Deura Information Security Consulting

Hugh Deura

Information Security advisor and ISO 27001 consultant

Hugh@DeuraInfoSec.com

www.DeuraInfoSec.com

Blog.DeuraInfoSec.com

www.Facebook.com/DiscInfoSec

http://www.linkedin.com/in/hdeura

(707) 998-5164

ISSA Information Systems Security Association The Global Voice of Information Security

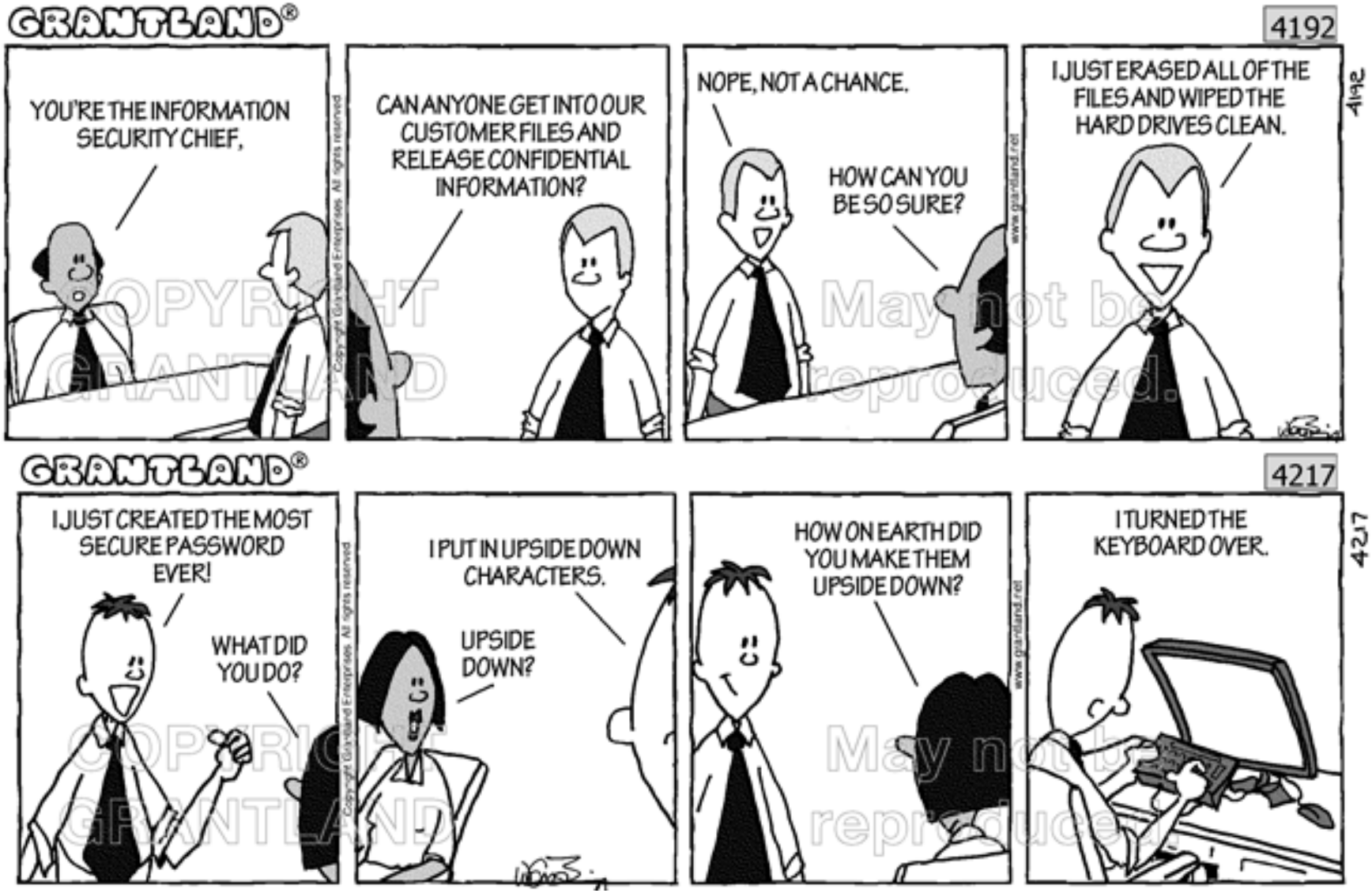
San Francisco Bay Area Chapter www.sfbayissa.com

