Skyral

Service Definition Document: Skyral Decision Support and Problem Solving as a Service – Risk, Vulnerability & Resilience

Service Name: Skyral Decision Support and Problem Solving as a Service – Risk, Vulnerability & Resilience
Supplier Name: Skyral Defence Ltd
Framework and Lot: G-Cloud 15, Lot 3

Version Number: v1.0

Date: 14 January 2026

Status: Final

Author: Mark Holland

Approver: Skyral Product Leadership



1. About Skyral

Skyral is a UK-headquartered modelling, simulation and decision-support company that helps governments, critical national infrastructure operators and enterprises understand, anticipate and manage complex risks. Using large-scale digital twins and advanced modelling, Skyral represents how assets, people, processes, systems and external threats interact as living networks rather than static diagrams.

Risk, vulnerability and resilience customers use Skyral to:

- See how risks emerge, propagate and interact across operations, supply chains, infrastructures and geographies.
- Test “what-if” scenarios for hazards, disruptions, failures and threats before they occur in the real world.
- Design and evaluate mitigation strategies, contingency plans and resilience investments with evidence rather than intuition.

Skyral CORE provides the underlying capability to build, run and govern simulation-driven risk and resilience digital twins as a long-lived decision-support capability.

2. Service Overview

Service name

Skyral Decision Support and Problem Solving as a Service – Risk, Vulnerability & Resilience

Purpose

Skyral Decision Support and Problem Solving as a Service (Risk, Vulnerability & Resilience Edition) is a focused, typically one-month engagement that shapes how modelling and simulation should be used to understand, anticipate and mitigate complex risks.

It is designed to:

- Turn broad concerns about risk, vulnerability and resilience into a structured, decision-ready view.
- Produce a prioritised set of risk levers, use cases and scenarios to focus limited resilience and risk-management resources on.

- Define a clear follow-on path into Skyral Modelling and Simulation Development as a Service (Risk & Resilience Edition) and full risk / resilience digital-twin programmes.

This edition serves organisations concerned with operational resilience, critical national infrastructure protection, supply-chain fragility, emergency management, climate-related risk, regulatory compliance and enterprise risk management.

Typical duration and team

A standard engagement is one month of effort, delivered by:

- A risk / resilience Subject Matter Expert (SME) with experience in operational risk, resilience, CNI or enterprise risk management.
- An Applied Scientist specialising in modelling, simulation and analytics.
- A Product Owner responsible for mapping outcomes into Skyral services, products and the organisation's risk, operations and data landscape.

Longer or multi-phase engagements can be scoped where risk and resilience concerns span multiple sectors, geographies or regulatory regimes.

3. Method and Activities

The service focuses on complex, interconnected risks—where standard risk registers and point tools struggle—and prepares the ground for synthetic environments that can test shocks, threats and mitigations at scale.

Core steps

1. **Clarify the risk and resilience problem**
    - Establish a shared understanding of key risk and resilience questions (e.g. operational resilience, CNI disruption, systemic supply-chain risk, climate hazards, cyber-physical threats, regulatory scenarios).
    - Capture desired outcomes and constraints: tolerances, impact thresholds, recovery objectives, regulatory tests, stakeholder expectations and time horizons.
2. **Map systems, interdependencies and threat surfaces**
    - Disaggregate the problem using logic trees and causal structures across assets, services, processes, people, suppliers, partners, infrastructure and external conditions.
    - Identify critical interdependencies and fragilities: single points of failure, tight couplings, capacity constraints, geographical or supplier concentrations, key data or system dependencies.



- Map relevant threat vectors and hazards (e.g. infrastructure failures, cyber-physical attacks, natural hazards, demand shocks, macro events).

