.... with more all the time. For example, the November 2012 national standard AE/HSC/NCEMA 7000:2012 from the United Arab Emirates (UAE), largely based on BS 25999 Business Continuity Management Standard, was developed by the National Crisis Emergency & Disasters Management Authority (NCEMA) and published under the auspices of His Highness Sheikh Khalifa Bin Zayed Al Nahyan, President of the UAE and Chairman of the Higher Security Council.

The Devil's Advocate

It is generally accepted that standards identify and promote best practice and that, by becoming audited and certified to a standard, an organization can prove its compliance with best practice. The leadership and culture of some organizations may require standards to demonstrate regulatory compliance – or just for the trophy wall.

But should we challenge this? Just how relevant are standards these days? BC is no longer an infant discipline, but an increasingly mature profession.

Unless there are powerful legal or regulatory requirements or arguments for certification, could standards be counter-productive? Consider some of the arguments against standards:

- Standards are not necessarily best practices: they are a consensus agreement of the standards committee, with the danger of settling for the lowest common denominator.
- Standards may encourage a "one size fits all" mentality whereas in real life public and private sectors have different roles and needs; each industry is different; each organization is unique, has different requirements and may justifiably select a BC approach that differs from its peers.
- An organization may be primarily concerned with:
  - Regulatory compliance (e.g., in banking and finance, compliance with requirements of the Finance Industry Regulatory Authority, Federal Financial Institutions Examination Council, relevant Financial Services Authority, or Central Bank).
  - Satisfying audit requirements (e.g., external audit companies, or Information Systems Audit and Control Association (ISACA), which may not require certification to a standard).
- Most of the current BC standards say broadly the same thing, follow broadly the same approaches, and broadly agree with the professional practices of BC-related institutes and associations. So, if you are using professionally qualified BC practitioners, why do you need to complicate life by compliance with standards?
- Once certified to a standard, it is difficult to argue that you no longer need to continue to bear the cost and overhead of annual audits, reviews, and inspections to remain compliant indefinitely.

So, the question remains: Are standards always appropriate, and do you really need to be certified to one?

2.2 Key Standards

Four standards are discussed in detail in this section due to their significance and level of acceptance.

The first three are used on a worldwide basis and are also specifically referenced in the United States PS-PREP initiative.

- National Fire Protection Association (NFPA) 1600, multiple editions.
- ISO 22301.
- ASIS SPC.1-2009.

As a fourth, we have included BS 25999, Parts 1 and 2. A number of organizations have been certified to it around the world.

Chapter 1 of NSP SP 800-34 provides an introduction.

Chapter 2, Background, introduces contingency planning and resilience and identifies the different types of contingency plans including BC, COOP, crisis communications, cyber incidents, critical infrastructure response, DR, information systems, and occupancy emergency.

Chapter 3 covers the information systems contingency planning process, including policy, BIA, resources, prevention, strategies, testing, and maintenance.

Chapter 4 is concerned with plan development – information, activation, and reconstitution.

Chapter 5 is a more technical guide highlighting issues relating to different types of equipment and telecommunications.

Appendices contain useful templates.

Recap: NIST SP 800-34 2010

Relevance:	Although aimed at US Federal information systems, it has wider applicability.
Importance:	Useful for public sector entities.
Usability:	Helpful templates.
Pros & Cons:	
Pro –	Good advice.
Con –	It tries to cover a rapidly moving target.

2.3.9 ISO/IEC 24762:2008 Guidelines for Information and Communications Technology Disaster Recovery Services[19]

First a Singapore standard (SS 507:2004), then the backbone of the international standard, this standard provides a basis for committed BC/DR service providers, whether in-house or commercial vendors, to differentiate themselves from other, lesser players and helps end-user organizations to lower BC/DR outsourcing risks. Vendors may get certified to these standards.

ISO/IEC 24762:2008 provides guidelines on the provision of information and communications technology (ICT) DR services as part of BCM. This standard applies to both in-house and outsourced IT service providers of physical facilities and services.

ISO/IEC 24762:2008 specifies:

- The requirements for implementing, operating, monitoring and maintaining ICT DR services and facilities.
- The capabilities which outsourced ICT DR service providers should possess and the practices they should follow, so as to provide basic secure operating environments and facilitate organizations' recovery efforts.
- The guidance for selection of recovery site.
- The guidance for ICT DR service providers to continuously improve their ICT DR service.

The standard supports the operation of an information security management system (ISMS) by addressing the IT and availability aspects of BCM in time of crisis.