How ISO 27001 compliance is relevant to business

Agenda

- What is ISO 27001?
- History of ISO 27001
- ISO 27001 relationship with ISO 27002
- Approach to ISO 27001 certification
- ISO 27001 implementation steps
- ISO 27001 certification timelines
- Q&A

Information Security best practice in action



What is ISO 27001…

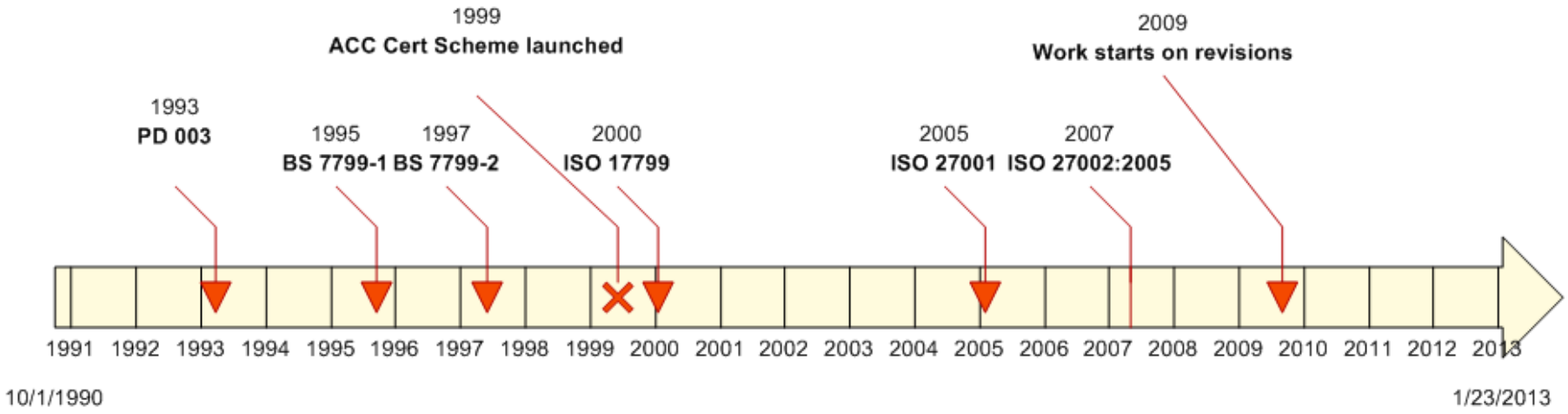
Two standards?

- ISO/IEC 27001:2005
  - –specification for an Information Security Management Systems (ISMS)

    An ISMS is the means by which Senior Management monitor and control their security, minimizing the residual business risk and ensuring that security continues to fulfill corporate, customer and legal requirements

- ISO/IEC 27002:2005 - code of practice.
  - –comprehensive catalogue of good security