3. **Define and refine risk and resilience metrics**
   - Identify metrics linked directly to risk and resilience (e.g. probability and impact of failure, time to recover, service continuity, cascade depth, regulatory thresholds, financial loss, safety and reputational indicators).
   - Clarify how trade-offs will be judged: cost vs resilience, redundancy vs efficiency, risk reduction vs time-to-implement, local vs systemic benefits.
4. **Develop high-level causal and probabilistic risk models**
   - Using Skyral's Simulation Scaffold Framework, build high-level causal and probabilistic models that describe how risks emerge, propagate and interact across the system.
   - Represent how different hazards, failures and threat vectors influence each other, and how mitigations or controls change risk and resilience profiles.
5. **Identify and prioritise critical risk levers**
   - Prior to and during delivery, Skyral and the customer identify critical risk levers such as system fragilities, interdependency points, threat vectors, capacity constraints, hazard impacts or organisational vulnerabilities.
   - Apply heuristics, cleaving maps and quantitative reasoning to prioritise these levers and associated initiatives by impact, likelihood, feasibility, time-to-value and regulatory/materiality relevance.
6. **Develop a practical risk and resilience work plan**
   - Convert prioritised levers and initiatives into a concrete work plan for further analysis, simulation, mitigation design and investment planning.
   - Define data needs (e.g. incident and loss data, asset and process inventories, supplier and logistics data, hazard layers, financials), stakeholders, integration points (risk tools, BI, operational systems) and decision checkpoints.
7. **Frame follow-on risk & resilience digital-twin and simulation work**
   - Define how risk and resilience digital twins should be scoped and built in follow-on Skyral Modelling and Simulation Development as a Service (Risk & Resilience Edition) engagements.
   - Outline key scenarios and experiments (e.g. stress tests, outage cascades, climate scenarios, supply-chain disruptions, regulatory scenarios) and decision-support use cases.

4. Service Outputs

At the end of the engagement, the customer receives:

- **Risk and resilience decision narrative**
    - A clear articulation of the risk and resilience problem, context, constraints and objectives.
    - A visual representation of key drivers, interdependencies, threat vectors and vulnerabilities across operations, assets, people, supply chains and external conditions.
- **Prioritised risk levers, scenarios and initiatives**
    - A ranked list of risk levers and resilience initiatives (e.g. controls, redundancy, diversification, hardening, process changes, contingency plans) with rationale and key assumptions.
    - Identification of the top levers and scenarios best suited for simulation and digital-twin development.
- **Risk and resilience metric framework**
    - Defined risk and resilience metrics mapped directly to prioritised levers and initiatives.
    - Commentary on how these indicators should be tracked and used in future scenario analysis, regulatory assessments and governance.
- **High-level causal / probabilistic risk model**
    - A high-level causal and probabilistic model of the risk landscape, suitable as a scaffold for more detailed simulation and for engaging boards, regulators and operational leaders.
- **Strategic roadmap and action plan**
    - A strategic roadmap and actionable plan that guides follow-on synthetic environment and digital-twin development, scenario testing, resilience planning and risk-reduction work.

Outputs are delivered in accessible formats (e.g. slide pack, report and, where appropriate, simple scenario exploration views) that can be used directly in risk committees, resilience forums and board or regulatory engagements.

5. Roles and Responsibilities

Skyral roles

Role	Description	Key responsibilities
SME	Risk / resilience expert leading the engagement	Form the core project team; define the risk and resilience problem; shape initiatives and levers; lead prioritisation and metric design; co-create work plan.
Applied Scientist	Modelling, simulation and analytics specialist	Understand systems and risk drivers; gather and analyse data; build causal/probabilistic models; apply statistics and heuristics for prioritisation; assess modelling feasibility.
Product Owner	Owns service delivery and transition into Skyral services / products	Plan and manage the work; translate outcomes into Skyral services and products; define follow-on Modelling and Simulation Development as a Service (Risk & Resilience Edition) scope.

Customer responsibilities

- Provide access to relevant risk, resilience, operations, finance, security and data/analytics stakeholders.
- Share existing risk registers, resilience plans, incidents and loss data, asset/process inventories and relevant models where appropriate.
- Confirm regulatory, data-governance, confidentiality and assurance requirements early.
- Participate in workshops, reviews and prioritisation sessions; agree scope boundaries, timelines and decision processes.

6. Service Features and Benefits for Risk, Vulnerability & Resilience

Key features

- Whole-system risk and resilience problem definition across operations, assets, people, supply chains and external conditions.
- Causal and probabilistic mapping of vulnerabilities, interdependencies and threat dynamics.



- Risk and resilience metric framework design linked directly to critical levers and initiatives.
- Evidence-based prioritisation of risk-reduction and resilience initiatives using advanced heuristics and structured reasoning.
- High-level decision model and strategic roadmap into synthetic environment and risk digital-twin programmes.

