Case Studies and FAQs

Case study

Case study

Example Case Study: High-Value, High-Risk Contract & Supplier Management

Please note: This is an example for illustrative purposes

Project Overview

Organisation: XXX
Contract Title: National Intelligent Transport Infrastructure Modernisation Programme
Contract Value: £100 million over 7 years
Risk Level: High value / high risk
Procurement Route: Competitive Procedure with Negotiation (CPN) under the Public Contracts (Scotland) Regulations
Supplier: Large multi-national infrastructure and ICT provider
Purpose: Upgrade national network of roadside sensors, traffic management systems, and data platforms to improve safety, analytics, and real-time public information.

Why the Contract Was High-Risk

Strategic and Operational Importance

- This infrastructure underpins safety-critical systems (e.g., variable speed limits, incident detection)
- Failure would have direct public safety impact

Complex Multi-Technology Solution

- Integration of ageing legacy infrastructure with new digital systems
- Significant cyber security requirements
- Dependence on interoperability between multiple Scottish public bodies

Supplier Market Conditions

- Very limited supplier market (only 3 global providers)
- Known risk of over-reliance on one provider creating long-term lock-in

Financial & Commercial Exposure

- Long-term technology contracts historically have cost-creep risks
- Supplier previously had delivery delays on large UK programmes

Procurement Stage Risk Management

Early Market Engagement

XXX conducted:

Prior Information Notice (PIN) with supplier briefings

- **Discovery sessions** with potential suppliers to test feasibility and innovation
- Publication of **standardised SPD statements** for consistent supplier responses

Robust Specification & Outcomes-Based Requirements

- Performance standards for system up-time, incident detection accuracy, and data latency
- Mandatory cyber-security controls aligned to Scottish Government Cyber Resilience Framework
- Clear exit and data handover requirements to prevent supplier lock-in

Multi-Stage Evaluation

- Technical capability weighting = **65%**
- Commercial/price weighting = **35%**
- Inclusion of scenario-based assessments and live demonstrations of key functionalities

Detailed Risk Allocation

- Supplier responsible for system performance and integration
- Authority retained responsibility for policy, governance, and network access permissions
- Shared risk register established before contract award

Contract Management Framework (Post-Award)

Governance Structure

Strategic Level (Quarterly)

- Senior Responsible Owner (SRO)
- Supplier’s Programme Director
- Independent Assurance Consultant
- Focus on: strategic risks, contract changes, long-term road map

Tactical Level (Monthly)

- Contract Manager
- Supplier Account Manager
- Performance and risk leads
- Review of KPIs, milestones, financials, workforce, supply chain, and cyber security posture

Operational Level (Weekly)

- Project delivery teams
- Issue logs, work package progress, testing results

KPIs and Performance Measures

Area	KPI Example	Target
System Availability	Up-time of traffic control platform	99.95%

Incident Detection	Accuracy of automated sensors	> 96%
Cyber security	Patch deployment time	< 48 hrs
Delivery Milestones	Infrastructure roll out	95% on time
Social Value	Local SME engagement	18% of contract value

Contract Management Issues & Response

Issue 1: Supplier Delays on Critical Milestones

The Supplier fell **9 weeks behind schedule** during Phase 1 due to shortages in specialist engineers.

Mitigation Actions

- Invoked the contract's **remedy plan clause** requiring a detailed recovery plan within 10 working days
- A joint task-force was created including XXX technical specialists
- Supplier re-allocated additional resources from EU teams at their own cost
- Milestone re-baselining approved with no increase in contract price

Issue 2: Cyber security Vulnerability

Independent assurance testing discovered a **medium-severity vulnerability** in the cloud analytics module.

Mitigation Actions

- Immediate escalation to Strategic Board
- Supplier required to deploy emergency patch within 72 hours (as per contract)
- Additional penetration testing introduced quarterly

Issue 3: Supplier Financial Health Concerns

Market analysis revealed the Supplier parent company experienced losses in two consecutive quarters.

- **Mitigation Actions**
- Financial monitoring increased from quarterly to monthly
- Supplier required to provide updated financial statements and parent-company guarantees
- Contingency planning for partial or full supplier failure (including alternative suppliers and in-sourcing scenarios)

Continuous Improvement and Social Value Delivery

The supplier delivered several social and economic benefits:

- **Apprenticeship programme** with Scottish colleges (14 apprentices across digital engineering)
- **Local supply chain development** with 22 Scottish SMEs
- Traffic safety educational sessions delivered to schools in deprived areas. XXX tracked these commitments quarterly against the **Fair Work and Community Benefits** requirements

Contract Close-Out & Lessons Learned

Positive Outcomes

- National intelligence transport system modernised on time (after early recovery) and on budget
- Incident response times improved by **19%**
- Availability levels exceeded the contractual requirement (achieved 99.95%)

Key Lessons Learned

1. **Early, structured risk allocation** prevented costly disputes later
2. **Strong governance** enabled quick escalation and resolution of issues
3. **Independent assurance** was critical to managing a complex digital contract
4. **Market concentration risk** must be continually monitored
5. Embedding **exit planning** from the start avoided long-term dependency

FAQs

1. What is a medium to high value, medium to high risk contract?

Open or close

- **Value:**Typically £500,000 – £5m (can vary by sector and thresholds).
- **Risk:** Contracts where failure could impact service delivery, finances, or stakeholder trust
- Often includes **IT systems, social care provision or consultancy frameworks**.
- Involves complex supply chains or innovative/IT-heavy solutions.
- Is strategically important or politically sensitive.
- Risk factors include supplier dependency, complex delivery requirements, or political/operational sensitivity.

