IT Contract and Vendor Management Guide

Purpose

This guide supports the IT Service Ownership Standard, Third-party Arrangements Manual, and the principles relevant to procurement in the Finance Policy by providing practical guidance and setting out the minimum requirements to effectively manage UNSW IT contracts and vendors in business-as-usual (BAU) engagements.

It is designed to:

- Provide a consistent approach to IT contract and vendor management.
- Support IT Service Owners in managing material BAU IT contracts.
- Enable IT Service Owners to ensure relationships with vendors are managed effectively to reduce risk and comply with IT Service Management Practice requirements.
- Provide example tools and templates to support IT vendor relationship management.

Scope

- This guide outlines the approach to ongoing management and operational oversight of IT contracts and vendors. It offers structured guidance across key focus areas, providing a clear set of activities and supporting actions to help IT Service Owners manage IT contracts, and drive ongoing value from the vendor relationship.
- It applies to all IT Service Owners, as outlined in the IT Service Ownership Standard with responsibility for Tier 1 (Core), Tier 2 (Mission Critical) and Tier 3 (Business Critical) IT Services. Elements of this guide (such as governance framework and vendor performance management) may support IT Service Owners of Tier 4 (Business Important) and Tier 5 (Non-Critical) IT Services seeking to strengthen their management practices.

Not in Scope

This document does not address:

- Approval to engage with a third-party
- Drafting, negotiation and execution of agreements

Exclusion of IT Material Vendors

Material enterprise IT vendors are subject to a higher level of governance and oversight, which falls outside the scope of this guide. Governance activity associated with the management of UNSW IT material vendors is supported by the IT Vendor & Commercial team within IT.

Contents

1. Introduction

1.1. UNSW effectively operates a federated model, where the CIO has overall responsibility for the management and oversight of UNSW enterprise IT vendors, while UNSW faculties have accountability for the IT vendors that support the delivery of their services. The management of IT vendors includes the management of contracts, agreements, entitlements and contract and vendor governance.

1.2. Effective contract and vendor management ensures all parties meet their obligations, deliver contract outcomes, and provide a quality IT service experience. It also plays a critical role in managing business risk and maximising value from technology investments through clear controls and risk mitigation.

2. Governance Framework

2.1. A robust governance framework ensures accountability, transparency, and effective oversight throughout the IT contract and vendor management process. This framework defines roles, responsibilities, and reporting requirements to ensure that vendor relationships are managed proactively and in alignment with UNSW's Technology Strategy.

2.2. **Accountability and Oversight**

- For all UNSW IT contract and vendor arrangements, the IT Service Owner must manage and monitor the arrangement in accordance with the contract, to manage service delivery, risk, and performance of the IT vendor. The appropriate level monitoring and management is based on the nature, size, complexity, and risk profile of the arrangement. This may include periodic meetings with the IT vendor, assessing performance against agreed Service Level Agreements (SLAs) and assessing compliance against the contract.
- The IT Service Owner will determine the appropriate management and oversight required of non-material IT vendors to oversee performance against SLAs and contract performance, as appropriate to the engagement. The IT Service Owner should retain minutes and reports to evidence oversight of the IT vendor arrangement where required.

2.3. **Establishing Core Principles for Effective Vendor Management**

- Set Clear Expectations:
    - Both parties should share an understanding of what success looks like and agree on the criteria for meeting or exceeding expectations.
- Define Roles and Responsibilities:
    - Establish a clear breakdown of who is responsible for what on both sides. Define the key contacts and decision makers.
- Align on Performance Metrics and Compliance Requirements:
    - Make sure both parties agree on the metrics that will be used to evaluate performance. This includes setting measurable goals (e.g., uptime, response times) and ensuring the vendor is compliant with UNSW's policies and procedures where applicable.
- Build trust through transparent communication:
    - Foster an open, collaborative environment from the outset. Regular check-ins, feedback loops, and clear communication of expectations and challenges will help build a foundation of trust, ensuring that both parties feel comfortable voicing concerns and suggestions.

2.4. **Contractual Obligations and Compliance**

- Delivery Against Contract Terms:
    - The contract provides a formal governance framework for managing the vendor relationship, as well as each parties' obligations. The IT Service Owner is responsible for ensuring that all

governance processes outlined in the contract are followed, including performance monitoring, reporting, and escalation procedures.
    - Periodic reviews should be conducted to confirm that the governance framework is being applied in practice, and that both parties are meeting their obligations.