Key benefits

- **Faster clarity on complex risks**: Move from long risk registers and qualitative assessments to a precise, shared understanding of how risks emerge and propagate.
- **Sharper focus of resilience investment**: Target resilience spending and controls at the levers and interdependencies that materially reduce exposure and improve recovery.
- **Decision-ready digital-twin scope**: Enter risk and resilience digital-twin work with a well-framed, prioritised scope, reducing rework and delivery risk.
- **Explainable, defensible risk insights**: Use transparent causal and probabilistic models to support regulatory engagement, board discussions and assurance, rather than opaque black-box outputs.
- **Continuous resilience improvement foundation**: Establish a structured path into ongoing simulation-driven stress testing, scenario analysis and resilience planning.

7. Dependencies and prerequisites (including customer responsibilities)

This service depends on access to sufficient business, operational and financial context to build a meaningful optimisation decision narrative and work plan.

- Key prerequisites (customer side):
- Access to relevant stakeholders across risk, resilience, operations, security, continuity, finance, compliance and data/analytics, including sponsors able to agree priorities and scope.
- Provision of current and target-state information on the systems, assets, services and geographies in scope, such as risk registers, resilience plans, asset and process inventories, organisational structures, supplier and partner maps and major change programmes.
- Provision of representative data where available: incident and loss data, outage and recovery histories, capacity and utilisation metrics, supplier and logistics data, hazard and threat layers, financial impact data and regulatory requirements.



- Early confirmation of regulatory, assurance and data-governance constraints, including treatment of sensitive operational information, personal data, security-sensitive data and any cross-border or cross-entity restrictions.

Where underlying tools or datasets are immature or unavailable, Skyral can use proxy data, synthetic scenarios or partial representations to proceed, with limitations and assumptions clearly flagged in the risk and resilience decision narrative and work plan.

8. Onboarding and implementation approach

Onboarding is structured as a short, time-boxed engagement that moves quickly from risk/problem clarification to decision-ready outputs for risk, vulnerability and resilience.

Indicative approach:

- Initiation and scoping
    - Confirm the risk and resilience questions in scope (e.g. operational resilience, CNI disruption, systemic supply-chain risk, climate hazards, cyber-physical scenarios, regulatory stress tests) and success criteria (tolerances, impact thresholds, recovery objectives, regulatory tests, time horizons).
    - Agree the systems, assets, services, supply chains, geographies and stakeholder groups in scope, plus cadence of sessions, data access and approvals.
- Discovery and data gathering
    - Run structured workshops with risk, resilience, operations, security, continuity and finance teams to map systems, interdependencies, threat surfaces, controls, vulnerabilities and constraints using Skyral's Simulation Scaffold Framework.
    - Ingest and review existing risk registers, resilience and continuity plans, incident and outage reports, supplier and asset inventories, hazard/threat assessments and relevant models or dashboards.
- Modelling and prioritisation
    - Build high-level causal and probabilistic risk models describing how hazards, failures, threats and controls interact across assets, services, processes, people and external conditions, including how disruptions propagate and cascade.
    - Apply heuristics and quantitative reasoning to rank risk levers, scenarios and resilience initiatives by impact, likelihood, feasibility, time-to-value and regulatory/materiality relevance, highlighting those best suited to simulation and digital-twin work.
- Playback and refinement



    - Test interim narratives, risk-lever lists and metric frameworks with stakeholders and, where appropriate, assurance or regulatory functions; refine assumptions, levers and scenarios based on feedback.
- Final outputs and transition
    - Deliver the risk and resilience decision narrative, prioritised risk levers, scenarios and initiatives, risk and resilience metric framework, high-level risk model and follow-on delivery plan, including options for Skyral Modelling and Simulation Development as a Service (Risk & Resilience Edition) and full risk/resilience digital-twin programmes.

9. Configuration, customisation and integration

This service is primarily a consulting and decision-support engagement configured around the customer's specific risk, vulnerability and resilience context.