2. Why is contract and supplier management (CSM) important for medium to high-risk contracts?

Open or close

Lack of CSM can result in issues including:

- Service disruption
- Cost creep
- Delays
- Supplier insolvency
- Supplier under-performance
- Reputational or political damage
- Litigation and contractual disputes

Effective management ensures value for money, protects the public purse, and maintains service continuity.

Medium-high risk contracts often lack dedicated resources, so structured management is very important.

3. What Governance arrangements should be applied?

Open or close

- Assign a **Contract Owner / Manager** with clear authority and other roles and responsibilities
- Define **escalation routes** for issues, including risk or financial alerts.
- Maintain **regular reporting** and audit-ready documentation.

4. Contract and supplier management activities

Open or close

Typical requirements could include:

- Early **risk identification and mitigation plan**.
- Detailed **mobilisation plans**
- Early **risk workshops** and continuous risk management
- **Performance monitoring** (bi-weekly/monthly/quarterly depending on risk).
- Use **KPIs or milestones** appropriate to contract scale with clear corrective action routes
- Schedule **regular review meetings** and document decisions
- Detailed **financial monitoring** of the supplier, including supplier solvency checks
- Formal **change control** processes
- Continuous **stakeholder communication**

5. How should risk be assessed and monitored?

Open or close

Using a structured approach, you may wish to:

- Maintain a **contract-specific risk register**
- Score **likelihood and impact** (financial, operational, reputational)
- Assign **risk owners** and track mitigation actions
- Review **risk quarterly** or more frequently for higher-risk areas

6. How do I ensure supplier performance is adequately monitored?

Open or close

You may wish to:

- Ensure **KPIs / milestones** must be clearly defined in the contract
- Conduct **quarterly progress reports** and financial checks
- Conduct regular **performance dashboards**
- Hold **formal review meetings** with agendas and minutes
- Maintain **communication logs** for decisions and clarifications
- Ensure **prompt action** if KPIs are not met

7. What should happen if a supplier is under performing?

Open or close

Steps could include:

- Informally raise performance issues early
- Issue formal **Improvement Notices** or **Rectification Plans**
- Escalation to **steering group** for high-impact risks
- Consider **contractual remedies** or contingency plans
- Escalate to the **contract board/other governance arrangement** if no progress
- Prepare business continuity and **exit strategies** if risk escalates

8. How should supplier financial stability be monitored?

Open or close

- Review annual accounts and financial health checks
- Quarterly financial checks (or monthly for very high-risk contracts)
- Monitor for **cash-flow problems, litigation, or management changes**
- Monitor market news, mergers, legal disputes
- Consider **parent company guarantees** or insurance clauses
- Use **contingency plans** in case of supplier failure

9. How is value for money protected during the contract?

Open or close

- Strong **change control** to avoid scope creep
- Benchmarking and market comparison
- Auditing of supplier invoices and open-book accounts
- Performance-linked payments
- Ongoing contract review for efficiency opportunities

10. What happens if a supplier becomes insolvent?

Open or close

Organisations should have:

- Pre-established **continuity plans**
- Step-in provisions (where applicable)
- Access to source data, assets, or IP
- Backup suppliers / frameworks identified
- Communication plans for stakeholders and service users

11. How should change requests be handled?

Open or close

Through a formal process that includes:

- Written request
- Impact analysis (cost, time, risk)
- Approval by the contract board/other agreed governance structure
- All changes should be **documented** and **approved**
- Assess impact on **cost, timeline, and risk**
- Update KPIs and reporting requirements if necessary
- Ensure **formal record** is maintained for audit purposes

No change should occur without formal approval.

12. What are some lessons learnt from Scottish public sector experience?

Open or close

- Medium-high risk contracts can fail due to **weak governance or unclear requirements**
- Supplier relationship management is critical; lack of oversight increases risk
- Financial and performance monitoring should **match risk level**, even for “medium” contracts.

Clear **documentation** and audit trails reduce dispute risk.

13. What documentation should be kept?

Open or close

- Contract and all schedules
- Change register
- Risk register
- Meeting minutes
- Performance logs
- Communication logs
- Payment records
- Supplier financial assessments
- Decision audit trail

This protects auditability and supports dispute resolution.