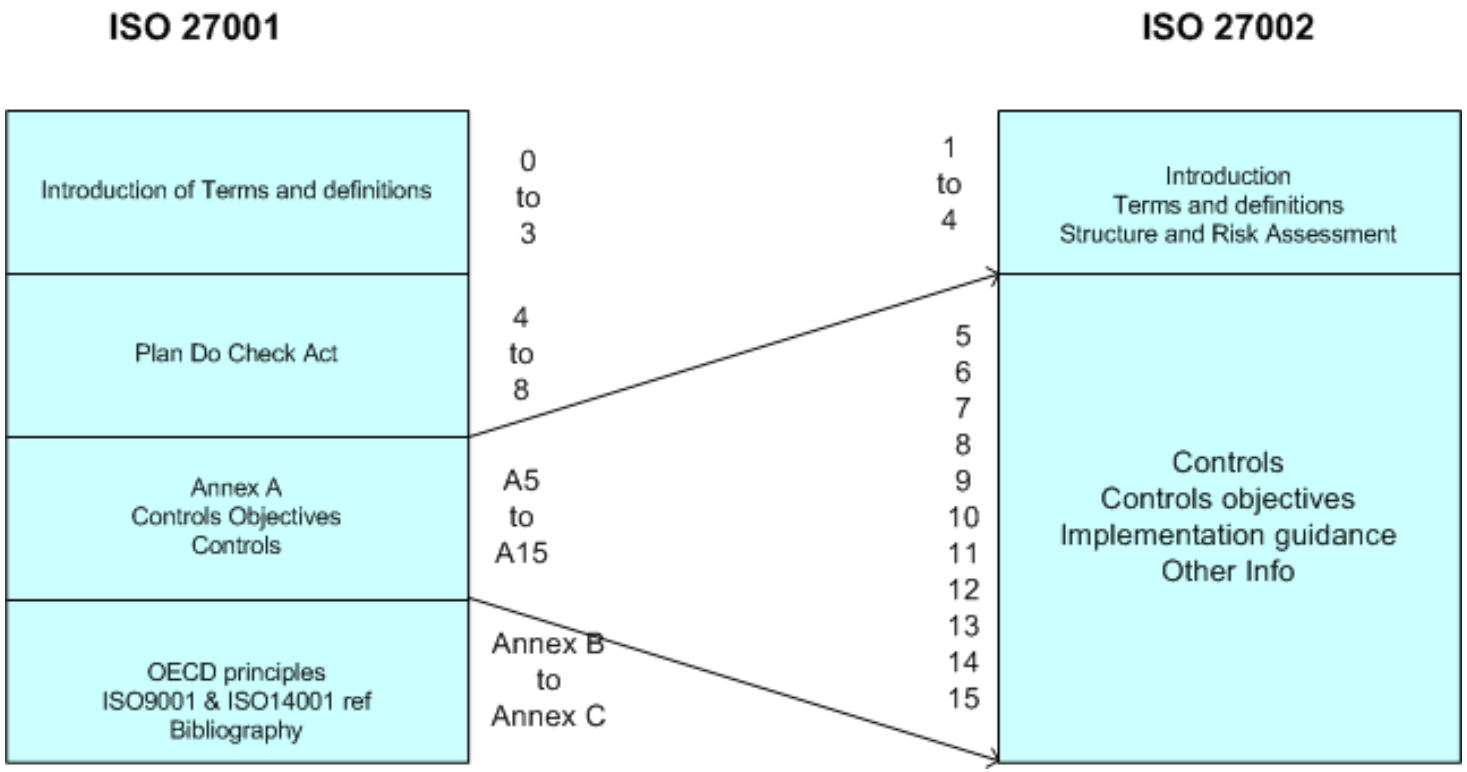
History of ISO 27001



ISO 27000 Family of Standards

- ISO/IEC 27000:2009 (ISO 27000) ISMS Introduction & Vocabulary.
- ISO/IEC 27001:2005 (ISO 27001) ISMS - Requirements (revised BS 7799 Part 2:2005).
- ISO/IEC 27002:2005 (ISO 27002) Code of practice for information security management as from May 2007 - formerly ISO/IEC 17799.
- ISO/IEC 27003:2010 (ISO 27003) ISMS implementation guidance.
- ISO/IEC 27004:2009 (ISO 27004) Information security metrics and measurements.
- ISO/IEC 27005:2011 (ISO 27005) Information security risk management (based on and incorporating ISO/IEC 13335 MICTS Part 2).
- ISO/IEC 27006:2007 (ISO 27007) Requirements for bodies providing audit and certification of information security management systems.
- ISO/IEC 27007:2011 (ISO 27007)– Guidelines for information security management systems auditing against ISO/IEC 27001, and guidance on the evaluation of ISMS auditors.
- ISO/IEC 27008:2011 (ISO 27008)– Guidelines for Auditors on Information Security Controls.
- ISO/IEC 27010:2012 (ISO 27010) Infosec Communications.