Configuration and customisation:

- Tailoring of workshops, problem decomposition and logic trees to the sectors, systems and risk domains in scope (e.g. CNI networks, supply chains, critical services, data centres, customer operations, cross-sector dependencies).
- Custom definition of risk and resilience metrics, levers and scenarios aligned with the organisation's risk appetite, regulatory tests, resilience objectives and stakeholder expectations.
- Adaptation of high-level causal and probabilistic models to reflect customer-specific assets, processes, interdependencies, controls, threat profiles and hazard layers.

Integration (lightweight in this service):

- Use of exports and artefacts from existing BI platforms, data warehouses, process-mining tools, workflow/CRM/ERP systems and planning tools (e.g. CSV extracts, reports, model outputs) as inputs, without requiring deep technical integration during this shaping engagement.
- Optional definition, within the strategic roadmap, of how future Skyral digital-twin deployments would integrate with data platforms, BI tools and operational systems to support ongoing forecasting, "what-if" analysis and optimisation

10. Service levels and performance (including availability targets)

As a time-boxed professional service rather than a 24×7 operational platform, service levels focus on delivery quality, responsiveness and agreed milestones.

Delivery cadence



- Milestones for discovery, interim findings, draft outputs and final deliverables agreed at kick-off and tracked against the one-month (or multi-phase) timeline.
- Responsiveness during the engagement
- Target response to project-related queries within the next UK business day during agreed working hours, with priority given to items that could delay workshops or governance decisions.
- Turnaround for major document/model revisions agreed upfront (for example 3–5 UK business days), dependent on the scale of change and timely customer feedback.

For any Skyral platform components temporarily used (e.g. to host interactive mobility or infrastructure scenario views), operational characteristics will follow the underlying Skyral CORE / SPORE practices in secure cloud or data-centre environments, but formal numerical availability SLAs are normally attached to ongoing managed services, not this shaping engagement.

11. Support model and service desk (hours, channels, response/resolve targets)

Given this is a time-boxed professional service rather than a 24×7 managed platform, service levels focus on delivery quality, responsiveness and agreed milestones rather than system uptime. Support is delivered by the named Skyral engagement team, reflecting the security-sensitive and mission-critical nature of defence work.

For any supporting Skyral platform components temporarily used to host interactive scenario views, target availability would generally follow the underlying Skyral CORE / SPORE operational practices in secure cloud or data-centre environments, but formal availability SLAs are normally attached to ongoing platform services rather than this shaping engagement.

Support for this service is primarily delivered by the assigned Skyral engagement team (SME, Applied Scientist, Product Owner) rather than a generic helpdesk

12. Security model and accreditations (including any ISO, Cyber Essentials, data protection)

Skyral’s approach to security is built around secure-by-design engineering, cloud-neutral deployment via SPORE, and formal certifications.

Security model:

- Support for deployment into secure cloud, on-premises data centres and sovereign or air-gapped environments, with consistent operational, monitoring and governance controls through Skyral’s SPORE layer.



- Role-based access and governance mechanisms across Skyral CORE components (Content Catalogue, Scenario Service, Orchestrator, Data Plane, Lens) to ensure that models, scenarios and outputs are controlled, auditable and appropriately segmented.
- Design and operation aligned to data-protection and information-assurance principles relevant to defence, national security and regulated sectors.
- Proven operation up to SECRET for UK MOD applications, with teams that include staff holding SC and DV clearances where required by the customer and contract.

Accreditations and standards (as provided):

- Cyber Essentials and Cyber Essentials Plus – Skyral holds both certifications. Verified by user; to be evidenced with current certificates on request.
- ISO 9001 – Skyral holds certification for quality management. Verified by user; to be evidenced with current certificates on request.
- ISO 27001 – Skyral holds certification for information security management. Verified by user; to be evidenced with current certificates on request.

Data protection:

- Operational or personal data used in this service is limited to what is necessary for analysis and scenario framing, with anonymisation, aggregation, masking or synthetic data used where appropriate to reduce sensitivity.
- Any processing of personal data follows applicable UK data-protection legislation, with roles and responsibilities defined in the underlying contract or data-processing agreement.

13. Data management (location, retention, backup, restore, portability)

Data used in this service typically includes: incident and loss data, asset and process inventories, hazard and threat datasets, capacity and performance metrics, supplier and logistics information and derived modelling artefacts.

