SERVICES

MANAGEMENT *(IT AND BUSINESS CONSULTING)*

Technology is changing faster every day – companies are looking to hire someone today with an expectation this person will be an expert tomorrow on something that doesn't yet exist but will likely be financially relied upon in the near future – an unlikely outcome. It's no longer reasonable to think an organization can feasibly expect to have the internal staff capable of managing all future technology in their enterprise; there is definitely a higher than ever need for outsourcing appropriate functions out to those with the actual expertise over hoping to maintain granular technological versatility in-house. Fortunately, one can still plan how to effectively manage the remote staff, contractors, and vendors who provide the latest cloud services and outsourced business functions, even if they don't have dedicated roles within the organization.

Privity offers management consulting services – focusing on secure operations – which help companies modernize and leverage emerging technologies in a cost-effective manner, allowing them to simultaneously future-proof processes against the inevitable accelerating changes in technology.

CATEGORIES OF SERVICE OFFERINGS

1. Cybersecurity and IT Management Consulting

Deploying a technical solution most often isn't as easy as just calling up a vendor after securing funds to pay their future invoices. In most cases, a business justification, budget planning, and confirmations of strategy alignment are all necessary to pursue before IT manager and staff can obtain senior management's approval. Other times, a company may know where they want to be with their existing information systems, but don't know how to get there. In either of these situations, they might benefit from Privity's advisory consultations.

Some of our Cybersecurity and IT Management Consulting services include:

- *Chief Information Security / Privacy Officer on Demand*
    - Respond to regulatory inquiries or complaints
    - Prioritize initiatives and communicate to the board
    - Champion or sponsor projects
    - Offer sober second thought
- *Strategy Consulting*
    - Develop mission statements, long-term goals

- Align cybersecurity goals with IT management and overall business objectives
- Prioritize responses to threats as part of a company's multiyear strategy plan

- *Cybersecurity Department Development*
  - Establish metrics for business cases to hire staff or build a department
  - Formalize roles and responsibilities
  - Define critical success factors for effectiveness

- *Business Continuity Planning*
  - Facilitate asset identification and classification / characterization
  - Conduct business impact assessments
  - Translate business requirements into technical requirements

- *Compliance Program Development*
  - Establish program requirements and securing funding
  - Formalize roles and responsibilities
  - Develop management procedures to protect assets
  - Limit scope and scope changes

- *Budget Planning*
  - Establish budgeting for projects, departments, and programs
    - ✓ CapEx
    - ✓ OpEx
    - ✓ One-time OpEx
  - Provide cost projections and contingencies

- *Training and Facilitation*
  - Create and/or provide staff security awareness training
    - ✓ Acceptable use awareness training
    - ✓ Senior executive training
    - ✓ Corporate user training
    - ✓ Field staff user training
  - Create and/or provide IT and security staff training
    - ✓ IT management program training
    - ✓ Privileged user account training
    - ✓ Third-party due diligence process training
    - ✓ Crypto-key custodian training
  - Create and/or provide regulatory and legislative compliance training
    - ✓ Privacy compliance (PIPEDA, PIPA, FOIPPA, GDPR, CCPA, etc.) for IT managers training
    - ✓ PCI DSS compliance for IT managers training

2. Cybersecurity and IT Business Analysis

Before costly IT decisions can be made, thorough and detailed analysis ought to occur to ensure the best course of action has been taken and that all requirements are met. Business analysis has become more and more important as the role of IT continues to evolve from managing technology to managing processes. Ensuring that IT business analysis includes all the necessary cybersecurity and compliance considerations is critical to a successful project.

