ITS Supplier Management Policy

Document Number: ITS-0025 **Date Published(sys):** 4/27/2022

General Description

Policy Summary:

Trinity University is committed to a secure information technology environment in support of its mission[1] and is dedicated to protecting the integrity of the competitive selection processes for the procurement of goods and services.

All contractor and supplier selection processes shall promote fair and open competition and shall be conducted in accordance with University Regulations and Texas Statutes. All contractor and supplier selection processes shall be free of conflict of interest, undue influence, and favoritism so that contracts are awarded equitably and economically. Information Technology Services will provide management and oversight over the procurement of technology related commodities and contractual services, working together Trinity Procurement Offices, Risk Management and Security organization.

No staff member or manager can sign a legal agreement (contract) unless they have the required authority (refer to *RISK-0007 Contract Policy and Procedures*) and subject to the consultative and/or approval requirements set out in this Policy and related Procedures.

Within this Policy, the terms “Trinity University” & “Trinity” may be used interchangeably.

[1] https://www.trinity.edu/about/mission-values

Purpose:

This policy is designed to provide the University with a documented and formalized process regarding managing the risk associated with legal agreements and provide clear direction to staff responsible for establishing and managing Technology Contracts with third parties.

Trinity relies on technology products, systems and services provided by a variety of vendors, including hardware and software vendors, consulting firms, technology and telecommunication services, and support personnel. It is ultimately the duty of management to ensure:

- Each vendor relationship supports the overall business requirements and strategic plans.
- The business or functional leader has sufficient expertise to oversee and manage the relationship.
- The business or functional leader has evaluated prospective vendors based on the scope and criticality of the procured service and products.
- The risks associated with the use of the vendor are fully assessed and understood.
- The appropriate oversight program is in place to monitor contractual performance and risk mitigation activities.

The ITS contract management and its technology and supplier selection processes shall be free from conflict of interest and undue influence, including any direct fund-raising solicitations by a competitive selection committee or its members. Official development / fundraising activities should be kept separate from contractor and vendor selection processes.

Competitive solicitations for the procurement of Technology, Technology services and related professional services (Consulting, Licensing, etc.) are based only upon qualifications of the firms responding, and competitive selection committees shall determine and select the most qualified firm(s).

Additionally, compliance with the stated policy and supporting procedures helps ensure the confidentiality, integrity, and availability (CIA) of University's system components.

Scope:

This Policy applies to all University employees responsible for negotiating or executing contracts for third party technology vendors on behalf of Trinity.

This policy and supporting procedures applicable to all system components that are owned, operated, maintained, and controlled by the University and all other system components, both internally and externally, that interact with these systems. All University-Related Persons with access to University Information or computers and systems operated or maintained on behalf of the University are responsible for adhering to this policy

- Internal system components are those owned, operated, maintained, and controlled by Trinity University and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and the underlying application(s) that reside on them) and any other system components deemed in scope.
- External system components are those owned, operated, maintained, and controlled by any entity other than Trinity University, but for which such external resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the description of "Internal system components".

- Trinity applications and systems must be configured to conform as closely as possible to these requirements within the Trinity systems or application's capabilities. For those systems or applications that do not have the capability of enforcing the security controls mentioned in this policy, an exception must be documented with by written permission from the authorized personnel.

Exceptions:

In few instances, Trinity systems may require to be exempted from the Supplier Management Processes due to possible technical difficulties or third-party contractual obligations. Any such exceptions to the current policy must be documented and approved via the Trinity's Exceptions Management Process.

Policy Content

Roles and Responsibilities

Implementing and adhering to organizational policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including management, internal employees, and users of system components, along with vendors, contractors, and other relevant third parties. Additionally, by being aware of one's roles and responsibilities as it pertains to Trinity University information systems, all relevant parties are helping promote the Confidentiality, Integrity, and Availability (CIA) principles for information security in today's world of growing cybersecurity challenges.

