WINTERSMITH ADVISORY LLC
Elevating Systems. Enhancing Performance.

Service Description: Enterprise Risk Management

DOC-140 Process Diagram - Enterprise Risk Management

1. Overview

Purpose:
This service delivers end-to-end expertise in holistic enterprise risk management. It is designed to help organizations integrate risk governance across operational and strategic areas, ensuring a comprehensive approach to identifying, prioritizing, and mitigating risks. This proactive management of risks not only enhances operational resilience but also supports strategic planning and continuous improvement.

Scope:
The service is ideal for mid-to-large enterprises across various industries that require an integrated risk strategy. It caters to organizations looking to implement or enhance risk frameworks such as COSO and ISO 31000, with a particular focus on establishing robust internal risk governance structures.

Key Benefits:

- Holistic risk management addressing both operational and strategic risks
- Proactive risk identification and prioritization, reducing potential disruptions
- Implementation of standardized risk assessment tools and ongoing monitoring
- Integration of risk management with strategic planning, driving continuous improvement
- Enhanced stakeholder engagement and confidence through transparent governance

---

2. Service Objectives

- **Goals:** Establish and implement an enterprise-wide risk governance framework within a defined timeframe (e.g., to enhance risk maturity across business units by 25% over 12 months).
- **Target Outcomes:**
  - Delivery of comprehensive risk assessments and prioritized risk registers
  - Provision of detailed risk mitigation strategies and integration plans
  - Standardized risk indicators and dashboard reporting tools to enable continuous monitoring

3. Service Scope and Components

Inclusions:

- Initial risk governance framework design and stakeholder alignment sessions
- Comprehensive risk identification and prioritization workshops
- Development of risk indicators, registers, and tailored assessment tools
- Integration of risk management practices into strategic planning processes
- Ongoing monitoring, reporting, and continuous improvement cycles
- Training and capacity building sessions in ERM best practices, including COSO and ISO 31000 frameworks

Exclusions:

- External regulatory audit services not directly related to risk management
- Post-implementation operational audits beyond the continuous improvement phase

4. Process Overview

- **Step 1: Initiation & Stakeholder Engagement**
    - Define the service scope and establish clear risk management objectives.
    - Identify key internal and external stakeholders and assign governance roles.
- **Step 2: Comprehensive Risk Identification & Prioritization**
    - Conduct baseline assessments to capture current risk exposure.
    - Identify and rank both operational and strategic risks based on impact and likelihood.
- **Step 3: Development of Risk Indicators & Registers**
    - Create standardized risk assessment tools and risk registers tailored to industry needs.
    - Establish key performance indicators for ongoing risk monitoring.
- **Step 4: Integration with Strategic Planning**
    - Embed risk management strategies into overall business planning and decision-making processes.
    - Develop a cohesive plan that leverages risk insights for performance improvement.
- **Step 5: Implementation & Training**
    - Execute the risk framework across business units with dedicated training and workshops.
    - Roll out standardized tools and processes to ensure consistent application across the enterprise.

- **Step 6: Monitoring, Reporting & Communication**
  - Implement regular reporting mechanisms to track risk status and performance metrics.
  - Engage stakeholders through transparent communication channels and management reviews.
- **Step 7: Continuous Improvement & Re-evaluation**
  - Regularly revisit risk frameworks and update strategies based on feedback and evolving threats.
  - Ensure the system remains agile and aligned with both operational and strategic objectives.

5. Key Outputs & Deliverables

- Comprehensive Risk Governance Framework document
- Detailed Risk Assessments and prioritized Risk Register reports
- Standardized risk indicators and real-time monitoring dashboards
- Customized risk assessment tools and templates
- Training materials, workshop guides, and capacity building documentation
- Final service report outlining implemented processes, lessons learned, and recommendations for continuous improvement

6. Roles and Responsibilities

Describe the roles of internal teams and client stakeholders.

- **Service Manager/Project Lead:** Direct overall service delivery, manage timelines, and oversee resource allocation.
- **Risk Consulting/Implementation Team:** Conduct risk assessments, develop documentation, lead training, and ensure implementation of risk controls.
- **Quality Assurance and Audit Experts:** Monitor risk management practices, ensure compliance with standards, and validate deliverables.
- **Client Stakeholders:** Provide organizational insights, review deliverables, and ensure alignment with internal risk management goals.

7. Performance Metrics & Success Factors

- **KPIs:**

- ○ Achievement of risk management milestones within defined timeframes
- ○ Reduction in risk incidents and cost exposure
- ○ Improvement in stakeholder satisfaction scores regarding risk governance
- ○ Measurable increases in risk awareness and mitigation effectiveness
- **Success Factors:**
  - ○ Clarity in service scope and seamless stakeholder alignment
  - ○ Robust and integrated risk management practices
  - ○ Timely communication and comprehensive reporting
  - ○ Continuous training and professional development in risk management best practices

---

8. Supporting Systems and Resources

- **Technology Platforms:** Use of risk management software, dashboard reporting tools, and secure document repositories
- **Templates & Checklists:** Customized risk assessment, risk register, and gap analysis templates
- **Training Modules:** Internal and externally curated workshops focusing on ERM methodologies (e.g., COSO, ISO 31000)

---

9. Contact Information

Contact details for further inquiries about the service:

Service Manager: Alex Lackey, alex.lackey@wintersmithadvisory.com, 801-558-3928