- Ensuring Contractual Compliance:
    - Monitor compliance with all contractual provisions, including legal, regulatory, information security, and operational requirements.
    - Respond to breaches or non-compliance through agreed escalation paths and corrective actions.
    - Maintain accurate records of contract variations, renewals, non-compliance incidents, and resolutions for audit and governance purposes.
    - Monitoring of contractual obligations can be carried out using UNSW's Contract Lifecycle Management (CLM) system, ContractPodAI. The CLM system is UNSW's system of record for storing third-party arrangements.
    - Where applicable, involve risk, legal or compliance functions in reviewing high-risk vendor arrangements to ensure obligations are being met.

3. Roles and Responsibilities

3.1. This guide supports the Contract and Vendor Management Service management practice, focusing primarily on the Service Owner role, as outlined in the IT Service Ownership Standard. While other roles such as Business Owner, Business Operations Owner, Delivery Owner, and Subject Matter Experts (SMEs) provide input or support as needed, this guide is intended for Service Owners responsible for the ongoing vendor management and governance of IT service providers. For detailed role descriptions and responsibilities, please refer to the IT Service Ownership Standard above.

4. Vendor Performance Management

4.1. Ongoing vendor performance management ensures that contractual commitments are met, service levels are maintained, and the vendor continues to deliver value throughout the relationship. This includes regular monitoring, formal reviews, and clear mechanisms for issue resolution.

4.2. Effective performance oversight also requires clarity on how the commercial relationship with a vendor is structured and managed. This may be done at the contract level, or across the broader vendor relationship. The IT Service Owner is responsible for determining the most appropriate approach:
    - Where there is a single material contract, performance can be managed at the contract level, with that contract forming the basis for performance oversight and governance.
    - Where there are multiple contracts or statements of work with the same vendor, managing performance at the vendor level - across all agreements - is considered better practice to ensure consistency, alignment, and a holistic view of vendor performance. This ensures that governance is proportionate to the scale and complexity of the relationship.

4.3. **Performance Expectations and Metrics**

- Operationalising SLAs and Key Performance Indicators (KPIs):
    - Embed SLAs and KPIs into every stage of the vendor relationship, from daily operations to strategic reviews. These metrics should be actively used to guide decision making, resource allocation and issue resolution.
    - Use tracking tools (e.g., dashboards, performance reports) to continuously monitor performance against the agreed metrics, adjusting as needed.
    - Ensure that internal teams are fully briefed on the SLAs and KPIs, and that performance expectations are clearly communicated to the vendor. This ensures alignment between internal goals and external deliverables.

4.4. **Ensure Adherence to Contract Terms**

- Review Contract Terms Regularly:

    - Conduct periodic reviews of the contract terms to ensure both parties are fulfilling their obligations. This includes reviewing SLAs, KPIs, compliance requirements, and deliverables.
    - Where necessary, initiate variations to the contract to account for significant changes in business requirements, market conditions, or performance issues. Ensure that any contract variations are formally agreed upon by both parties, documented and captured to the CLM system and/or to an appropriate University System of Record.

- Address Deviations Immediately:
    - If a deviation from contract terms occurs, address it immediately. Work with the vendor to identify the cause and determine a solution.
    - Ensure that corrective actions are clear, documented, and followed up on to prevent recurrence.
    - Should a deviation remain unremedied and risk escalating to a breach, Legal & Compliance must be engaged.

- Contractual Changes:
    - Maintain accurate records of any contract variations or renewals which should be stored in the CLM system. Changes should be formally agreed by all parties and clearly documented to ensure accountability.

4.5. **Track and Measure Vendor Performance**

- Monitor Performance Continuously:
    - Use the agreed SLAs and KPIs to continuously track and measure vendor performance. Leverage real time monitoring tools like dashboards and automated reports to regularly assess the vendors output, quality, and adherence to timelines.
    - Regularly review both quantitative metrics (e.g., delivery time, cost) and qualitive factors (e.g., customer service, responsiveness) to assess overall vendor performance.

- Regular Performance Reviews:
    - Hold scheduled review meetings with the vendor to discuss performance outcomes. These meetings should focus on both successes and areas needing improvement, aligning both parties on how to address any issues.
    - Agree on corrective actions where necessary, ensuring they are documented for transparency and accountability.

