LUMEN®

Lumen Service Guide

Cybersecurity Consulting Retainer Service

Updated: May 30, 2024

This Lumen Service Guide ("SG") sets forth the description of each of the Service Focus Areas available, including technical details and additional requirements or terms. "Lumen" is defined as CenturyLink Communications, LLC d/b/a Lumen Technologies Group or its affiliated entities. This Service Guide is subject to and incorporated into the Solution Service Order ("SSO") for Cybersecurity Consulting Retainer Services.

Lumen may re-label, substitute, and/or add new service activities at any time, including during a Service Term. Requests for additional activities and/or new Service Focus Areas may require a Change Request. Lumen may from time to time remove existing activities and/or new Service Focus Areas. For removing an existing activity or existing add-on services, Lumen will provide notice at least 60 days prior to the end of the current Service Term and changes will take effect at the conclusion of the Service Term.

Service Focus Areas. The available activities are general, on-going objectives and are not a finite, exhaustive list of available activities. Customers can request additional related activities, which may be included in the scope of Customer's engagement at Lumen's discretion.

Cybersecurity Policy Review and Recommendations. Typical activities include:

- Collect and assess policies, procedures, compliance requirements, and governance frameworks provided by Customer.
- Perform an initial assessment to understand the structure, comprehensiveness, and alignment of existing policies with Customer's organizational goals.
- Benchmark Customer's policies against industry best practices, relevant standards (e.g., ISO/IEC 27001, NIST), and Customer's stated regulatory requirements and perform a gap analysis.
- Conduct interviews and workshops with key stakeholders identified by Customer ("Stakeholders") from various departments (e.g., IT, legal, HR) to gather insights into Customer's policy implementation, change control, and adherence to those processes.
- Develop recommendations for updating existing or creating new policies.
- Prioritize recommendations based on risk tolerance, regulatory urgency, and operational impacts.
- Present draft recommendations to Stakeholders for feedback.
- Refine recommendations based on Stakeholder input to validate alignment with Customer's organizational capabilities and culture.
- Document findings, gap analysis, and recommendations.
- Develop an implementation roadmap that outlines steps, timelines, responsibilities, and resources required by Customer to implement the recommendations.
- Provide tactical short-term recommendations and strategic long-term adjustments designed to enhance Customer's cybersecurity posture, build momentum, and enable sustainable improvements.
- Recommend training and awareness programs.
- Advise on establishing mechanisms for ongoing monitoring of policy adherence and effectiveness.
- Recommend a process that enables Customer to regularly review and update security policies to adapt to new threats, technologies, and business changes.

Example Document Deliverable: Security Policy Review Report

Cybersecurity Policy Development. Typical activities include:

- Evaluate Customer's current cybersecurity posture and policy landscape.
- Gather Customer's business objectives and align cybersecurity policy objectives accordingly.
- Identify and engage with key Stakeholders across different departments (e.g. IT, HR) to understand cybersecurity goals, concerns, and expectations.
- Facilitate workshops or meetings to discuss and define Customer's future security policy goals and priorities.
- Develop a structured cybersecurity policy framework that outlines the scope, responsibilities, and governance structure.
- Define policy categories (e.g., access control, acceptable use, incident response, data protection).
- Draft actionable policies for each identified category that are consumable by all Stakeholders, not just IT personnel.
- Review drafted policies with Stakeholders for feedback and validation.
- Adjust policies based on Customer feedback to validate practicality and enforceability within Customer's organization.
- Develop an implementation plan that outlines how policies can be communicated, enforced, and integrated into Customer's existing business processes.
- Identify and communicate necessary training and awareness programs to support policy adoption.
- Update policies to reflect changes in the cybersecurity landscape, Customer's regulatory requirements, and Customer's organizational objectives.

Example Document Deliverable: Cybersecurity Policy Development Document

Compliance Advisory. Typical activities include:

- Aid Customer's understanding of compliance requirements associated with cybersecurity frameworks relevant to Customer's organization.
- Provide coaching to Stakeholders responsible for conducting compliance audits and gap analyses.
- Assist Customer with developing reports and documentation related to Customer's compliance requirements.
- Provide guidance on compliance best practices.
- Create materials and conduct Customer training sessions on security compliance topics.
- Monitor regulatory developments potentially impacting Customer's cybersecurity program.
- Assist Customer in risk assessment and management processes.