Location:

- Skyral can operate in the cloud, on-premises or sovereign environments using SPORE, enabling deployment of modelling and decision-support components in regions or infrastructures that align with customer and regulatory requirements.
- For this one-month engagement, data and artefacts are usually stored in Skyral's secure collaboration and modelling environments, or in customer-hosted repositories where preferred.



Retention and backup:

- Working data and artefacts (models, narratives, roadmaps) are retained for at least the duration of the engagement plus an agreed period (e.g. 6–12 months) to support follow-on work, unless customer policies require earlier deletion.
- Underlying platforms used by Skyral provide standard backup and resilience capabilities for the environments in which they are deployed; recovery time objectives (RTO/RPO) are normally defined at the platform or managed-service level rather than for this shaping service.

Portability and export:

- Final outputs (documents, diagrams, models at appropriate granularity) are provided in commonly used formats (e.g. Office formats, PDFs, and where possible, model exports or structured configuration/parameter sets) to facilitate reuse by the customer and partners.
- On request, Skyral will support reasonable data export and documentation of model structures to aid internalisation or third-party uptake, subject to licensing and IP terms.

14. Business continuity and disaster recovery approach

- For this service, business continuity focuses on ensuring the engagement can proceed and deliver its outputs despite issues affecting personnel, tools or hosting environments.
- Formal DR metrics (RTO/RPO) and continuity obligations are normally associated with ongoing managed services, and would be detailed in platform-level or enterprise agreements rather than this shaping engagement.

15. Service usage limits and constraints

This is a scoped, time-boxed decision-support engagement focused on business optimisation, not an open-ended modelling or managed-service arrangement.

Typical limits and constraints:

- Duration and scope: designed around an approximately one-month effort; more complex groups, multi-region footprints or multi-line portfolios may require multi-phase scoping and delivery.
- Breadth vs depth: emphasis on high-value problem framing, causal/probabilistic modelling and prioritisation of initiatives and levers, rather than building fully detailed, production-grade digital twins of every process, product and geography.
- Model fidelity: models produced are high-level business decision scaffolds suitable for decision-support, stress-testing and roadmap definition; detailed



operational or engineering models are developed as follow-on Skyral Modelling and Simulation Development as a Service or digital-twin programmes.
- Data availability: where data is limited or incomplete, outputs include clearly labelled assumptions and caveats, and some quantitative results may be directional rather than exact.

16. Pricing model and units (linking to framework pricing rules)

The pricing model for this service is a fixed-scope, time-boxed engagement, with options to extend into further phases through follow-on engagements (such as Skyral Synthetic Development Services).

Core structure:

- Core one-month engagement priced as a fixed-price package based on defined deliverables (decision narrative, prioritised initiatives, KPI framework, high-level model, roadmap) and agreed stakeholder footprint.
- Extensions or additional phases (e.g. extra domain deep-dives, expanded stakeholder scope, additional scenario families) priced either as additional fixed-price work packages or time-and-materials under the relevant framework rate card.
- Any subsequent Skyral Modelling and Simulation Development as a Service or digital-twin deployment would be priced separately, reflecting model build effort, platform usage and, where relevant, managed-service components.
- Exact pricing, units (e.g. person-days, work packages) and linkage to framework pricing rules are defined in the commercial schedule.

17. Change management (how changes to scope or volumes are handled)

Change management is designed to protect outcome quality while accommodating evolving questions in complex risk and resilience environments.

- Initial scoping defines the in-scope systems, services, assets, geographies, threats/hazards, stakeholder groups, indicative datasets and planned workshops/playbacks.
- Material changes (e.g. adding additional systems or geographies, introducing significant new regulatory or hazard scenarios, or requiring deeper technical integration with operational systems) trigger a joint impact assessment on timelines, effort and deliverables.
- Minor adjustments (e.g. refining metrics, adjusting prioritisation criteria, adding closely related scenarios) are handled within the existing scope where feasible, with impacts recorded in an engagement log.



- Larger changes require a formal change note or contract variation, which may introduce additional work packages, adjusted timelines and revised commercial terms (price, units or rate-card usage).

CORE's governance mechanisms make it straightforward to track which models, content and scenarios are affected by scope changes.