A BCP comprises strategies to prepare for national, regional, or local crises that could jeopardize an organization's capacity to continue with its core mission, as well as its long-term stability.

According to ISO/IEC 24762:2008, BCM is part of the RM process and involves:

- Identifying potential threats that may cause adverse impacts on business operations and associated risks.
- Providing a framework for building resilience for business operations.
- Providing capabilities, facilities, processes, and action task lists for responses to disasters and failures.

Using this standard, organizations will be able to build resilience into their ICT infrastructure, complementing their BCM initiative and information security management initiative.

The standard includes guidelines on the implementation, testing, and execution aspects of DR and can be applicable to both in-house and outsourced ICT DR service providers of physical facilities and services. It provides guidance on:

- Implementing, operating, monitoring, and maintaining the facilities and services necessary for DR.
- Fallback and recovery support for the organization's ICT systems.
- The capabilities that outsourced ICT DR service providers should possess and the practices they should follow to provide basic secure operating environments and facilitate recovery efforts.
- The selection of a recovery site.
- Requirements for ICT DR service providers to improve their ICT DR services.

While this standard covers physical recovery sites, users are increasingly turning to cloud services like Recovery as a Service as potentially cheaper options. In September 2013 the Cloud Security Alliance and BSI announced STAR Certification for cloud service providers, based upon meeting the ISO/IEC 27001 IT security standard and the specified set of criteria outlined in the CSA Cloud Controls Matrix. Eleven controls areas within this matrix cover compliance, data governance, facility security, human resources, information security, legal, operations management, RM, release management, resiliency, and security architecture.

See http://www.bsigroup.com/Cloud-Security

Other relevant standards and initiatives include:

- ISO/IEC 27017 standards and initiatives include BSI's announced STAR Certification for cloud service and 27018 covering security aspects, although it will be several years before these are mature and published.
- The Telecommunications Industry Association (TIA) and the Enterprise Product Integration (EPI) have entered a licensing agreement that will allow EPI to develop international certified training courses for the TIA-942 Telecommunications Infrastructure Standards for Data Centers – a standard that addresses installation, maintenance and architectural considerations of data center designs for providers.

Recap: ISO/IEC 24762: 2008

Relevance: Any BC/DR service vendor and their potential clients.

Importance: Useful to establish vendor credibility and to consider its requirements in Pre-Qualification Questionnaires and Requests for Proposals.

Usability: Requirements laid out clearly.

Pros & Cons:

Pro – Helps to benchmark internal DR capability and to identify credible vendors.

Con – Smaller, local vendors may find the cost of certification high.

2.3.10 UAE Business Continuity Standard AE/HSC/NCEMA 7000:2012

The United Arab Emirates (UAE) National Emergency Crisis and Disaster Management Authority launched a BCM standard in December 2012 to ensure organizations across the country continue operating throughout any emergency. It aims to help organizations identify their key services and the threats to them and mitigate impact of potential disruption. This standard, UAE Business Continuity Standard AE/HSC/NCEMA 7000:2012, was produced after consulting the British, Australian, New Zealand, Swiss, and Singaporean standards, and considering the nature of the UAE's activities and services. The UAE standard sets out elements to the BCM process in both the private and public sectors. It provides for developing and implementing incident management, BC, and business recovery plans that detail the steps to be taken during and after an incident to maintain or restore operations. It also requires validation of supply chain resilience.

The standard has a number of differentiators:

- It is the first standard in Arabic in the region.
- It focuses on the entire country and its infrastructure, rather than being enterprise-centric. It reflects convergence of BCM and EM on a country-wide level.
- It was designed within the culture of the region. While BC has been maturing in the Middle East over the last decade, it was still largely IT-centric and embedded typically in major financial and multinational institutions and telcos. Impetus was necessary to stride beyond these limitations and reflect increasingly regulated, structured, and sophisticated public and private sector business operations and demonstrate the significance of the region as a leading global player.

Recap: UAE Business Continuity Standard AE/HSC/NCEMA 7000:2011

Relevance: Particularly relevant to enterprises with business activities predominantly within the region. However, international partners can have confidence that organizations complying with this standard are applying sound EM and BC practices.

Importance: The first EM/BC standard in Arabic, it demonstrates government determination to create and maintain an orderly and structured public and commercial business environment.

Usability: Tailored to its specific market.

Pros & Cons:

Pro – Reflects good practice, convergence of and interaction between EM and BC activities.

Con – May be less valued outside the Middle East.