Example Document Deliverable: Compliance Advisory Report

Cybersecurity Governance Consulting. Typical activities include:
- Engage Stakeholders to understand their perspectives, challenges, and expectations regarding cybersecurity governance.
- Assess Customer's existing cybersecurity governance structures and processes to identify strengths, weaknesses, and gaps.
- Identify and assess the regulatory and compliance requirements which are, in Lumen's reasonable belief, relevant to Customer's industry and geography of operations.
- Design a cybersecurity governance framework that includes Customer organizational roles, responsibilities, decision-making processes, and reporting structures.
- Validate that the framework supports oversight, accountability, and communication across all levels of the organization.
- Develop or update cybersecurity policies and procedures that support the Customer's governance framework and compliance requirements.
- Develop an implementation plan that the Customer may leverage for the new governance framework, including timelines, resource allocation, and change management strategies.
- Facilitate Customer's adoption of the governance framework by supporting communication, training, and implementation activities.
- Advise on metrics and key performance indicators (KPIs) for Customer to measure the effectiveness of the cybersecurity governance framework.
- Develop reporting processes and documents Customer may leverage to regularly communicate the status of cybersecurity initiatives, risks, and compliance to Stakeholders and executive leadership.
- Recommend a continuous improvement process for the cybersecurity governance framework, including regular reviews and updates based on Customer's changing business needs, emerging threats, and regulatory requirements.
- Engage in benchmarking and best practice reviews to support alignment between Customer's governance framework and industry standards.

Example Document Deliverable: Cybersecurity Governance Framework Document

Security Awareness Program Development. Typical activities include:
- Conduct training needs analysis and customize training programs (topics, forums, Stakeholders, content).
- Develop and deliver workshop or seminar-style cybersecurity training content intended for a wide audience or tailored to specific resource groups, as determined by Customer.
- Develop security awareness materials.
- Support Customer's customization of existing e-learning platform or online training modules.
- Conduct surveys and interviews to measure and report upon improvements to Customer's security awareness program.
- Provide Customer with updates regarding current cybersecurity industry trends and threats.
- Provide one-on-one coaching on cybersecurity best practices.
- Facilitate cybersecurity awareness events and activities.

Example Document Deliverable: Security Awareness Training Program Plan

Data Protection and Privacy Consulting. Typical activities include:
- Provide guidance, consultation, and support with Customer's:
  - Data protection and privacy-by-design strategies.
  - Data protection strategy implementation.
  - Data Protection Impact Assessments (DPIAs) and related processes.
- Develop and update Customer's privacy policies and procedures.
- Coordinate with Customer on data protection activities.
- Facilitate Customer training sessions regarding data privacy and protection.
- Support the assessment of Customer's data processing activities for adherence to compliance requirements.

Example Document Deliverable: Data Protection and Privacy Best Practices Guide

Cybersecurity Strategy Formulation. Typical activities include:
- Collaborate with Customer's senior leadership to understand business goals, objectives, and strategic priorities, and advise on how cybersecurity can support and further enable each.
- Discuss Customer's current cybersecurity posture, including preventative technologies, policies, processes, and capabilities.

- Identify Customer's strengths, weaknesses, opportunities, and threats through SWOT analysis or similar frameworks.
- Analyze the current and emerging threat landscape specific to Customer's organization and industry.
- Review applicable regulatory and compliance requirements that impact Customer's cybersecurity strategy.
- Determine if Customer's current cybersecurity strategy incorporates necessary controls and processes to meet these requirements or has gaps.
- Identify and engage with Stakeholders to gather input and build consensus around the cybersecurity strategy.
- Support the development of a communication plan to keep Stakeholders informed and involved in the strategy development process.
- Recommend architectural improvements or technology investments to support Customer's cybersecurity strategy and/or develop a detailed cybersecurity document that outlines goals, objectives, priorities, initiatives, and performance metrics and incorporates NIST industry best practices and Lumen's recommendations.
- Create an implementation plan for the established cybersecurity strategy that Customer may leverage, including project plans, resource allocation, and timelines.
- Identify short and long-term projects to balance immediate impact with sustainable improvements.
- Recommend metrics and KPIs to measure the effectiveness of the established cybersecurity strategy.
- Develop a plan for Customer's regular reviews of the strategy to adapt to new threats, business changes, and technological advancements. Customer has the option for Lumen to coordinate and conduct the regular reviews with the Advanced and Premium Service Tiers.