ISO 27001 relationship with ISO 27002



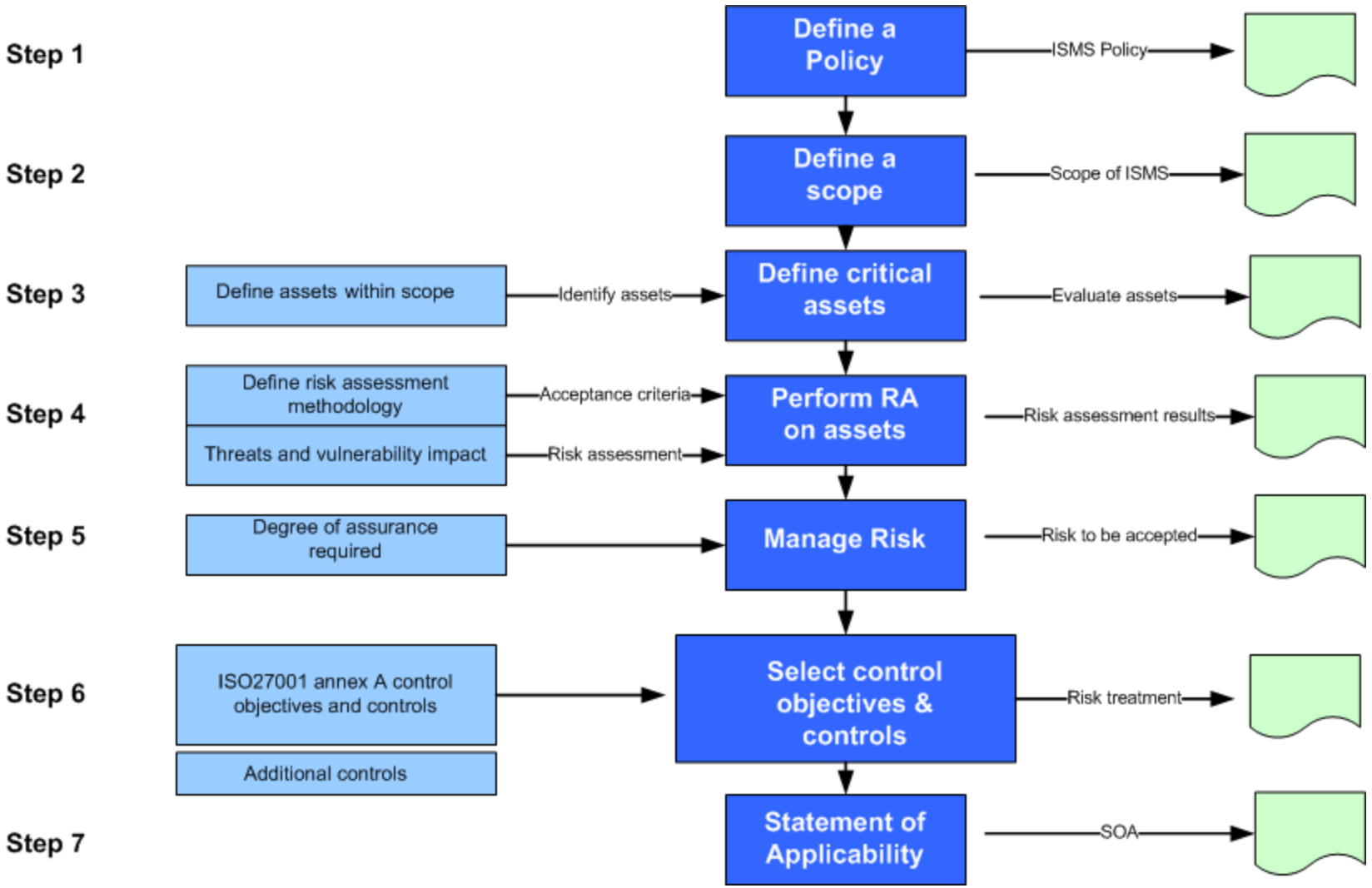
ISO 27001 ISMS

ISO/IEC27001:2005 ISMS - Requirements

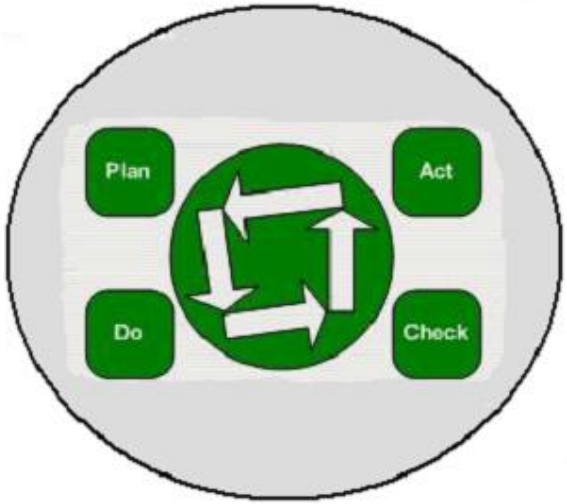
- –Scope
- –Terms and definitions

- General requirements
- Establishing ISMS → Plan
- Implementation → Do
- Monitor and review → Check
- Maintain and improve → Act
- Documentation
  - –Document control
- Management responsibility
  - –Training and awareness
- ISMS audits
- Review
- ISMS improvement

7 ISMS Implementation Steps



Control Domains and continuous ISMS maintenance



Security Policy