ROLES	RESPONSIBILITIES
Management Commitment	Responsibilities include providing overall direction, guidance, leadership, and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The Chief Information Officer CIO is to report to other members of senior management on a regular basis regarding all aspects of the organization's information systems posture.
Internal Employees, Academic Community and Users	Responsibilities include adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any Trinity University system components. Additionally, end users are to report instances of non-compliance to senior authorities, specifically those by other users. End users – while undertaking day-to-day operations – may also notice issues that could impede the safety and security of Trinity system components and are to also report such instance immediately to senior authorities.
Vendors, Contractors, another	Responsibilities for such individuals and organizations

Workforce	are much like those stated for end users: adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such system components.
ITS Business Affairs Unit	Responsible for ensuring that the ITS sourcing strategy is aligned to University objectives. Evaluate classifications for existing suppliers annually with support from Contract Owners. prepare multiple reports based on CIO needs in order to monitor overall ITS TU Technology performance
Contract Managers	Manage the vendor relationship. Evaluate vendor's product and services, negotiate pricing and contract terms with support of ITS respective groups, in line with established policies and procedures. Are responsible for identifying, assessing, and mitigating risk activities; and implementing controls consistent with University's Practices.
ITS Managers	Support Contract Managers with the selection and evaluation of technology and during discussions with vendors if required.
Information Security	Assists in supporting supplier risk management by completing the Data Security Assessment and Security Analysis Questionnaire for compliance with ITS security requirements.
Risk Management	Assists in supporting the supplier risk management by ensure compliance with internal policies / external regulations.

Policy

Trinity is to ensure that all applicable users adhere to the following policy for purposes of complying with the mandated organizational security requirements set forth and approved by management.

Technology Suppliers Rationalization

The Supplier based consolidation is a reduction in the number of suppliers. By achieving rationalization, especially in IT sectors due to the many and fast changes in technology, ITS achieves many benefits for the university specifically in the areas of;

- Cost Reductions:
  - Price Decreases through Consolidated Purchases and Increased Negotiating Power
- Supplier Development:
  - Lead Time reductions
  - Quality Improvements

- Supplier Design Support
- Inventory Reductions

To achieve a successful Supplier Rationalization plan there are a series of steps required by ITS involving;

- Evaluation of Current Supply Base
  - ITS determine the Number of Suppliers and break them down by Commodity. Skills should be evaluated as well as their performance within the university.
- Determine the Type of Supply Base Needed
  - Look for suppliers that are Fast and Flexible, that take advantage of innovation and are good communicators.
- Classify Suppliers by criticality
- Plan the Project
  - Plan with your internal customers in mind. Do not forget of Transaction costs and leverage on opportunities.
  - Design support needed to succeed with the supplier that will stay providing the University technology needs.

For the strategy to success a set of key meaningful measures should be defined and implemented. It is important to stay focus on the efforts and Communicate / Publish successes.

Technology Supplier Classification

The supplier criticality is viewed as how important the product or service is to the day-to-day operations of Trinity University. Classifying vendors by criticality is an important step of the ITS supplier risk management program. Specifically:

Strategic: Strategic supplier are those that account for a considerable amount of business (60-80%), demonstrate loyalty to their partners (exclusivity, limited distribution), are easy to do business with, and provide both growth and profitability.

Operational: Operational supplier are those that provide services to the University, managing the inner workings of our business so it runs as efficiently as possible. Whether the supplier provides products or services, the business unit owner must oversee and closely monitor the supplier relationship.

Tactical: These suppliers are important, but minimally impactful in comparison to strategic or operational vendors. Potentially high in spend, but short in duration.

Commodity: Non-critical to University operations, where if a break in the supply chain occurred, there would be little or no consequences to maintaining service levels and

customer service.

The criticality for new suppliers being on-boarded will be determined by the contracting party. All classifications for existing suppliers will be annually assessed by the ITS Business Affairs Unit with support from the contracting organization or Contract Manager.

Technology Supplier Risk Management

ITS Supplier Risk Management is the process of managing risks associated with third party vendors. It's important to understand these risks, what they are, and how ITS can readily identify any issues, concerns, or constraints pertaining to these risks. Failure to mitigate and prevent these risks can result in significant financial loss, reputational damage, and/or legal/regulatory issues.

