

RISK ADVISORY SERVICES

ENTERPRISE SECURITY

THE TECHNICAL LANDSCAPE OF BOTH BUSINESS AND ENTERPRISE SECURITY ARE EVOLVING AT AN ASTRONOMICAL RATE. AS A RESULT, ORGANIZATIONS ARE REQUIRED TO ADOPT VARIOUS STANDARDS OF SECURITY CONTROLS TO PROTECT SENSITIVE DATA AND INFORMATION SYSTEMS.

In the past, slow rates of change were attributed to a focus on managing outdated security structures implemented during the early stages of enterprise security. However, options presently available allow organizations to implement cost-effective and efficient solutions that can successfully mitigate organizational risks.

The objective of enterprise security is to:

- Protect the interests of those relying on the information;
- Safeguard the systems and communications that deliver the information; and
- Ensure the integrity, confidentiality and availability of the information.

Defining, achieving, maintaining, and improving information security has also become increasingly important to sustaining and increasing an organizations' competitive edge.

Key trends in information security include:

- Integration of information security systems with overall organizational objectives
- Promoting the value of information security through compliance initiatives
- Communicating the risks associated with third party relationships to management
- An increased focus on privacy and personal data protection;
- Ensuring implemented information security systems are in tune with overall business objectives and
- Adoption of recognized standards and frameworks

The Solution

BDO's enterprise security service professionals can assist in the design and assessment of processes and controls within an organization's security chain in the following key areas of concern:

- Security strategy and planning
- Security controls and architecture (process and technology)
- Threat and vulnerability management
- Crisis and incidence response and
- Penetration testing

Our team of qualified professionals can provide a clear and concise framework to assist in the evaluation of key areas of exposure to your organization. Our phased methodology (based on the ISO 17799 / 27001 standards) will enable you to assess, control, monitor and measure your exposure in the areas of information security, privacy and confidentiality, outsourced process controls and systems reliability.

Key components of our methodology include:

Phase 01 - Information gathering: Gaining an understanding of the current state (of security) in sufficient detail to identify key infrastructure components in scope.

Phase 02 - Perform risk assessment: Assessing components in scope to understand business risks.

Phase 03 - Assess infrastructure: Conduct a detailed assessment of the infrastructure and identify vulnerabilities using the information garnered in the previous phase. This can include penetration testing, if appropriate.



CONTACT BDO

National

Sam Khoury
416 369 6030
skhoury@bdo.ca

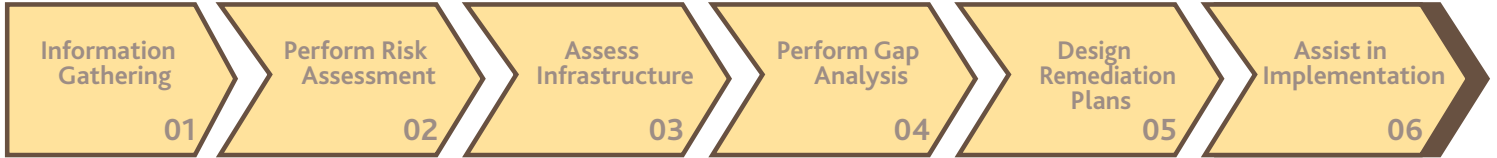
Central Canada

Carlo Mariglia
416 369 3078
cmariglia@bdo.ca

David Knott

416 815 3016
dknott@bdo.ca

ENTERPRISE SECURITY METHODOLOGY



Phase 04 - Perform gap analysis: Perform a gap analysis by comparing the results from the previous phase against generally accepted 'best practices' frameworks (ISO 17799/27001) and highlight the related risk implications of the gaps.

Phase 05 - Design remediation plans: Develop remediation plans addressing key risks identified in the previous step. These plans would outline short term enhancements and long term solutions in any gaps.

Phase 06 - Assist in implementation: Implement remediation plans and perform testing to ensure that identified gaps are appropriately addressed and risks are mitigated.

Enterprise Security Assessment

Our methodology can assist in:

- Tracing transactions through their lifecycle to identify both business process controls and system security controls
- Designing and supporting the implementation of system security controls
- Documenting and testing of key security controls
- Defining roles to ensure security supports business processes
- Reviewing access rights and authorizations for segregation of duties
- Designing and configuring authorizations and
- Aligning your organization with internationally accepted standards (ISO 17799/27001)

Technology Risk and Security

Reliance on process and control automation is on the rise. Senior management is under intense pressure to accomplish more with their current infrastructure, without increasing risk. Consequently, increased reliance on information systems outside your direct control (e.g.

Internet, ASPs, e-commerce) can lead to heightened security risks. Your organization's information technology is a strategic asset that must to be managed.

BDO's Technology Risk and Security services helps organizations realize the full value of their IT investment by ensuring IT decisions are aligned with business objectives. With our industry-proven proprietary methodologies and frameworks, our professionals will assist you in sustaining and managing your information risk exposure and reducing your IT risks in a sustainable manner.

As technology continually changes, so do the underlying risks. Some of our risk advisory services include:

- Service Auditor Reports - CICA Section 5970 or SAS 70 Reports
- Enterprise security
- Business continuity & disaster recovery planning
- Privacy and data control
- Change management controls
- IT general and application controls evaluations

Contact BDO

As part of our value-added service, BDO offers a complimentary needs and requirements assessment. This provides you with the opportunity to identify and review your risk advisory needs with our team of trained professionals. We encourage you to contact us to learn more about our services and to meet our team.