Example Document Deliverable: Cybersecurity Strategy Report

Technology Trend Analysis and Forecasting. Typical activities include:
- Collaborate with Customer to understand its specific industry, existing technology landscape, strategic objectives, and areas of interest.
- Identify key technologies currently in use and assess their maturity levels, benefits, and limitations.
- Conduct and provide research related to emerging technologies and trends in technology that may impact Customer's cybersecurity posture.
- Evaluate the drivers behind these trends, including economic, social, regulatory, and environmental factors.
- Assess the potential impact of identified technology trends on Customer's business model, operations, end customer experience, and competitive landscape.
- Forecast the future trajectory of key technology trends relevant to Customer, including potential timelines for development and market adoption.
- Develop recommendations that inform Customer's decision making when responding to identified technology trends.
- Conduct a risk analysis for Customer's adoption of new technologies, considering factors such as cost, integration challenges, and security implications.
- Provide Customer with recommendations for adopting new technologies, mitigating risks when doing so, or pursuing new innovation opportunities.
- Suggest key indicators of change that trigger Customer's review of the technology strategy. These indicators can include changes in the market, such as new competitors or shifts in customer demand, as well as changes within Customer's organization, such as the introduction of new technologies or changes in leadership.
- Prepare reports and presentations to communicate the findings, forecasts, and recommendations to Customer's senior management and other Stakeholders.

Example Document Deliverable: Cybersecurity Trends Analysis Report

Board and Executive Cybersecurity Advisory. Typical activities include:
- Provide an overview of the current cybersecurity landscape, including prevalent threats, trends, and regulatory changes.
- Evaluate Customer's current cybersecurity measures, policies, and risk management practices.
- Identify gaps and areas for improvement within Customer's existing cybersecurity framework.
- Explain the potential impact of the identified gaps on the Customer's organization.
- Advise on risk assessment methodologies, risk prioritization, and risk mitigation strategies.
- Review and advise on Customer's cybersecurity governance structure, including roles, responsibilities, and reporting lines.
- Provide guidance related to Customer's compliance with relevant cybersecurity regulations and standards (e.g., GDPR, CCPA, ISO 27001).
- Advise on the allocation of resources and investments in cybersecurity and align with Customer's risk profile and strategic priorities.
- Provide methods Customer may leverage to measure return on cybersecurity investments.
- Recommend strategies to promote a culture of cybersecurity awareness throughout Customer's organization.
- Recommend cybersecurity training programs for Customer's workforce.
- Provide insights into how emerging technologies (e.g., AI, blockchain) could impact Customer's cybersecurity strategy.
- Advise on incorporating security by design in digital transformation and other innovation initiatives to Customer's business processes.
- Recommend strategies for conducting security assessments and monitoring third-party risk.
- Develop cybersecurity performance reporting frameworks and metrics for Customer's executive management.
- Advise on communicating cybersecurity risks and initiatives to Stakeholders in an understandable and consistent manner.
- Provide tailored training sessions on cybersecurity topics, trends, and best practices.

- Enhance Customer's understanding of cyber risks and their specific roles in cybersecurity governance.
- Assist in the strategic planning process to validate that cybersecurity is considered in long-term business planning and digital transformation efforts.

Example Document Deliverable: Executive Cybersecurity Briefing Document

Incident Response Strategy Consulting. Typical activities include:
- Assess Customer's current incident response capabilities, including processes, tools, and team expertise.
- Identify the types of cybersecurity risks and threats that organizations similar to Customer commonly incur.
- Identify and engage with key Stakeholders to understand expectations, concerns, and requirements for incident response.
- Assess the degree to which Customer's business objectives and incident response strategies align.
- Review Customer's existing incident response policies and plans to identify gaps and areas for improvement.
- Benchmark against industry best practices and Customer's compliance requirements.
- Review and incorporate Customer's regulatory requirements related to incident response.
- Support the development or updating of Customer's incident response plan, including clear procedures for detection, analysis, containment, eradication, recovery, and post-incident activities.
- Define roles and responsibilities for Customer's incident response team and other key Stakeholders.
- Develop protocols, templates, and guidelines that Customer may leverage to communicate and coordinate with internal Stakeholders, end customers, third-party vendors, law enforcement, and other external entities during and after a cybersecurity incident.
- Assess Customer's existing incident response tools and technologies and make recommendations designed to enhance Customer's incident detection, analysis, and response capabilities.
- Support Customer's integration of the incident response strategy to its business continuity and disaster recovery plans, as applicable.
- Provide chain of custody process guidance for evidence collection and preservation.
- Evaluate Customer's need for external incident response services and forensic experts.
- Establish a process for regular review and updating of Customer's incident response strategy and plan to adapt to evolving threats, technologies, and business changes. Customer has the option for Lumen to coordinate and conduct the regular reviews with the Advanced and Premium Service Tiers.
- Recommend metrics Customer may leverage to measure the effectiveness and efficiency of incident response activities.
- Develop reporting templates Customer may leverage to inform executive management and key Stakeholders about incident response readiness and past incident outcomes.

Example Document Deliverable: Incident Response Strategy Guide