The following risks are to be assessed regarding contractual relationships entered with suppliers:

Strategic Risk: Risk of failing to implement or achieve planned business goals, objectives, or initiatives. Inability to address the fundamentals required to execute the agreed strategy, as evidenced by deviations from business plans.

Compliance Risk: Risks arising from violations of applicable laws, rules, regulatory mandates, and along with other issues, such as non-compliance of operational, and information security policies, procedures, and processes.

Operational Risk: Risks from a failed system of operational internal controls relating to relevant policies, procedures, and practices. Specifically, failures associated with processes, systems, or people.

Financial Risk: Risks related to the financial condition of the third-party vendors, such as any "going concern" issues, or a vendor under the threat of liquidation in the foreseeable future.

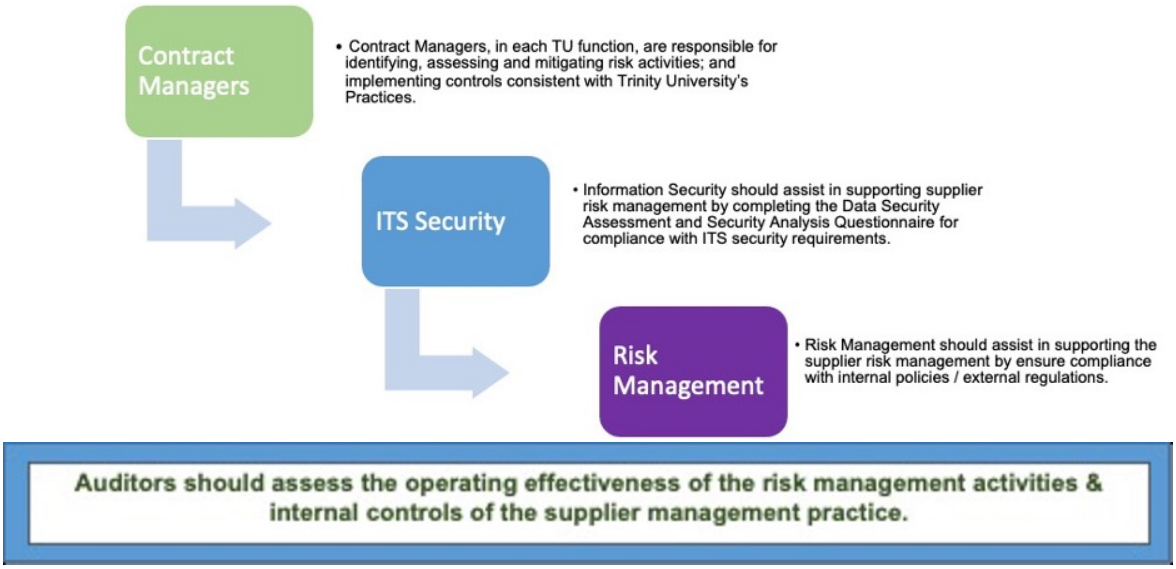
Reputation Risk: Risks of negative public perception and opinion, such as unethical business practices, data breaches resulting in loss of sensitive and confidential consumer information.

Technology Risk: Risks from any number of information technology and information governance and security issues, including inadequate resources (hardware, software, or manpower).

Country Risk: Risks arising from the political, economic, and social landscape and other relevant events within a foreign country that can impact the services provided by vendors, ultimately affecting Trinity University operations.

