Information security, business continuity & the telecoms sector

Bahrain's Telecommunications Regulatory Authority – the TRA – released Resolution 5 of 2017, regulating risk management for critical telecommunications infrastructure, in May 2017. The resolution establishes a risk management process, sets out expectations for business continuity, standardises licensees' approach to assessing and protecting the security and availability of critical telecoms infrastructure and defines licensees' responsibilities.

Licensees which install, operate or manage critical telecoms infrastructure, as well as holders of particular licences , should expect to receive, if they haven't already, a risk management determination (RMD). Based on the RMDs, licensees are expected to adhere to two specific timelines – a three-month deadline requiring an asset inventory and an 18-month deadline requiring licensees to develop, implement and maintain:

- A business continuity plan
- ISO27001 certification
- A certification audit report
- A risk assessment

The TRA expects business to recertify every three years and reserves the right to ask for additional risk assessments, including penetration testing.

Licensees that are found to be non-compliant will be deemed to be in material breach of the telecommunications law and could face penalties and sanctions.

What is leading practice?

As a regulator, the TRA has a mandate to ensure critical telecoms infrastructure is identified and protected. By aligning this mandate with leading practice in information security management systems and business continuity, it can ensure that TRA licensees are compliant with international norms.

Globally, the International Organization for Standardization (ISO) has developed a suite of ISO/IEC 27000 standards, helping organisations keep information assets secure. ISO27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) and includes requirements for the assessment and treatment of information security risks, covering people, processes and IT systems, helping to keep information assets secure.

Business continuity means having a plan to deal with difficult situations so organisations continue to function under any circumstances, recognising potential threats, analysing their impact on day-to-day operations, and mitigating those threats.

Leading practice – such as ISO 22301 - is an ongoing process to continually build and improve organisational resilience by identifying threats, designing responses, implementing a plan and measuring effectiveness.

Contact us

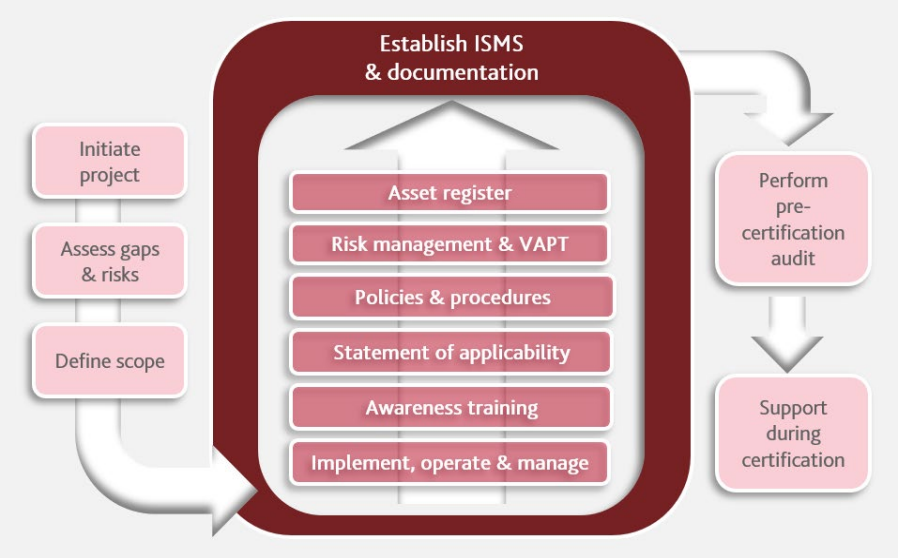
Srikant Ranganathan
Senior Director
IT consulting
+973 1720 6827
+973 3626 6286

Darrshan Manukulasooriya
Assistant Manager
IT consulting
+973 1720 6866
+973 3592 9859

How can Keypoint help?

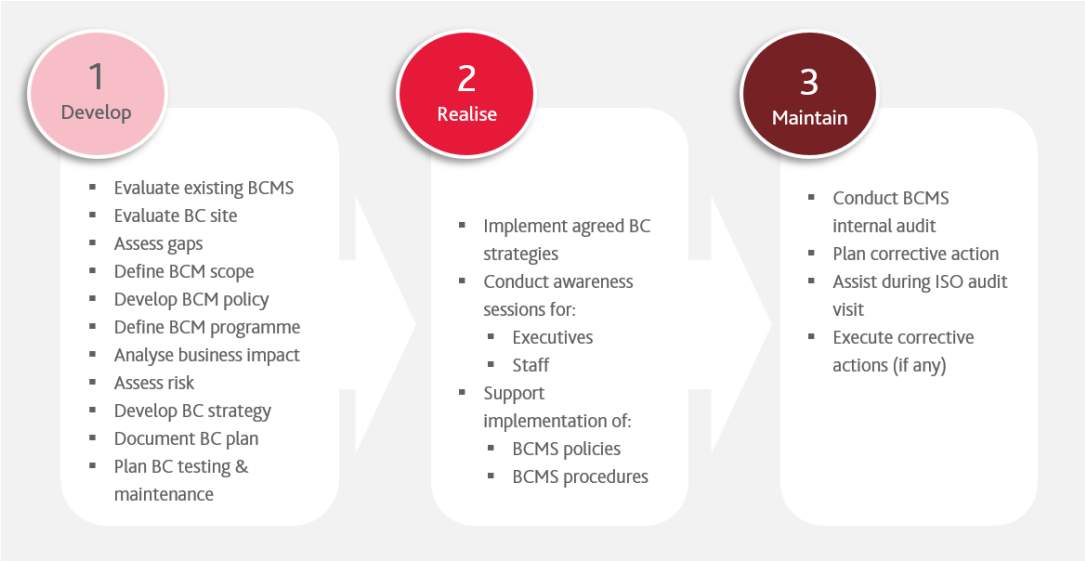
Our ISO 27001 methodology

As a leading professional services firm that has worked with telecommunications providers across MENA for over a decade, we have significant, relevant expertise and credentials. We have a tried and tested ISO 27001 methodology which enables us to assist your compliance with the requirements of the standard.



Our ISO 22301 methodology

Our end-to-end ISO 22301:2012 methodology results in a tailored business continuity management system (BCMS) solution. In the first (develop) phase, we assess, analyse and plan. In the next two phases - realise and maintain – we focus on tailoring your BCMS solution to your requirements and adding value in a number of other ways:



Resolution 5 of 2017 sets difficult - if attainable - targets, tight deadlines and high expectations. TRA licensees would be well-advised to start proactively preparing now to comply, rather than having to belatedly react to receiving a risk management determination. We have the team, experience and credentials needed to make information security and business continuity a source of competitive advantage, rather than a barrier to success.