- Identify Trends and Act Early:
    - Look for patterns in performance data over time (e.g., recurring delays, customer service complaints) to identify issues early. Take proactive steps to resolve these patterns before they impact the broader business.

4.6. **Issue Management and Resolution**

- Monitor Early Warning Signs:
    - Leverage monitoring tools and regular reviews to catch issues early, allowing for proactive intervention. This reduces the need for formal escalation and can prevent more serious issues from developing.

- Collaborate to Resolve Issues:
    - Work with the vendor to find solutions quickly and collaboratively and use the opportunity to strengthen the partnership and ensure both sides understand the root cause of the issue.
    - Document outcomes and corrective actions to ensure clarity and prevent future recurrence.

- Review and Improve the Process:
    - After resolving issues, evaluate the effectiveness of current operational issue management and escalation triggers. Share lessons learned with both internal teams and vendors to enhance future issue resolution.

5. Risk Management

5.1. Risk management in vendor relationships and contracts ensures that potential disruptions are anticipated and minimised. This includes both strategic and operational risks that could impact performance, security, compliance, or business continuity.

5.2. **Identify and Assess Risks**

- Identify potential risks related to the vendors' performance, including operational, financial, compliance, and security risks.
- Conduct regular risk assessments to evaluate both the likelihood and impact of each identified risk.
- Ensure that the assessment considers both external and internal factors, such as market shifts, vendor instability, and changing regulations.

5.3. **Establish Risk Mitigation Plans**

- Develop mitigation strategies for high-priority risks, such as introducing contingency plans, considering alternative vendors, or obtaining insurance for key areas.
- Ensure the vendor is aligned with the risk mitigation strategy and understands their role in addressing potential risks.
- Implement contingency measures (e.g., back-up vendors) for critical risk areas to ensure business continuity.

5.4. **Monitor and Review Risks Continuously**

- Monitor risks regularly to ensure that they remain within acceptable limits. This involves ongoing surveillance of performance, financial health, cybersecurity threats, and compliance status.
- Use a risk register to document and track risks over time, allowing both parties to stay informed of emerging issues.
- Review risk levels periodically to identify any new risks, emerging threats or changes in the vendors situation that may require adjustments to the risk management strategy.

5.5. **Collaborate on Risk Management**

- Collaborate with the vendor to develop shared risk management plans, particularly for high-impact risks that affect both parties.
- Ensure that both parties have a clear understanding of responsibilities and actions in the event of risk activation.
- Review and update risk management plans regularly, ensuring that both parties remain prepared for changes in market, operational, or regulatory conditions.

6. Contractual Issue Escalation and Resolution

6.1. Escalation is a critical part of contract and vendor management, providing a formal process for managing issues that cannot be resolved at the operational level. Timely and structured escalation ensures service continuity, risk mitigation, and contractual accountability.

6.2. **Escalation Framework and Responsibilities**

- The escalation framework is defined in the contract and outlines the formal path for resolving unresolved or high-impact issues.
- The IT Service Owner is responsible for initiating and managing escalations in accordance with this framework.
- Escalation should follow a clearly defined, tiered path - from operational contacts through to senior stakeholders - as outlined in the contract or agreed governance approach.
- Escalation activity should be documented and escalated through the appropriate oversight structures as defined in the contract.
- Before exercising any dispute resolution or termination rights under an agreement, the IT Service Owner must seek legal advice from Legal & Compliance to manage any legal risk to the University.

6.3. **Early Warning and Proactive Engagement**

- Monitor vendor interactions and performance data for early indicators of potential issues (e.g., repeated delays, service outages, poor responsiveness, or policy breaches).
- Escalation should not be the first step - engage the vendor early to clarify expectations and initiate corrective action.
- Early and proactive action can avoid formal escalation and maintain a productive working relationship.
- Engage legal for guidance during renewal or renegotiation where risks have been identified to ensure appropriate review.

6.4. **Collaborate to Resolve Issues Prior to Formal Escalation**

- Aim to resolve issues collaboratively before moving into formal escalation stages.
- Ensure all parties have a shared understanding of the issue, its impact, and the desired outcome.
- Agree on a clear set of corrective actions, owners, and deadlines - documented and tracked.