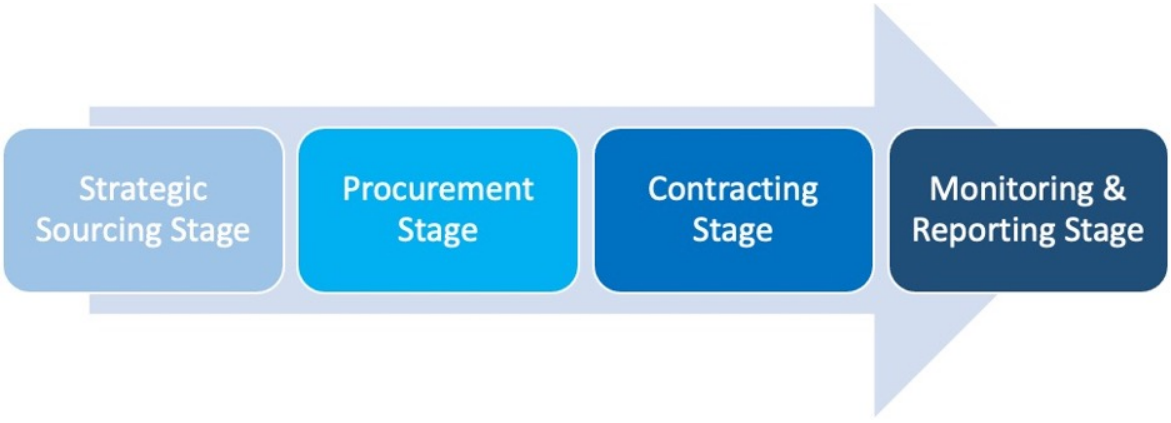
Environmental, Social and Governance Risk: Risks related to climate change impacts, environmental practices, and duty of care, working and safety condition, respect for human rights, and compliance with laws and regulations.

The risk should be assessed and mitigated during the stages of the Technology and Supplier Selection process;



Supplier Management Practice

TU ITS Technology Supplier Management lifecycle:



Strategic Sourcing Stage

The ITS Business Affairs Unit is responsible for ensuring that the ITS sourcing strategy is aligned to University objectives. To create a synergy between ITS and

its Suppliers, team should reinforce the focus on the supplier's core capabilities, seek to build long-term relationships with them, and must select the right supplier for the right sourcing objective. The objectives are to:

- Maximize the value of the vendor spend and reduce cost.
- Streamline the procurement process.
- Obtain an expert understanding of our suppliers and the supplier market.
- Build strong, trustworthy relationships with existing and new suppliers.
- Ensure supplier relationships comply with all internal policies and external laws and regulations.

Strategic sourcing is decentralized within the University business and functional areas.

The Procurement Stage

The procurement stage is where the initial relationship with many vendors begins. The representative(s) leading this stage is referred to the 'Contract Manager'. If the Contract Manager is not from ITS, then he / she needs to work together with their ITS counterpart to ensure that all technology decisions are aligned with ITS organization strategy based on currently defined university technology landscape and architecture platforms.

The Contract Manager needs to follow the next steps or phases:

The Acquisition Planning

The effective acquisition of needed commodities begins with proper planning. The Contract Manager / Requesting Area should define needs, prior to the procurement process, to determine the exact requirements for a commodity. Contract Manager / Requesting Area should determine:

- The commodity and quantity needed,
- Quality level,
- Delivery location, and
- Time frame in which the commodity is needed.

In addition, the Contract Manager should consider the following:

- All parties directly or indirectly involved with the vendor or use the contracted services.
- The subsequent supporting steps to facilitate the solicitation, due diligence, and selection

- The documentation needed to ensure that the service or products procured meet Trinity University's requirements.
- Any technical expertise required to complete the procuring and on-boarding process.

Solicitation

This is the process of notifying qualified vendors that the University wishes to receive proposals on the specified products or services. All solicitation documents should contain instructions to ensure the vendors submit an adequate response and ensure the process to collect and evaluate bids is consistent. Contract Manager should include the following:

- Description of the objectives, scope, and nature of the work to be performed,
- Expected service levels,
- Key performance indicators (KPI's) to be measured against,
- Delivery timelines,
- Change controls,
- Financial penalties around poor service,
- A schedule including any fees,
- The selection criteria and
- The procedures for requesting additional information.

Is recommended for the Contract Manager to gather competitive bids from at least 3 sources to mitigate the risk of potential or perceived conflicts of interest.

