redesign

SERVICE BRIEF

Cyber Risk Assessment

Aligned to the NIST Risk Management Framework

re

This document outlines the scope, deliverables, responsibilities, and terms governing Redesign's Cyber Risk Assessment services. The Cyber Risk Assessment service is designed to help organizations identify, assess, and manage risks to information systems and operations in alignment with the NIST Risk Management Framework (RMF).

This service provides a structured approach to assess threats, vulnerabilities, and impacts, and to develop actionable recommendations for risk treatment.

This service engagement is governed by this Service Brief and associated with SKU: SEC-RISK-GAP. The quantity defined in the quote reflects the number of business units, environments, or assessment domains to be evaluated during this engagement.

The FUTURE BELONGS
to the CURIOUS.

Table of Contents

01. Services Overview

The Cyber Risk Assessment service is designed to help organizations identify, assess, and manage risks to information systems and operations in alignment with the NIST Risk Management Framework (RMF).

This service provides a structured approach to assess threats, vulnerabilities, and impacts, and to develop actionable recommendations for risk treatment. By applying NIST RMF's tiered approach—spanning organizational, business process, and information system levels—this engagement ensures that security decisions are risk-informed and traceable to mission objectives.

02. Offer Structure

PRIMARY SERVICES

- Scoping of assets and processes, assess business/regulatory context, and assign impact levels.
- Evaluation of current practices, policies, and technology controls
- Stakeholder interviews and evidence review
- Assign likelihood/impact scores, produce risk register, and propose treatment actions
- Risk-prioritized remediation recommendations

OPTIONAL ADD-ONS

Separate SOW

- Remediation roadmap development
- Control documentation or policy creation
- Business Impact Analysis
- Board-level or executive briefing

03. Project Scope

The engagement is scoped to a defined number of domains (e.g., business units, cloud environments, data centers, or subsidiaries). Redesign will assess each environment's risk and provide recommendations based on observed control maturity and risk.

Risk Assessment:

- **Covers risk assessment based on NIST Risk Management Framework across Tier 1 (Organization), Tier 2 (Processes), and Tier 3 (Systems), based on company maturity**

---

04. Quantity & Effort Model

- **Service SKU: SEC-RISK-GAP**
- **Quantity: Number 3 of distinct domains or business environments evaluated**
- **Work per Unit Includes:**
  - One risk assessment for an entity entity (e.g., business unit, cloud platform, data center, site)

EXAMPLE

A quantity of 3 may include assessments of 3 separate lines of businesses with different systems, tools and applications, or a system specific risk assessment eg O365 environment.

COMPANY SIZE	?	?	DEPARTMENT	LOE HOURS
Small (<250)	1-3	25 each	1-10	40
Medium (250-2000)	1-3	40 each	1-10	80
Large Enterprise (2000+)	1-3	80 each	1-10	150

05. Services & Key Activities

Stage	Key Activities
Prepare & Categorize	▪ Define scope, assumptions, constraints associated with assessment ▪ Identify sources of information ▪ Identify assets and processes, assess business/regulatory context ▪ Identify risk model and analytic approachs
Conduct Risk Assessment	▪ Interview stateholders and gather information ▪ Identify threat sources and events ▪ Identify Vulnerabilities ▪ Determine likelihood and Impact ▪ Determine Risk
Communiate and Share	▪ Determine appropriate method for executive briefing ▪ Share risk assessment report
Maintain Risk Assessment	▪ Build risk register for ongoing maintainance

06. Deliverables

Risk Assessment Report

Risk Register

Knowledge Transfer Session (virtual, 1 hour)

07. Services Scope Changes

Changes to the number of environments, business units or sites may require a revised quote or separate SOW.

08. Services Scope Exclusions

This engagement does not include:

- **Implementation of missing controls or configurations**
- **Compliance certification or attestation**
- **Vulnerability assessment**
- **Technical penetration testing (available separately)**
- **Continuous control monitoring or managed services**

09. Customer Responsibilities

- **Provide access to relevant documentation and system overviews**
- **Designate technical and business stakeholders for interviews**
- **Grant permission for review of applicable logs, screenshots, or reports**
- **Approve scope boundaries and target framework prior to kickoff**
- **Review draft deliverables and confirm feedback**

10. Services Schedule

- **Start Date:**
  Upon signed quote and stakeholder availability
- **Completion:**
  Final deliverables submitted and DocuSign approval by customer

---

11. Terms and Conditions

This engagement will be governed by the Seller's terms and conditions located at:

SERVICES WILL NOT BEGIN UNTIL THE FOLLOWING PREREQUISITES ARE MET

- Signed quote referencing SKU: SEC-RISK-GAP and quantity
- Assessment framework and scope confirmed
- Stakeholders assigned and documentation shared

Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

redesign

The FUTURE BELONGS
to the CURIOUS.