Organization of Security

Asset Management

Human Resources

Physical and Environmental

Communication Management

Access Control

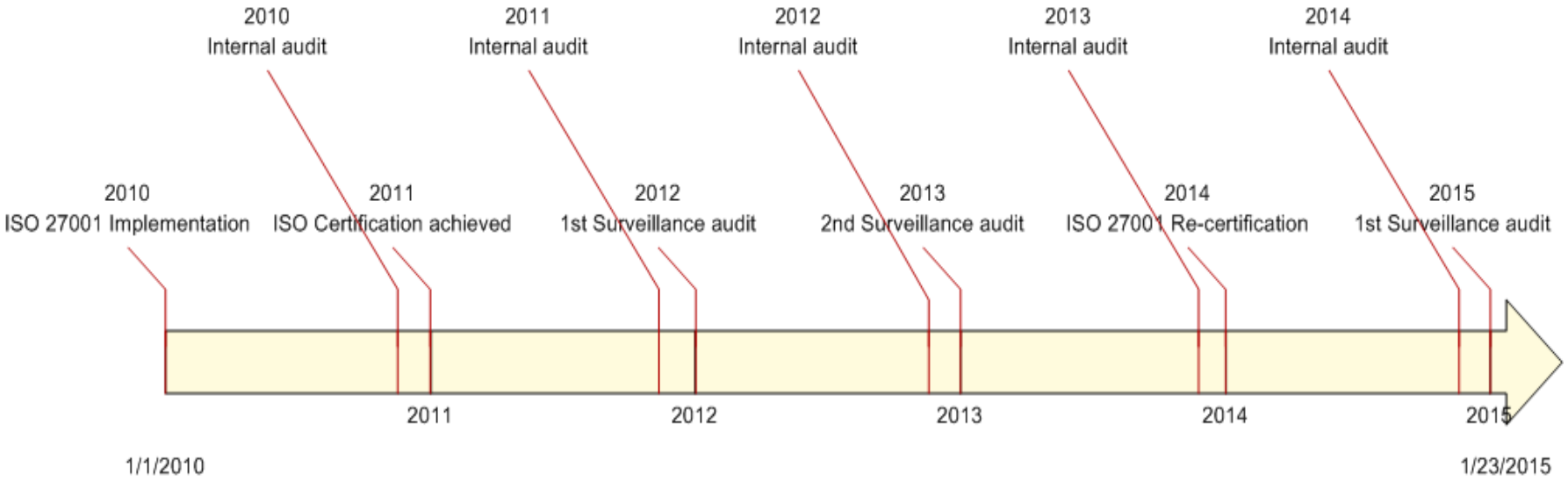
Info Systems Development

Incident Management

Business Continuity

Compliance

ISO 27001 Certification Timelines



Q&A

Hugh Deura CISSP, CISM, G7799 , CIS LI , NSA-IAM
Information Security advisor and ISO 27001 consultant
Hugh@DeuraInfoSec.com
www.DeuraInfoSec.com
Blog.DeuraInfoSec.com
www.Facebook.com/DiscInfoSec
http://www.linkedin.com/in/hdeura
(707) 998-5164

Thank you for your time – DISC InfoSec