keypoint

# IT security services

Keypoint is one of the GCC's most comprehensive providers of business advisory services. Our services - including accounting solutions, statutory & corporate advisory, investment administration & share registry services, trust services, IT consulting, tax services, human capital solutions, management consulting and financial regulatory compliance advisory - are valued by a wide range of clients, from large multinationals and financial services and insurance institutions to family-managed conglomerates and small and medium-sized enterprises.

# IT security

Our specialist team of subject matter resources and consultants with deep domain knowledge and industry experience help clients identify and manage their information technology-related requirements, including risks from the use of IT, through innovative services. One significant focus area, where our team has recent, relevant credentials, is IT security.


We offer IT services that help key decision makers understand the technology needs of their organisation, identify and implement suitable IT systems, align technology with business requirements and manage the risks that result from the use of information technology. While working on these areas, we also develop comprehensive risk analysis and contingency plans.

Our tailor-made services are focused on implementing proven methodologies, international leading practice and benchmarked internationals standards, delivering superior services through experienced resources.

### Information security consulting services

An organisation's core information security infrastructure cannot add all potential value without effective information security policies, processes, procedures and standards. Keypoint's consulting team, with diverse industry experience, helps organisations build and self-govern information security needs in a way - and at a pace - that it is comfortable with. Our information security consulting services include:

- Attack and penetration testing (APT)
- APT and incident response services
- Information security framework development
- Enterprise security strategy and roadmap design
- Application assessments and code reviews
- Anti-fraud consulting services
- Internal security compliance consulting and audits
- IT security architecture design
- Disaster recovery and business continuity planning
- Application security consulting
- Cloud security consulting

# ISO 27001:2013

ISO 27001 is a specification for an information security management system (ISMS) - a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information security management processes. ISO 27001 - which uses a top-down, risk-based approach and is technology-neutral - was developed to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving ISMSs.

The planning process for most ISO 27001 engagements is generally fairly consistent:

- Define a security policy
- Define the ISMS scope
- Prepare a statement of applicability
- Assess risks
- Manage identified risks
- Select control objectives and controls to be implemented

The specification for ISO 27001 is broad - including details for documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action - and requires cooperation across all sections of an organisation.

ISO 27001 focus areas include:

- Risk assessment
- Organisation of information security
- Cryptography
- Asset management
- Human resources security
- Physical and environmental security
- Communications security
- Access control
- System acquisition, development and maintenance
- Information security incident management
- IS aspects of business continuity management
- Compliance

## Keypoint's ISO 27001:2013 methodology

keypoint

| A typical ISO 27001:2013 scope | | |
|---|---|---|
| Establish ISMS policy, objectives, processes and systems and procedures | Implement and operate ISMS policy, controls, processes, systems and procedures | Assess and measure process performance against ISMS policy, objectives and practical experience |
| Design an information security effectiveness measurement framework and KPIs | Train the internal ISMS audit team | Use internal ISMS audit review to improve the ISMS |
| Define ISMS scope and boundaries - location, assets and technology | Define a risk assessment approach | Develop criteria for acceptable risk levels |
| Assess impact of confidentiality, integrity and availability losses | Assess vulnerabilities and test penetration (VAPT) | Assess risks |
| Identify and evaluate risk treatment options | Select control objectives and controls for risk treatments | Prepare a statement of applicability – justify the exclusion of any control objectives |
| Review implemented controls and control objectives and recommend additions and modifications | Prepare documentation and required procedures | Check certification readiness |
| Assist with identifying a certification body | Co-ordinate certification audit and assist with closure of non-conformities (NCs) | Provide a risk and compliance tool to manage gap assessments, policies and procedures, risk management module and separate dashboards for administrators and users |

# ISMS policies and procedures

Once we have assessed a client's current information security risks as part of a standard engagement, we generally:

- Develop:
  - Information security policies and procedures
  - Mandatory documents such as controls of documents and records (see table)
- Identify, assign and document roles and responsibilities for various functions including:
  - Information security
  - IT
  - Other impacted functions
- Review and update existing security policies and procedures
- Prepare a document master list with document reference numbers and classification to facilitate ISO 27001:2013 certification requirements
- Define information security effectiveness measurement framework and KPIs