6.5. **Escalation Documentation and Closure**

- Keep full records of escalated issues, including the trigger, steps taken, decisions made, and final outcomes.
- Escalated issues should be reviewed regularly as part of performance and governance discussions.
- Use escalation data to identify recurring themes and systemic improvement opportunities across vendor relationships.

7. Vendor Development and Continuous Improvement

7.1. Beyond contractual compliance and performance monitoring, vendor development focuses on strengthening relationships, enhancing value, and driving ongoing improvements. This is particularly important for strategic or long-term IT vendors where alignment, innovation, and adaptability impact business outcomes. The IT Service Owner is responsible for identifying opportunities to engage vendors in continuous improvement efforts that benefit both parties.

7.2. **Promote Collaborative Development**

- Establish regular engagement beyond operational reviews to discuss forward looking opportunities, innovations, or pain points.
- Encourage openness, transparency, and a joint problem-solving mindset to strengthen the working relationship.
- Involve relevant business and technical stakeholders to ensure input into vendor capability development and service evolution.

7.3. **Identify and Prioritise Improvement Opportunities**

- Use performance insights, risk reviews, and lessons learned to identify areas where service quality, process efficiency, or outcomes can be improved.
- Align improvement initiatives to business priorities, emerging technology needs, or future capability gaps.
- Document agreed improvement actions, assign ownership, and track progress over time.

7.4. **Support Innovation and Uplift**

- Where appropriate, invite vendors to propose innovative technologies, tools, or delivery models that could improve business performance.
- Enable pilots or trials under controlled governance to assess the feasibility of proposed innovations.
- Recognise and reward vendors who actively contribute to business innovation or uplift capability beyond minimum expectations.

7.5. **Review Development Outcomes**

- Conduct periodic development reviews to evaluate the progress and impact of improvement initiatives.

- Adjust development focus areas in response to changing business needs, vendor maturity, or contract evolution.

8. Exit and Transition Management

8.1. Vendors exit and transition must be planned and executed to ensure continuity of operations, data security, and contractual compliance. Whether the exit is due to contract expiry, termination, or vendor change, effective transition planning protects the University from operational and reputational risk.

8.2. Exit and transition responsibilities should be embedded in the contract and managed proactively by the IT Service Owner in collaboration with Procurement, Legal, IT and other relevant stakeholders.

8.3. **Planning**

- The IT Service Owner must be familiar with the vendors exit and transition provisions and ensure they are accessible, understood, and ready to be enacted if needed.
- A formal exit and transition plan must be developed and maintained, outlining key activities, timeframes, roles, and dependencies.
- Planning should address practical requirements such as resource handover, system access and data transfer, IP rights, disengagement protocols, data removal and destruction from vendor systems and dependencies.
- Exit scenarios should be regularly evaluated during vendor relationship discussions to ensure plans remain fit for purpose and aligned to business needs.

8.4. **Execution**

- The IT Service Owner is responsible for activating and managing the agreed plan when exit is triggered.
- Progress should be tracked against defined milestones, with risks and issues actively managed.
- Ensure all contractual requirements are met, including appropriate handling of data, access and permissions, systems and infrastructure, and any agreed technical deliverables.
- Maintain clear communication with internal stakeholders and the vendor to support a controlled and well managed exit process.

8.5. **Close Out and Learn**

- Confirm all exit and transition activities are complete and documented.
- Capture lessons learned and feedback from stakeholders to improve future vendor selection.
- Confirm all data, documentation and systems access have been returned or securely decommissioned.
- Ensure final records are retained in line with UNSW policies and audit requirements.

9. Tools, Templates and Support

9.1. A selection of tools and templates is available to support activities in this guide. These resources are designed to bring structure, consistency, and visibility to your contract and vendor management. They can be applied as needed, to suit the scale and complexity of your vendor relationships. See the appendices section of this guide for more detail.

- If you have any questions, or need assistance using these resources, please contact the IT Vendor & Commercial team within IT.