Supplier Selection

To establish a successful supplier relationship, the process should contemplate the following, regarding the vendor;

- Existence and corporate history. Vendor's business history and market share for a given service.
- Qualifications, backgrounds, and reputations of company principals, including criminal background checks where appropriate.
- Vendor's reputation and past performance with similar business partners.
- Financial Condition: Obtain the audited financial statements for review by Corporate Finance (during their Vendor Validation process).
- Reputation.

    - Review year-end financial statements for litigation disclosures, past and any pending litigation.
- Internal control environment.
    - Consider reviewing audit reports, internal control evaluations and assessments of the third parties. If applicable obtain their most recent Statement on Standards for Attestation Engagements (SSAE) report.
- Legal and compliance including any regulatory actions and/or anti-bribery corruption risk.
- Reliance on and success in dealing with third party service providers.
- Insurance coverage.
    - Ensure that the vendor has sufficient coverage to insure against losses due to dishonest acts, and liability coverage for losses due to negligent acts in an amount of the potential exposure to risk.
- Ability to meet disaster recovery and business continuity requirements.

Steps to initiate the supplier selection process are detailed on the *Tech Supplier Selection procedure*.

Once a potential supplier has been pre-selected, the Contract Manager will complete the *Technology Acquisition Form*, which includes their Supplier recommendation and business case. It is recommended to include a copy of the most competitive bids/quotes of Suppliers participating to add transparency to the process. Contract Manager will follow the steps detailed on the *Technology Acquisition Procedure*.

Budget Validation

Once the possible supplier is selected, organization needs to make sure that the appropriate budget amount is available or allocated to support the contracting relation.

Contract Manager needs to ensure that all individuals involved on the approval process are aware of their Authorized approval limits (CAPEX and OPEX) established by Trinity University and documented on the *BUSO-0031 Purchasing Policy and Procedures*.

Security and Risk Management Assessments Stage

A due diligence must be performed on the likely selected supplier. The depth of the due diligence may vary according to the relative importance of the supplier relationship, but it should cover the following areas, as

described in detail on the *TU ITS Security and Risk Assessment Intake Form*;

- **Security Assessment**: The type of security surveys completed will be driven by criticality and the inherent risk for the university. The evaluation of security risk will align to financial, operational, compliance/legal, strategic and information security risk factors. Criticality will also be the driver.
    - If University data is accessible by, shared with, or stored by an Outside Party, request that the Outside Party submit a SOC 2 Report and complete the Higher Education Community Vendor Assessment Toolkit (HECVAT) for ITS review.
        - If University data is accessible by, shared with, or stored by an Outside Party request that the Outside Party sign Trinity's Confidentiality Agreement.
    - If the contract involves non-public information, Supplier will be required to complete a HECVAT questionnaire and / or a SIG Questionnaire.
        - If it is a renewal and includes handling new non-public information, the Supplier only needs to update its most recent questionnaire copy on file.
    - If the contract is for a SaaS (Software as a Service) or Cloud Service, the supplier will be required to complete a SOC2 Report for Cloud Services.
- **Risk Management Assessment**: A pre-contract risk assessment will be completed by the University Risk Management Organization, leveraging the information collected from the proposal, and due diligence. Please refer to the *RISK-0007 Contract Policy and Procedures* for more detail information

Supplier Selection Communication

The vendor that can best meet the University's technology business needs, operational requirements and has completed necessary due diligence is notified of the final selection.

Contracting Stage

The contracting stage is the management of the University contracts from contract initiation, negotiation, execution, and the administration of the agreements. The vendor contract translates policies and expectations into specific enforceable terms and conditions to ensure compliance, while maximizing performance and reducing risk. The contracts between the University and its vendors must clearly specify in a level of detail commensurate with the scope and risks of the service provided all relevant terms, conditions, responsibilities, and liabilities of both parties.

Contract Manager will follow the steps detailed on the *Technology Acquisition Procedure* when is time to proceed with the actual generation of the Purchase Order.

