities, inadequate building maintenance and/or physical security, excessive costs associated with facilities and related services
Donor Gift Acceptance	Acceptance of impaired or encumbered gifts from donors, gifts in which the costs (financial or otherwise) outweigh the benefit
Legal and Risk Management	Failure to maintain adequate insurance coverage, the company is not aware of potential exposures related to events, inadequate management of litigation in which the company is a party
Business Continuity/Disaster Recovery	Lack of knowledge transfer due to excessive dependence on informal procedures/tribal knowledge, critical data is not recoverable in the event of a disaster or other loss, critical business functions cannot efficiently resume in the event of a disaster
IT System Strategy and Configuration	IT infrastructure is not adequate to support the needs of the company, cost of implementation may not be evaluated for appropriate return on investment, selection criteria for new systems may not be defined, internal controls may not be in place after implementation
IT Asset Management	IT asset misuse or loss, software license non-compliance, inefficiencies resulting from a failure to effectively manage IT asset lifecycle

Source: www.summitcl.com

Specific Risk Areas/Embedded Risk Definitions

Operational Risk Areas - Continued	"What Can Go Wrong" (Sample)
Major Campaigns and Planned Giving	Undefined campaign goals and objectives, failed major campaign due to inadequate planning or insufficient resource allocation, "feast or famine" resulting from improper gift planning
Donor Relations	Failure to identify viable donor prospects; cultivation processes do not result in prospects being converted into donors, poor service results in annual donors not being retained
Payroll and Benefits	Inaccurate or inappropriate payments to employees, fictitious employees are on the payroll, inaccurate payroll information is reported to finance and accounting, incorrect tax/benefits withholdings, employee benefit packages are not competitive
Human Resource Operations	Formal policy/procedures may not be in place and/or may not be adhered to, insufficient processes to effectively recruit, select, hire/orient, train, evaluate and separate employees, higher turnover or other inefficiencies due to the lack of a comprehensive staffing model/strategy

Source: www.summitcl.com

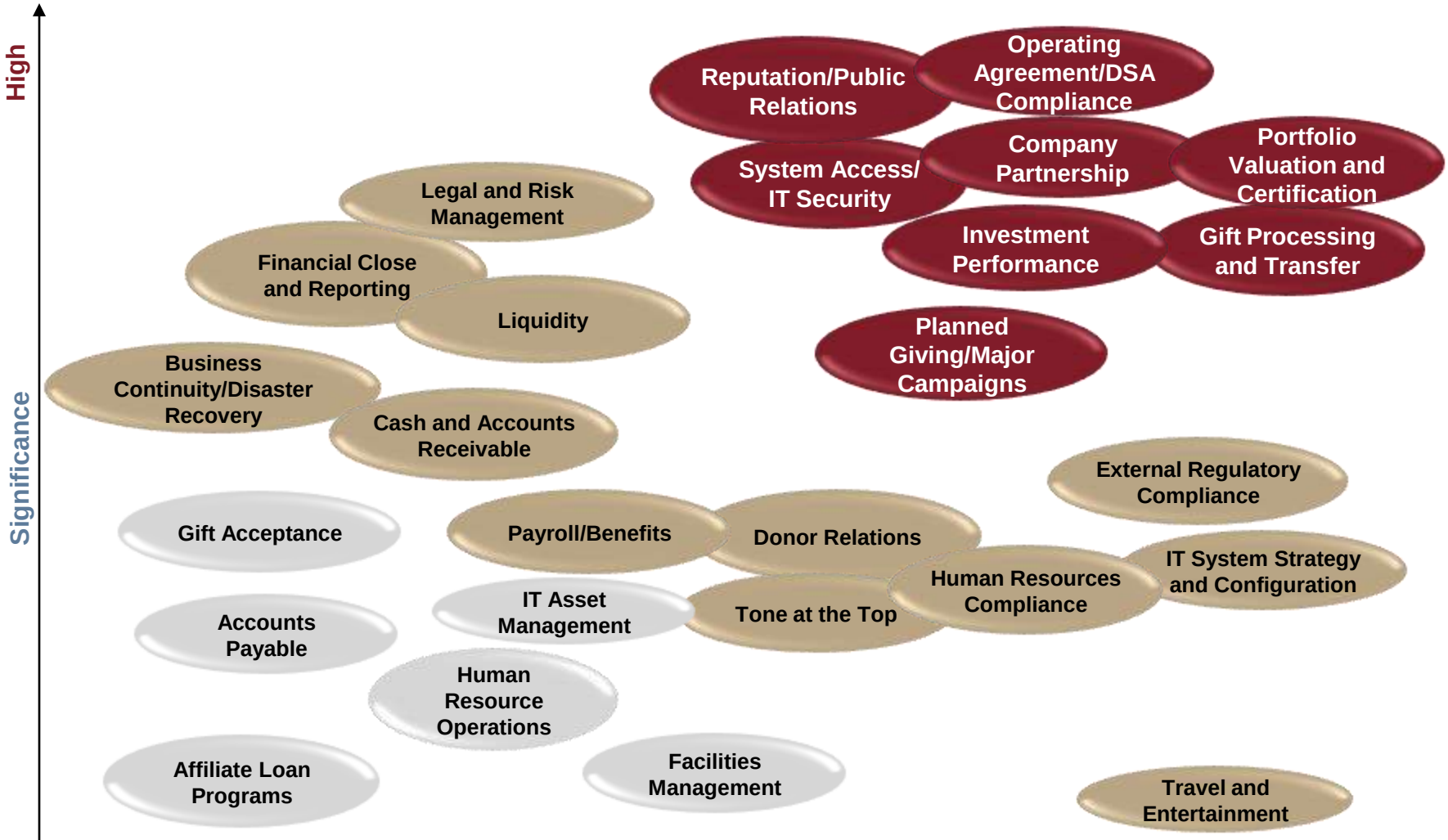
Specific Risk Areas/Embedded Risk Definitions