18. Exit and offboarding (including data export and handover)

Exit deliverables and handover:

- Provision of final deliverables in agreed formats, including decision narrative, visual driver/lever maps, prioritised initiatives, KPI framework, high-level model description and roadmap.
- Walkthrough session(s) to explain the outputs, underlying assumptions, and how they can be used to inform architecture, planning and operational decisions, as well as the path into digital-twin build-out.
- On request, export of relevant configuration or model artefacts (e.g. scenario definitions, parameter sets, simplified model structures) in documented form, to support internal teams or partner organisations.

Data and environment offboarding:

- Removal or anonymisation of customer-specific data from Skyral environments in line with contractual data-retention terms and any customer-specific security requirements.
- Termination of access for customer users to any temporary, Skyral-hosted interactive scenario views unless explicitly agreed as part of ongoing services

19. Key assumptions and exclusions

Key assumptions:

- The customer provides timely access to stakeholders and data sufficient to meet the agreed timeline and deliverables.
- The primary goal is decision-support, strategy and prioritisation across risk, vulnerability and resilience, rather than full production implementation or detailed design of all controls and systems.
- Initial models and scenarios are used to compare options, highlight trade-offs and stress-test strategies rather than to produce exact forecasts at every product, process or site level.



Key exclusions (unless explicitly added to scope):

- Full-scale, production-grade risk and resilience digital-twin implementation and ongoing integration with live operational systems (e.g. core operational platforms, risk engines, incident management systems), which are covered by subsequent Skyral Modelling and Simulation Development as a Service and platform services.
- Detailed vendor-specific configuration or custom development of operational or risk systems, low-level engineering tasks or direct changes to production environments.
- 24×7 operational support, incident management and availability SLAs typical of managed operational platforms.
- Formal regulatory submissions, statutory reports or audit opinions; Skyral's outputs can inform such work but do not replace formal assurance or regulatory processes.

20. Related services and optional add-ons

Related Skyral services:

- Skyral Modelling and Simulation Development as a Service (Risk & Resilience Edition) – builds detailed risk and resilience digital twins and agent-based models aligned to the prioritised levers and scenarios from this engagement, enabling ongoing stress testing, "what-if" analysis and resilience planning.
- Skyral Modelling and Simulation Development as a Service (Business Optimisation) – builds detailed, business-focused digital twins and agent-based models aligned to the prioritised levers and scenarios from this engagement, enabling ongoing "what-if" analysis and optimisation.
- Skyral Modelling and Simulation Development as a Service (Defence and National Security) – builds detailed mission and theatre-level synthetic environments and digital twins aligned to the prioritised mission threads, levers and scenarios from this engagement.
- Skyral Modelling and Simulation Development as a Service (Health) – builds detailed health-system digital twins and agent-based models aligned to the prioritised levers and scenarios from this engagement, enabling ongoing "what-if" analysis, optimisation and operational decision-support.
- Skyral Modelling and Simulation Development as a Service (Mobility & Infrastructure) – builds detailed digital twins and agent-based models of cities, corridors, ports, airports, logistics networks and interdependent infrastructures, aligned to the prioritised levers and scenarios from this engagement.
- Skyral Modelling and Simulation Development as a Service (Network Edition): builds detailed network digital twins and agent-based models aligned to the prioritised levers and scenarios identified in this engagement.



- Mission Planning & Decision Support services for defence and national security, using large-scale agent-based modelling to explore courses of action, logistics and resilience across multi-domain operations.
- Health Policy & Programme Strategy simulation services, applying similar techniques to patient flows, resource allocation and intervention strategies for health systems.

Optional add-ons to this specific service:

- Additional deep-dive modules on specific risk domains or systems (e.g. particular supply chains, critical facilities, regions, customer-facing services or technology stacks), delivered either as extended discovery within this service or as Skyral Advisory/Synthetics Development phases depending on need.
- Rapid proof-of-concept risk and resilience digital-twin instances (e.g. for a specific asset network, region or supply chain) using existing data and synthetic agents to demonstrate interactive scenario analysis and resilience testing beyond the initial decision narrative, delivered via Skyral CORE and Modelling and Simulation Development as a Service.
- Extended roadmap, business-case and regulatory-engagement support, including structured inputs to investment cases, resilience plans and regulatory submissions that depend on robust risk and resilience evidence.

21. Contact, account management and reporting

- E. enquiries@skyral.io
- W. www.skyral.io