Selecting Contract format or Template:

- Trinity has developed Contract Templates that should be used whenever possible when entering into a contract with an outside party. Please refer to the *RISK-0007 Contract Policy and Procedures* to get access to those templates, based on the type of contract.
- If the university's templates are used, and no changes are made to the contract language, then no review by Risk Management and Insurance Organization is necessary, expediting the process. These templates contain the necessary language to protect and minimize the risk exposure of the University and of employees entering into the contract if no changes are made.

Contract Administration:

- **Contract Storage and Records Management**: All Technology Contracts and related documentation must be kept and stored by the Risk Management and Insurance Organization. ITS Business Affairs Unit will keep an electronic version stored on their centralized files. Contracts will be accessible only to those with a business need. The contracts will be maintained in a central repository in accordance with the Risk Management and Insurance Organization's record management retention policy to ensure compliance with regulatory document retention requirements. Please refer to the *RISK-0007 Contract Policy and Procedures* for more detail information.
- **New Contractual Agreements**: The first review of all contracts, whether on established University Contract Templates or on an Outside Party's contract, should be conducted by the department or individual entering into the contract (Contract Manager). Often contracts are department or technology specific and only the Contract Manager responsible for the negotiations with the Supplier will know if the terms and details of the contract are as agreed upon. Please refer to the *RISK-0007 Contract Policy and Procedures* for details.
- **Expiry, Modify, and Renew**: Contracts approaching their expiration date will be flagged for review 6 months in advance the notice period to amend, modify, extend, or renew the original agreement. It is the responsibility of the Contract Manager to complete any due diligence and/or vendor risk assessment prior to renewal. If the contract is not modified, extended, or renewed before the expiration date, the

contracting process is repeated. Please refer to the *RISK-0007 Contract Policy and Procedures* for more detail information.

- **Termination**: Termination may be required when a contract expires, the terms of the contract have been satisfied, in response to contract default, or due to changes in business strategy. In the event of planned or eminent termination, the contract sponsor should consider the following:
    - Capabilities, cost, resources, and time frame to transition the activity.
    - Risks associated with data retention and destruction, Information System IS connections, access controls or other transition issues.
    - Handling of any joint Intellectual Property rights developed during the relationship.
    - Any possible reputational risk arising from contract disputes or performance issues.

Monitoring and Reporting Stage

A key component of the ITS Supplier Management Practice is the ongoing monitoring of vendor spend, performance and risk.

Spending

The following is not an exhaustive list, but the basic types of spending analysis to be provided by the ITS Business Affair Unit in collaboration with the Contract Manager are;

- Totals spend by vendor
- Spend by category
- Totals spend v. budget
- Spend for vendors (contract/no contract)
- Spending by ITS Cost Center, or ITS Budgets
- Spend by vendor type

Spend analysis benefits include:

- Advance data-driven strategic sourcing
- Full visibility of spend
- Identify cost savings opportunities
- Align and streamline procurement process
- Manage vendor risk and “rogue” spending
- Enhance vendor performance
- Improve vendor relationship management
- Leverage spend data across business units

Performance

Contract Manager is responsible to monitor performance of the supplier contracted against expectations as delineated on the signed agreement. The scope should include the following:

- Vendor Relationship Oversight
- Service Level Agreements
- Quality of Services
- Contract Terms
- Billings and Disbursements

Reporting

Should be expected that the ITS Business Affairs Unit will prepare multiple reports based on CIO needs in order to monitor overall ITS TU Technology performance.

Performance Evaluation

Consequences of Policy Violation:

Any behavior in violation of this policy is cause for disciplinary action and violations of this policy may result in, but are not limited to, any or all the following:

- Loss of university computing, email and/or voice mail privileges.
- Disconnection from the residential hall internet network.
- University judicial sanctions as prescribed by the student code of conduct.
- Reassignment or removal from university housing and/or suspension or expulsion from the university.
- Prosecution under applicable civil or criminal laws.

Violations will be adjudicated, as appropriate, by the CIO, the Office of the Dean of Students, the Office of Housing and Residential Life, and/or the Office of Human Resources.