**For more information on our ISO 27001 team and credentials, please see pages 10 and 11.**

| **Mandatory** ISMS documents | |
|---|---|
| ISMS committee charter | ISMS scope document |
| Information security policy and objectives | Definitions of roles and responsibilities |
| IT asset registers | Monitoring and measurement results |
| ISMS manual | Statement of applicability |
| Internal audit plan and report | Training and skills records |
| Document control procedures | Corrective action procedures |
| Risk assessment and treatment methodology - including a risk register | |

| **Illustrative** ISMS policies and procedures | |
|---|---|
| Corporate IS policy | Document controls |
| Acceptable usage | Network security |
| Asset management | Backup management |
| Access control | Passwords |
| IT management operating procedures | Physical and environmental security |
| Secure system engineering principles | HR security |
| Supplier security | Mobile device and teleworking |
| Incident response plan | Secure software development |
| Business continuity | Compliance |
| Change management | |

keypoint

# ISO 22301:2012

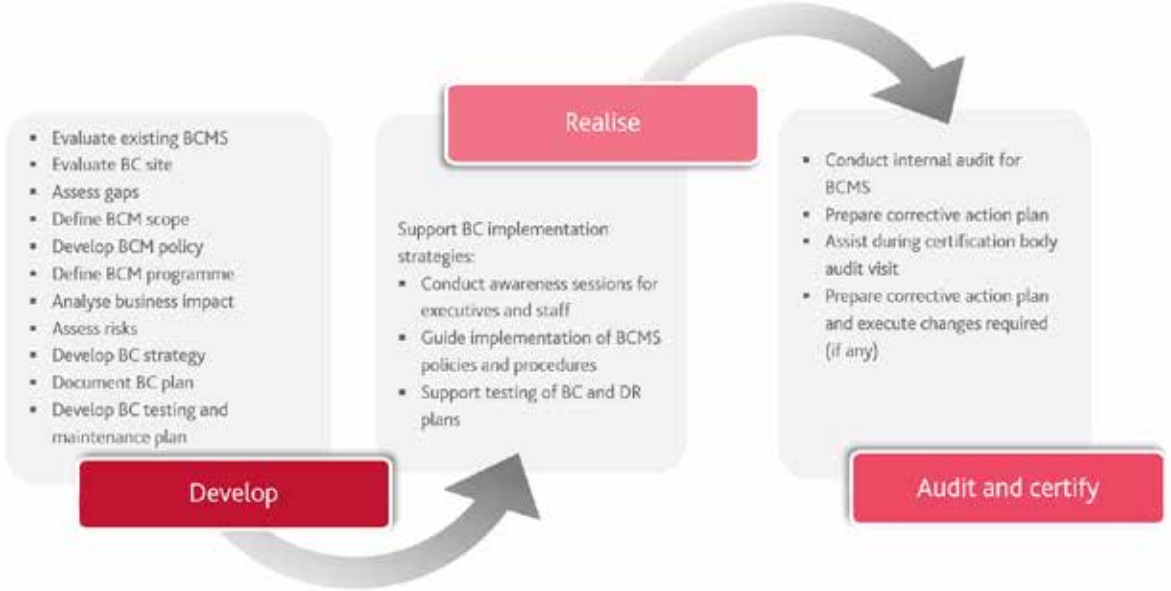
ISO 22301:2012 is a management system standard that specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of, prepare for, respond to, and recover from disruptive incidents. The standard was designed to suit all organisations, regardless of their type, size and nature.

ISO 22301 emphasises the need for a well-defined incident response structure, ensuring that, when incidents occur, responses are escalated in a timely manner and people are empowered to take necessary actions.

To work as intended, organisations need to thoroughly understood ISO 22301's requirements. Business continuity management (BCM) must become an ongoing management process, requiring competent people working with appropriate support and structures that perform as and when needed. When implemented properly, ISO 22301 can help organisations reduce risks, increase resilience, and deliver real benefits.

ISO 22301 reduces the frequency and impact of **disruptions**, helps businesses return to "business as usual" as quickly (and seamlessly) as possible, sets clear expectations (and so improves relationships across supply chains) and can - in certain circumstances - reduce insurance premiums. ISO 22301 builds stakeholder confidence and trust, enhancing your **reputation** and supporting your business development efforts and helping ensure business continuity plans are robust, resilient and ready for change. By helping organisations understand the impact of disruption, ISO 23001 increases internal and external **risk** visibility, keeping you current with regulatory changes and societal needs, while giving increased comfort that recovery plans are effective. Finally, ISO 23001 helps build **engagement** throughout a function or an organisation as all levels - from top management down - are involved in the process, helping to raise employee engagement and understanding while ensuring that staff throughout the organisation have the skills and knowledge they need to effectively manage the BCMS.