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Head of Vendor & Commercial	13 October 2025	01 November 2025	Baseline Version

Appendix A - UNSW IT Contract and Vendor Management - Meeting Minutes & Action Items

UNSW IT Contract and Vendor Management

Meeting Minutes & Action Items

Meeting Specifics					
Meeting Name:				**Meeting No:**	
Meeting Date:		**Start:**		**Finish:**	
Meeting Location:					
Meeting Leader:					
Members:					
Attendees:					
Minute Taker:					
Apologies:					

Agenda Items	
Item No.	***Description***

Minutes of Meeting

Decisions	
Mtg / Decision No	***Decision***

New Action Items					
Mtg / Action No	***Action***	***Owner***	***Raised Date***	***Due Date***	***Status***

Previous Outstanding Action Items					
Mtg / Action No	***Action***	***Owner***	***Raised Date***	***Due Date***	***Status***

Closed Actions from Previous Meeting					
Mtg / Action No	***Action***	***Owner***	***Raised Date***	***Due Date***	***Date Closed***

Appendix B - IT Contract and Vendor Management Risk Register

This risk register template is a business-as-usual (BAU) operational oversight tool designed to help teams monitor IT contract and vendor performance. It supports tracking vendor risks, documenting actions, and promoting good contract management practices.

This template operates independently of the enterprise risk management (ERM) framework and does not use ERM risk ratings or categories. Risks should be escalated into the enterprise risk process if they present material business impact, regulatory concern, or cannot be resolved through normal business oversight.

If unsure whether a risk requires escalation, please refer to the Risk and Compliance Policy or consult your Risk Management team.

ID	Risk Description	Risk Category	Status	Potential Impact	Mitigation / Action Plan	Owner	Last Reviewed	Escalation Needed	Comments
R001	*Consistent delays in delivery of critical updates/releases*	*Performance*	*Active*	*Moderate*	*Weekly progress meetings, monitor delivery against SLA*	*Mary J.*	*15/09/25*	*No*	*Minor operational disruption noted*

Field Definition
ID: Unique identifier (e.g., R001)
Risk Description: Concise summary of the risk
Risk Category: This refers to the broad type of risk being monitored. Categories should be tailored to reflect the key risk areas relevant to your contract and vendor, such as Performance, SLA Compliance, Security, Financial or Compliance risks. Use categories that help you organise and prioritise risks effectively.
Status:

- **Potential:** Risk identified but no impact yet
- **Active:** Risk currently impacting performance or operations
- **Ongoing:** Risk unresolved, under continuous monitoring or action
- **Resolved:** Risk closed or effectively mitigated

Potential Impact: Minor, Moderate, High
Mitigation / Action Plan: Planned or active measures to address the risk
Owner: Person or role responsible for managing the risk
Last Reviewed: Date the entry was last updated or reviewed
Escalation Thresholds: Escalate if:

- Risk has high or critical impact on business operations, data security, or reputation
- SLA breaches result in significant delays or service interruptions
- Risk remains Active or Ongoing beyond agreed remediation timelines
- Risk mitigations are insufficient or ineffective

If unsure about escalation, please contact your risk team for guidance.

Comments: Any relevant notes, updates, or context

Note: The risk categories, statuses, examples, and escalation thresholds provided are for guidance only. Please tailor the risk register template to fit your specific contract, vendor and operational context.

Appendix C - Key Activity Checklist

Key activities to guide effective IT contract and vendor management.

IT Contract and Vendor Management Key Activity Checklist	
Roles and governance	
Identify key personnel and their responsibilities on both sides (UNSW and vendor)	☐
Agree on meeting cadence and participation to ensure consistent communication	☐
Define decision making authority and clear escalation pathways for issues	☐
Relationship	
Define mutual goals and success measures for the relationship	☐
Review strategic alignment and business priorities at least annually	☐
Performance monitoring and reporting	
Define reporting requirements and ensure a shared understanding of SLAs/KPIs	☐
Schedule regular performance reporting and reviews to identify gaps and agree actions	☐
Periodically review and adjust SLAs/KPIs to keep them relevant to business needs	☐
Risk mitigation and management	
Identify and assess key vendor related risks	☐
Confirm vendors business continuity and disaster recovery plans are current and tested	☐
Maintain a risk register with regular updates and reviews	☐
Issue Management and Resolution	
Implement the agreed process for raising, logging, and tracking issues	☐
Confirm escalation points and timelines are understood by both parties	☐
Vendor development and continuous improvement	
Set focused goals that drive real improvements in value or performance	☐
Exit and Transition Management	
Confirm vendor has developed detailed exit & transition plans	☐