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Bid	A competitive offer received from a seller or vendor.
Bidding	The process of soliciting prices and any other considerations for goods and

Term:	Definition:
	services from qualified vendors. The solicitation of prices from more than one vendor constitutes competitive bidding. Bids may be solicited in an informal manner by telephone, facsimile, internet, mail, or through a formal sealed bid process.
Buyer	Person who performs the purchasing.
CAPEX	Capital Expenditure
Commodities	Supplies, materials, equipment, furniture, contractual services, and any other goods required by the University.
Contract	Legal agreement between Trinity University and a vendor or supplier
Emergency	An unexpected situation or sudden occurrence of a serious and urgent nature that demands immediate action, otherwise, it would endanger life, property or adversely affect essential University operations.
Invoice	An itemized bill for goods purchased or services contracted, containing individual prices, the total charge and payment terms.
OPEX	Operating Expenditure
Packing or Delivery Slip	Proof of delivery from vendor
Performance Specification	Based upon the specific needs. Total ownership cost for operating and maintaining the product should be included as an element of the specification.
Purchase	Acquiring a commodity in exchange of money or other valuable consideration. The basic types of purchases that can be made may include but are not limited to: • The purchase of commodities or services on a one-time basis each year. • The direct purchase of commodity or service that is available from only one source. • Contracts used to obtain commodities or specific professional, technical, or other specialized services throughout the year.
Purchase Order	Form, generated by the Procurement unit that documents the purchase agreement or contract.
Quotation	An official document received from vendors that includes prices, availability of requested goods, payment, and delivery terms.
Requestor or Requesting Party	Person that is requesting the contracting or purchase of a commodity
Request for	An invitation to bid, a solicitation, made often through a bidding process, by

Term:	Definition:
Proposal RFP	the Procurement Unit to potential (qualified) suppliers to submit business proposals
Risk Management	Risk management refers to the forecasting and evaluation of financial, legal, and other negative factors that together could harm your business while identifying potential solutions or procedures to avoid or minimize their impact.
Security and Risk Assessment	A Security and Risk assessment or risk review will help the team evaluate the potential risks that could arise from using a product or service from a specific company. It is a crucial process to the ongoing monitoring and due diligence processes. The risk assessments will give you a better understanding of each vendor and their potential vendor risk to the university.