Our end-to-end methodology delivers turnkey business continuity and disaster recovery solution needs



| Area | Scope |
|---|---|
| **Policy and programme management** | ▪ Define company's BCM policy and how it should be implemented, controlled, validated and governed |
| **Business continuity (BC)** | ▪ Define how to integrate BC into day-to-day activities and embed BC into the organisational culture |
| **Analysis** | ▪ Analyse business impact (BIA), threats and risks |
| **Design** | ▪ Define and highlight optimal recovery strategies and incident response procedures |
| **Implementation** | ▪ Execute agreed BCP strategies |
| **Reviews and health checks** | ▪ Regularly review the system and support maintenance and testing activities |
| **Evaluation** | ▪ Evaluate existing business continuity management system<br>▪ Evaluate business continuity site<br>▪ Correct identified gaps |
| **Awareness** | ▪ Prepare ISO 22301 awareness portals<br>▪ Develop evaluation material to test staff understanding<br>▪ Conduct information security awareness for all staff |
| **Test BC and DR plans** | ▪ Test business continuity plan (BCP)<br>▪ Test disaster recovery (DR) plan |
| **BCMS internal audit** | ▪ Conduct internal audit<br>▪ Prepare corrective action plan |
| **Certification assistance** | ▪ Support during certification body visit<br>▪ Prepare corrective action plan<br>▪ Make required changes (if any) |

# PCI DSS advisory

The payment card industry's (PCI) security standards council, which manages security standards for the industry, has established a data security standard (DSS) to govern the technical and operational aspects of security standards for card-holder data.

Any entity that stores, processes or transmits any kind of card data should be compliant with the PCI DSS. The current version - v3.2.1 released in May 2018 - has 12 mandatory requirements based on six objectives:

1. Build and maintain a secure network
2. Protect card-holder data
3. Manage vulnerability
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

The Central Bank of Bahrain (CBB) mandates compliance with PCI DSS for all licensees – non-compliance could result in hefty penalties. Founder members of PCI SSC can impose non-compliance penalties and remove the ability to accept payment cards.

## Who should be PCI DSS-compliant?

- Organisations accepting card-based payments
- Organisations processing card data
- Institutions that issue or process card data
- Point of sale (POS) vendors

## Already certified?

If you are already certified, ensure:

- Your organisation has implemented v3.2.1
- Mandatory activities are performed on time
- Reports are submitted on time

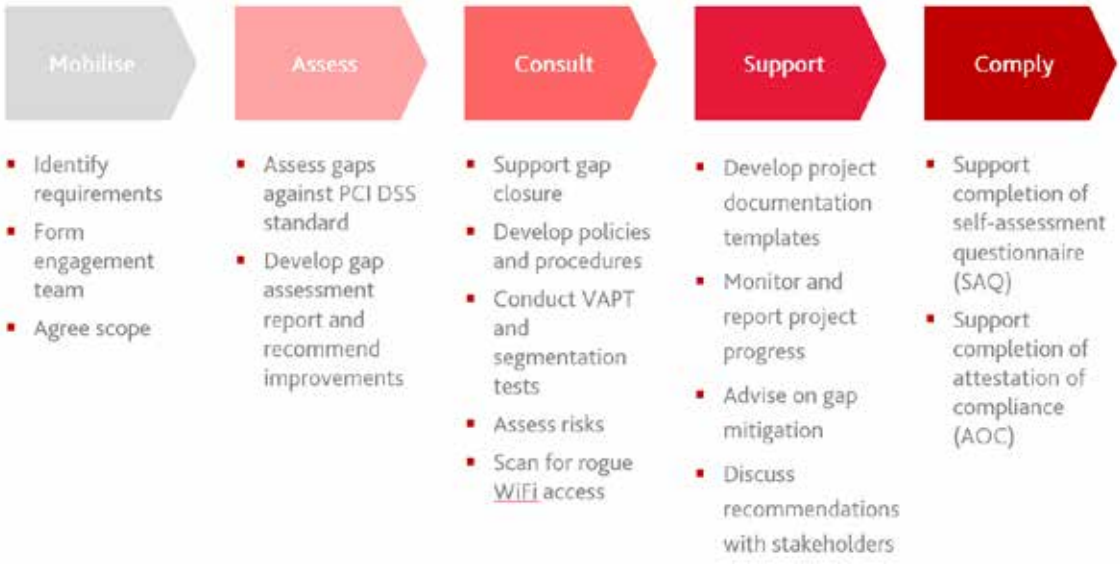
## Not yet PCI DSS compliant?

