Set best practice while maintaining regulatory standards for your organisations' cybersecurity requirements'.

WHAT IS CYBERSECURITY RISK, AUDIT, ASSURANCE AND COMPLIANCE?

The BCX Cybersecurity Risk, Audit, Assurance and Compliance management services entail maintaining standards defined by:

- legal and regulatory mandates;
- contractual obligations, and internal policies;
- standards;
- industry frameworks and best practices.

Effective delivery of Cybersecurity risk assesment and enforcing compliance results in the satisfactory assurance and management of security risks and threats at a level deemed acceptable to an organisation's stakeholders. This service is available on request from clients who seek to understand their cybersecurity state and maturity level and wish to transition up the security curve for their core business processes and critical IT and Data assets.

WHAT IT DOES

Clients can select from a suite of Cybersecurity Risk, Audit, Assurance and Compliance management services that meet their unique situations and business requirements.

Services include:

1. Information Security Management System (ISMS) Audit and Assurance Program (ISO 27001, NIST CSF)
2. PCI DSS Compliance Program: Assurance Engagement
3. SAP ERP BASIS Administration and Security Audit/ Assurance Program
4. Cloud Computing Security Management Audit/ Assurance Program
5. POPIA Audit/Assurance Program
6. GDPR Audit Program for Small, Medium, and Large Enterprises
7. Business Continuity Management Audit/Assurance Program
8. IT Continuity Planning Audit/Assurance Program
9. Mobile Computing Security Audit/Assurance
10. VPN Security Audit/Assurance Program
11. Identity Management Audit/Assurance Program

HOW IT WORKS

ISMS AUDIT AND ASSURANCE PROGRAM (ISO 27001, NIST CSF)

- Information security touches all aspects of the business environment. Failure to implement adequate information security requirements could result in serious critical operational issues, business/customer losses, reputational damage and legal/regulatory sanctions.
- Provide management with an assessment of the effectiveness of the information security management function.
- Evaluate the scope of the information security management organisation and determine whether essential security functions are being addressed effectively.

PCI DSS COMPLIANCE PROGRAM: ASSURANCE ENGAGEMENT

- PCI DSS is a mandatory compliance requirement for all enterprises that process, store, transmit or access cardholder information for any of the major payment card brands.
- To provide management with an independent assessment relating to the governance, effectiveness and efficiency of PCI DSS security requirements across the enterprise, including the management of services that are delivered by external providers.

SAP ERP BASIS ADMINISTRATION AND SECURITY AUDIT/ ASSURANCE PROGRAM

- SAP is widely used in many enterprises. Improper configuration of SAP could result in an inability for the enterprise to execute its critical business processes.
- To provide management with an independent assessment relating to the effectiveness of configuration and security of the enterprise's SAP ERP architecture.

CLOUD COMPUTING SECURITY MANAGEMENT AUDIT/ ASSURANCE PROGRAM.

- Using cloud services brings multiple benefits to cloud users, but it also raises many concerns, which, if not handled well, can quickly turn the cloud experience into an information security management nightmare derived from the loss of controls over physical and logical assets.
- Provide management with an assessment of cloud computing policies and procedures and their operating effectiveness.
- Identify internal control and regulatory deficiencies that could affect the organisation.
- Identify cloud computing vendor management control concerns that could affect the reliability, accuracy and security of the enterprise data due to weaknesses in mobile computing controls.

POPIA AUDIT AND ASSURANCE PROGRAM

- The South Africa POPIA Act came into effect on 1 July 2020 and businesses have 12 months to prepare and comply.
- The business impact of the loss, disclosure or inappropriate use or modification of Personally Identifiable Information (PII) can be legal, regulatory or reputational leading to significant financial and operational costs.
- Provide management with an assessment of PII policies and procedures and their operating effectiveness.
- Identify internal control and regulatory deficiencies that could affect the organization.
- Identify information security control concerns that could affect the reliability, accuracy and security of enterprise data due to weaknesses in-network or mobile computing controls.