Compliance Risk Areas	"What Can Go Wrong" (Sample)
Development Services Agreement/Operating Agreement	Process-level policy/procedures do not support compliance with agreements, failure to meet specific performance metrics/criteria in the agreements, inadequate oversight and accountability for agreement compliance
External Regulatory Compliance	Adverse findings resulting from audits, inaccurate filing of IRS form 990, failure to identify and/or properly report unexpected income, tax inaccuracies resulting from Life Income Arrangements, inaccurate 1099s or related non-compliance, non-compliance with payroll/benefit tax requirements, loss of tax-exempt status
Human Resources/Employment Regulations	Non-compliance with EEOC, HIPPA, FCRA and other relevant regulations regarding employment practices/employee privacy, etc.

The Risk Assessment Survey results were combined with other portions of the risk assessment process to prioritize these risks based on perceived likelihood of occurrence and perceived significance of impact, resulting in the Company X Risk Prioritization Map on the following page.

Source: www.summitcl.com

Risk Prioritization Map



Source: www.summitcl.com

Potential (Year) Internal Audit Projects

The following table provides potential internal audit projects for the upcoming year, based on the Risk Assessment Process and Risk Prioritization Map.

Project Description	Estimated Hours*
Audit Committee Reporting and Follow Up on Prior Findings/Action Plans (# Quarters @ # Hours per Quarter)	# Hours
Development Services Agreement/Operating Agreement Contract Compliance • Accuracy/use of performance evaluation metrics defined in/required by DSA • Compliance with other DSA/Operating Agreement terms and conditions	# - # Hours
Investment Policies and Practices • Authorization for transactions/policies and procedures • Investment valuation • Investment allocation and performance monitoring	# - # Hours
Information Security and Privacy • IT system security and protection of data from persons external to company • Data encryption • Privacy policy/practices for sharing customer information with affiliates	# - # Hours
Cash/Pledge Receivables • Controls around cash receipts/segregation of duties • Processes and controls to process/record new donor pledges • Processes and controls around monitoring/follow up and collection of outstanding donor pledges • Valuation of pledge receivable assets (e.g., provision for pledges that may not be collected)	# - # Hours
IFAS General Controls Review • System access controls/roles and responsibilities (segregation of duties) • Input/data integrity controls • Data backup and recovery • Support management	# - # Hours

* *Hours are subject to change based on detailed audit planning and final scope determination*

Source: www.summitcl.com

Potential (Year) Internal Audit Projects

Project Description	Estimated Hours*
Company Gift Expenditures (Collaborate with Company Internal Audit Department) • Processes and controls around company expenditure of gift funds • Authorization for and documentation of expenditure transactions	# - # Hours
Cash/Pledge Receivables • Controls around cash receipts/segregation of duties • Processes and controls to process/record new donor pledges • Processes and controls around monitoring/follow up and collection of outstanding donor pledges • Valuation of pledge receivable assets (e.g., provision for pledges that may not be collected)	# - # Hours
Human Resources/Payroll • Pre-employment due diligence practices (background/credit checks, etc) • Employee privacy/HIPPA compliance controls • Employee performance evaluations • Processes and controls around payroll processing (segregation of duties, review and approval) • Analytical review of payroll data (e.g., excessive overtime)	# - # Hours
IT Asset Management • Processes to manage IT assets from procurement to retirement • Processes and controls to monitor compliance with licensing and vendor agreements • Processes to measure system problems, performance, availability, responsiveness, etc.	# - # Hours
Accounts Payable • Payables analysis using Spend Risk Assessor – overall spend summary, analysis for possible duplicate payments, comparison of vendor payment terms to actual payment, discount analysis, etc. • Roles and responsibilities/segregation of duties	# - # Hours
IT Outsource Contract Review (xxx) • Compliance with contract terms and conditions, including any performance standards/evaluation metrics	# - # Hours

* *Hours are subject to change based on detailed audit planning and final scope determination*

Source: www.summitcl.com