If your business is expected to comply with the PCI DSS but have not yet completed the compliance process, start now:

- Assess current status against requirements
- Fix any identified gaps
- Report your status to the CBB

## The Keypoint approach

At the heart of Keypoint's methodology is a structured, comprehensive approach featuring five independent sets of activities:




The PCI DSS standard requires a qualified security assessor (QSA) to issue a report on compliance (ROC) if an entity has more than six million transactions annually or if members of the PCI SSC request an ROC submission. Keypoint can work with a QSA counterpart to assist with ROCs.

# Our people

Our IT security team offers a broad range of relevant regional and sector experience. Combining almost 50 years of deep information security experience, gained working in Bahrain, across the GCC, in Sri Lanka and in India, our team - with a 'Big 4' professional services background - has advised business and organisations across a variety of industry sectors.

Keypoint's senior IT leaders are widely recognised as leaders in their fields. As the head of Keypoint's IT consulting function, **Srikant Ranganathan** has over 25 years of IT and ISMS experience, has been involved with over 100 ISO engagements, is ISO 27001 LI, CISA, CISSP, CFE qualified and is also a chartered accountant. As well as PCI DSS, ISO 27001 and ISO 22301 implementation experience, **Darrshan Manukulasooriya** has significant IT consulting, IT auditing and software engineering expertise. An ethical hacker, **Sagar Rao** is CEH and ISO 27001: 2013 LA qualified and has over seven years of security testing experience.

**Srikant Ranganathan**
**Senior Director**
srikant.ranganathan@keypoint.com

**Darrshan Manukulasooriya**
**Technical lead**
darrshan.m@keypoint.com

**Sagar Rao**
**Subject matter expert | IT security**
sagar.rao@keypoint.com

| An selection of our broader IT services | | |
|---|---|---|
| **IT security** | **IT internal audits** | **Information security** |
| Vulnerability assessment and penetration testing (VAPT) | IT process audits | Policy and process manuals |
| Application code reviews | IT special assignments | IT security architecture design |
| Configuration and architecture reviews | Technology control reviews | Application security |
| Web and mobile app security assessments | IT security management reviews | Cloud security consulting |
| Social engineering assessments | Business continuity reviews | Programme management services |
| OS configuration reviews | Disaster recovery management | Disaster recovery and business continuity planning |
| Anti-virus configuration re-views | Post-implementation reviews | Enterprise security strategy and roadmap design |

Keypoint's IT security team has worked across a wide range of economic sectors:

- **Financial services** - conventional and Islamic wholesale and retail banks, as well as insurance businesses
- **Telecoms** - TRA-regulated service providers offering a variety of local, international and regional services
- **Listed businesses** - including a Saudi paper manufacturer
- **Oil & gas businesses** - including a government-owned oil & gas holding company
- **Logistics, travel and distribution companies** - including the GCC's leading travel agency
- **Sovereign wealth funds** - a strategic sovereign investor with stakes in over 60 local and international commercial enterprises, operating in 14 countries with over US$16b in total assets

| PCI DSS implementation and audits | | |
|---|---|---|
| Kanoo Travel - five GCC countries and Egypt | Kalaam Telecom | Sinnad |

| IT security services | | |
|---|---|---|
| Ahli United Bank | First Energy Bank | Albaraka Bank Group |
| Al Baraka Islamic Bank | Al Salam Bank-Bahrain | GFH Financial Group |
| Ithmaar Bank | Oil & Gas Holding Company | Ibdar Bank |
| United Gulf Bank | Alubaf Arab International Bank | Kuwait Finance House Bahrain |
| Bahrain Mumtalakat Holding Company | | |

| Vulnerability assessments and penetration testing (VAPT) | | |
|---|---|---|
| Arab Shipbuilding Repair Yard | First Energy Bank | Infonas |
| Ministry of Youth and Sports | Midal Cables | YBA Kanoo |
| Kanoo Group | Al Zayani Group | United Gulf Bank |

| Business continuity management (BCM) | | |
|---|---|---|
| Arab Shipbuilding Repair Yard | First Energy Bank | Bank of Khartoum International |
| Ministry of Youth and Sports | United Gulf Bank | Arab Paper Manufacturing Co. |

| ISO implementation | | |
|---|---|---|
| YBA Kanoo - Bahrain | First Energy Bank | Bank of Khartoum |
| Kanoo Group (UAE) | Midal Cables | YBA Kanoo - Saudi Arabia |
| Kanoo Travel (UAE) | Ahli United Bank - Bahrain | The BENEFIT Company |

keypoint

November 2019