Some of our Cybersecurity and IT Business Analysis services include:

- *Business Plan / Business Case Development*
    - Provide business justification of costs and expenditures for projects, departments, and programs
        - ✓ Net Present Value
        - ✓ Total Cost of Ownership
        - ✓ Return on Investment
    - Develop formal documents for executive approval
    - Define functional and non-functional requirements
    - Compare solutions
    - Detail CapEx, OpEx, and one-time OpEx
    - Provide cost justifications
- *Gap Analysis*
    - Conduct root-cause analyses
    - Map compliance issues to management programs
- *Cost-Benefit Analysis*
    - Analyze cost of controls vs. expected impact
    - Consider ROI, TCO, DCF, etc.
- *Business Impact Analysis (BIA)*
    - Measure criticality impact on business
    - Determine recovery time and point objectives (RTO/RPO)
- *Privacy Impact Analysis (PIA)*
    - Measure the impact of change on privacy program compliance
- *Compliance Impact Analysis*
    - Analyze technical scope changes and their impact on:
        - ✓ Managerial procedures
        - ✓ PCI DSS
        - ✓ Business processes

3. Cybersecurity and IT Project Management

Considering all of company's data and infrastructure security requirements as part of the planning process is required for the organizational security objectives to be met. Similarly, ongoing adaptation to evolving project requirements is paramount for delivering business value quickly – but how can one be sure that the necessary security and compliance requirements aren't ignored due to fast, agile development methodologies or DevOps implementations? How can one be sure that their "shift left" approach to technology doesn't shift so far past the page margin that it's entirely outside the security process?

Some of our Cybersecurity and IT Project Management services include:

- *Project Participation*
  - Participate in projects as subject matter experts (SME)
    - ✓ IT & Cybersecurity Management and Business Consulting
    - ✓ IT & Cybersecurity Business Analysis
    - ✓ Due diligence
    - ✓ Compliance scope reduction planning
    - ✓ Remediation plan development Impact assessments and analysis
    - ✓ Cloud security architecture
  - Provide project management
  - Provide project planning
  - Provide project and compliance oversight
    - ✓ Technical implementations (DevOps / DevSecOps)
    - ✓ Cybersecurity projects
    - ✓ PCI DSS
    - ✓ Privacy (GDPR, CCPA. PIPA, PIPEDA, etc.)
    - ✓ Operational Technology
    - ✓ Transition projects (lift and shift to cloud, outsourcing)
    - ✓ Transformation or modernization projects (automation)

4. Governance

As technology changes continue to occur at an increasing rate, the importance of having management processes over technology implementations becomes tantamount. Rethinking how organizational governance affects staff is essential to having an efficient security program with cost-effective controls. Documentation should not be an afterthought; organization's policies and procedures should clearly define management and staff expectations, offering unambiguous guidance without hindering progress. A strong governance structure supported by management programs that serve as its foundation is the key to running cost-effective, secure operations.

Some of our Governance services include:

- *Development*
    - Work with stakeholder to collect requirements
    - Establish governance structure
        - ✓ Mutually exclusive, collectively exhaustive structure
        - ✓ Easy to find and understand relevant content
    - Create cybersecurity and IT policies
    - Create management procedures and programs
    - Create technical standards, benchmarks, baselines
        - ✓ Hardened standards aligning with best practices like those from the Centre for Internet Security (CIS)
        - ✓ Templates or Infrastructure-as-Code documentation
    - Create and/or document existing daily operating procedures
        - ✓ "Click here, go there" level of instructions
        - ✓ E.g. build procedures, adding new users in Azure Active Directory, etc.

- *Reviews and Assessments*
    - Provide purpose-driven reviews (customer choice of scope)
    - Test against best practices, like ISO 27002, NIST CSF, NIST 800-53, etc.

  ➢ See our *Assessments (Security Audits and Assurance)* service offerings for more details

- *Implementation*
    - Orient managers and staff with new governance
    - Assess existing operations against new governance
    - Prioritize areas for operational changes
    - Work with management and staff to adopt changes
    - Provide report on progress

- *Integration with Commercial GRC platforms*
    - Implement management procedures on commercial off-the-shelf software or services, like RSA Archer, ServiceNow, or LogicGate Risk Cloud
    - Customize templates or deploy new procedures