GDPR AUDIT PROGRAM FOR SMALL, MEDIUM AND LARGE ENTERPRISES

- As of 25 May 2018, GDPR gives EU residents control over their data wherever in the world they or their data may reside.
- The objective of a GDPR audit is to provide management with an evaluation of how effectively GDPR is being governed, monitored and managed. The review will focus on GDPR governance and response mechanisms as well as supporting processes which can help manage the risk associated with noncompliance.

BUSINESS CONTINUITY MANAGEMENT AUDIT/ASSURANCE PROGRAM

- A business continuity plan is an enterprise-wide group of processes and instructions to ensure the continuation of business processes – including, but not limited to, Information Technology - in the event of an interruption.
- Provide management with an evaluation of the enterprise's preparedness in the event of a major business disruption.
- Identify issues that may limit interim business processing and restoration of the same.
- Provide management with an independent assessment of the effectiveness of the business continuity plan and its alignment with subordinate continuity plans.

IT CONTINUITY PLANNING AUDIT/ASSURANCE PROGRAM

- IT continuity planning is the process that ensures continuous operations of business applications and supporting IT systems (i.e., desktops, printers, network devices.]
- Business reliance on automated solutions is tightly woven within the DNA of the enterprise.
- Provide management with an evaluation of the IT function's preparedness in the event of process disruption.
- Identify issues that may limit interim business processing and restoration of the same.
- Provide management with an independent assessment relating to the effectiveness of the IT continuity plan and its alignment with the business continuity plan and IT security policy.

MOBILE COMPUTING SECURITY AUDIT AND ASSURANCE

- Mobile devices have become an integral part of the IT infrastructure and thus become Mobile Computing. Convenience and availability are its major advantages, but these attributes are also its major risks to the enterprise.
- Provide management with an assessment of mobile computing security policies and procedures and their operating effectiveness.
- Identify internal control and regulatory deficiencies that could affect the organisation.
- Identify information security control concerns that could affect the reliability, accuracy and security of enterprise data due to weaknesses in mobile computing controls.

VPN SECURITY AUDIT/ASSURANCE PROGRAM

- A virtual private network (VPN) is a technology to protect data as they travel through public networks. The impact on the business transmitting data through public networks and the accompanying risks are significant.
- The objective of the audit/assurance review is to provide management with an independent assessment of the VPN implementation and ongoing monitoring/ maintenance of the effectiveness of the supporting technology.

IDENTITY MANAGEMENT AUDIT/ASSURANCE PROGRAM

- Identity Management (IdM) —also known as Identity and Access Management, (IAM)—is the set of procedures to issue and manage digital identities (identifiers) of people and systems so that they can be uniquely authenticated (identified) to IT systems before being granted online access to sensitive IT assets.
- The impact on the business and the accompanying risk is significant. IdM and its processes are the keys to the organization's information doors.
- The primary objective of the audit/assurance review is to provide management with an independent assessment relating to the effectiveness of identity management and its policies, procedures and governance activities.

WHY CHOOSE BCX?

BCX Cybersecurity leverages our knowledge, experience and effective delivery of Cyber Security risk assessments, audits, data privacy regulations, industry standards, and best practice security frameworks to give reasonable assurance that the security posture of your business complies with contractual, customer, legal and regulatory requirements.

FEATURES AND BENEFITS

FEATURES	BENEFITS
Tap into a pool of highly experienced and skilled Cyber Security Risk, Audit and Compliance professionals available on short notice when required	Achieve Cyber Security compliance while reducing the burden of external audit engagements and saves you money. Existing personnel can focus on other pressing requirements
Use of proven internationally recognized audit and compliance standards and frameworks	Gives you peace of mind about your security posture and compliance status
Customised service offering	Meet your specific and unique Cyber Security requirements
Our hands-on knowledge and experience in the integration of IT, Business and Security processes	Achieve an acceptable security posture level for your business

PRICING AND AVAILABILITY

The Cybersecurity Risk, Audit, Assurance and Compliance service is available nationwide. For more information and specific pricing details, speak to your account manager or send an email **ITS@bcx.co.za.**

BCX Head Office, 1021 Lenchen Avenue North, Centurion 0157
Reg No 1993/003683/07