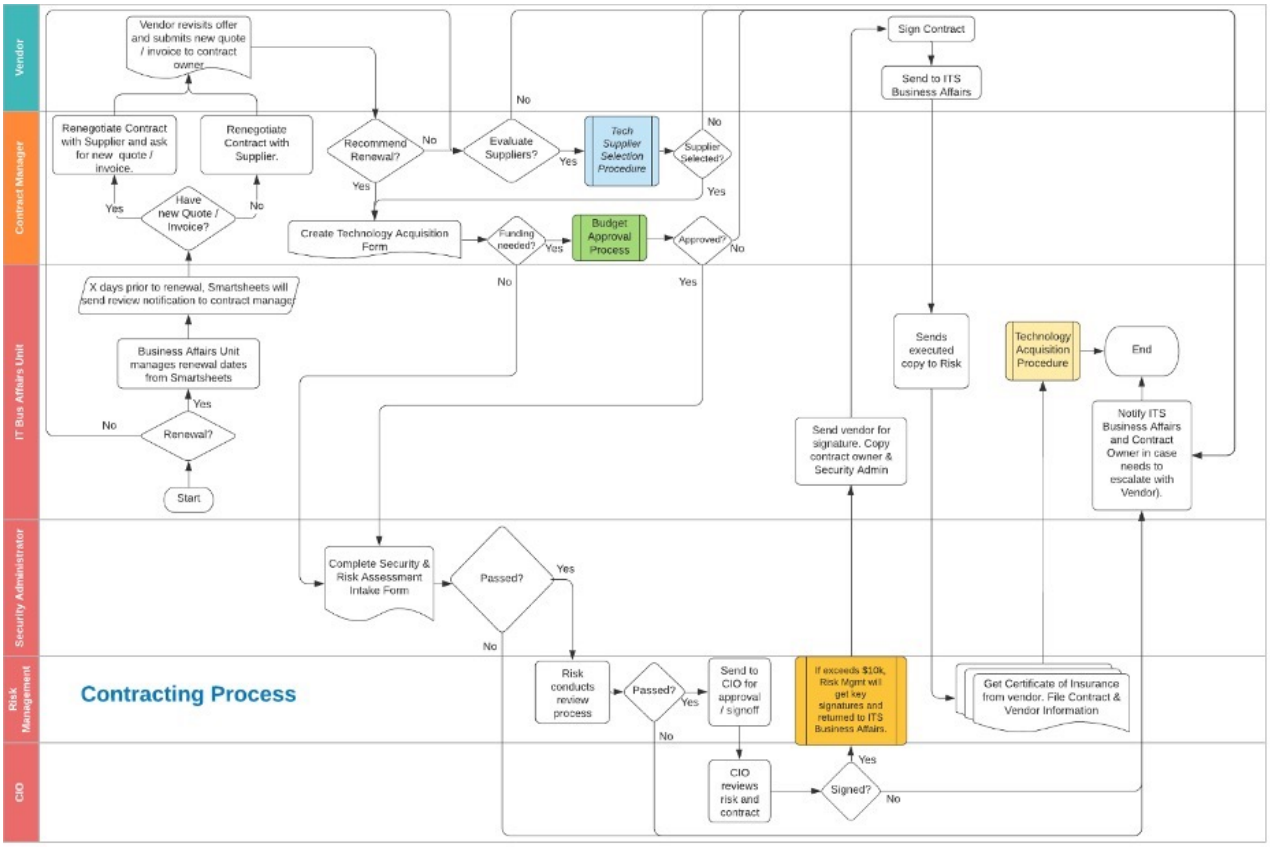
Service Organization Control (SOC) Reports	In addition to SSAE 16, three new reports have also been established as the framework for examining controls at a service organization, aptly named Service Organization Control (SOC) reports.
	• SOC 1 report is mainly concerned with examining controls over financial reporting,
	• SOC 2 and SOC 3 reports focus more on the pre-defined, standardized benchmarks for controls related to security, processing integrity, confidentiality, or privacy of the data center's system and information.
	  ○ SOC 2 examines the details of data center testing and operational effectiveness.
	  ○ SOC 3 is a public-facing document that gives a high-level overview of information in the SOC 2 report.

Software as a Service or SaaS	Software as a service (or SaaS) is a way of delivering applications over the Internet—as a service. Instead of installing and maintaining software, you simply access it via the Internet, freeing yourself from complex software and hardware management. SaaS applications are sometimes called Web-based software, on-demand software, or hosted software. Whatever the name, SaaS applications run on a SaaS provider's servers. The provider manages access to the application, including security, availability, and performance.
Specification	A concise statement explaining the type of product or service, the quality level, special requirements in design, performance, delivery, and usage.

Term:	Definition:
	Specifications must not be restrictive (locking in a specific vendor and limiting competition) or be vague (allowing a vendor to provide a lower than acceptable quality level product or service).
SSAE 16	In April 2010, the AICPA (American Institute of Certified Public Accountants) announced the replacement of SAS 70 by a new and refined auditing standard, the Statement on Standards for Attestation Engagements or SSAE 16. While SAS 70 was originally intended for financial and accounting auditing, the SSAE 16 audit was established to verify data center operational and security excellence.
Vendor	Any supplier who has business with Trinity University.

Attachments

Supplier Management Workflow



Related Documents

Related Content:

The ITS Supplier Management Policy is aligned with ISO 20400 Sustainable Procurement Guidance and with applicable laws and regulations. The *ITS Supplier Management Policy* complements the following internal policies: *BUSO-0031 Purchasing Policy and Procedures* as well as the *RISK-0007 Contract Policy and Procedures*.

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v2.0	4/27/2022 11:29 AM	Ben Lim
v1.0	2/7/2022 2:25 PM	Dan Carson

Vice President Approval:

Name:	Title:
Ben Lim	Chief Information Officer