

**Compliance with California Senate Bill 1386 (SB 1386)
SB 1386 Requirements cross-referenced to ISO27002**

The State of California has formally adopted ISO/IEC 27002:2005 as the state's information security standard. The Information Security Program Guide was developed for and adopted by the State's CIO IT Council and April 2007.

Clearly, any organisation seeking compliance with SB1386 and with the information security requirements in the State Administrative Manual will look to ISO27002 for detailed guidance on vendor-neutral best-practice information security management.

The IT Governance *SB-1386 & ISO27002 ISMS Toolkit* is specifically designed to help organisations and agencies that must comply with SB1386; it conforms to ISO27002 and, if desired, also helps organizations prepare for external certification that would demonstrate conformance to such a standard.

This document lists, below, the SB1386 compliance recommendations provided in the State of California's Office of Privacy Protection's *Recommended Practices on Notice of Security Breach Involving Personal Information* (May 2008 Revision) and identifies, for each of them, the relevant clause(s) in ISO/IEC 27002¹ and in the IT Governance *SB-1386 & ISO27002 ISMS Toolkit*.

1. Collect the minimum amount of personal information necessary to accomplish your business purposes, and retain it for the minimum time necessary
 - a. See ISO 27002 clause 15.1.4 and Toolkit Doc 15.6
2. Inventory records systems, critical computing systems, and storage media to identify those containing personal information
 - a. See ISO 27002 clause 7.1.1 and Toolkit Doc 7.1
3. Classify personal information in records systems according to sensitivity
 - a. See ISO 27002 clause 7.2.1 & 7.2.2 and Toolkit Doc 7.6
4. Use appropriate physical and technological security safeguards to protect personal information, particularly notice-triggering information, in paper as well as electronic records.
 - a. See ISO 27002 clause 11.1 and Toolkit Doc 11.1
5. Pay particular attention to protecting notice-triggering personal information on laptops and other portable computers and storage devices.
 - a. See ISO 27002 clause 11.4.5 and 11.7.1 and Toolkit Doc 11.11
6. Do not use data containing personal information in testing software or systems.
 - a. See ISO 27002 clause 12.4.2 and Toolkit Doc 10.10
7. Promote awareness of security and privacy policies and procedures through ongoing employee training and communications.
 - a. See ISO 27002 Section 8 and Toolkit Section 8
8. Require service providers and business partners who handle personal information on behalf of your organization to follow your security policies and procedures.
 - a. See ISO 27002 Section 10.2 and DOC 10.9
9. Use intrusion detection technology and procedures to ensure rapid detection of unauthorized access to higher-risk personal information.

¹ In many cases, there is more than one clause of ISO27002 that is relevant; we have identified, in this list, only the most important of them – the documents in our SB1386 & ISO27002 ISMS Toolkit reference all the relevant and applicable clauses of ISO27002.

**Compliance with California Senate Bill 1386 (SB 1386)
SB 1386 Requirements cross-referenced to ISO27002**

- a. There is no specific ISO27002 control dealing with intrusion detection, although it is referenced in a number of areas in the standard and most closely linked with ISO 27002 clause 15.1.5. It is covered in Toolkit Doc 10.18
- b. Penetration testing is covered in ISO 27002 clause 15.2.2 and in Toolkit DOC 15.4
- 10. Wherever feasible, use data encryption, in combination with host protection and access control, to protect higher-risk personal information.
 - a. In respect of notebook computers, this is covered under point 5, above. In respect of data encryption elsewhere in the network, see ISO 27002
 - b. Encryption is otherwise covered in ISO 27002 clauses 12.3.2 and 15.1.6 and in Toolkit Doc 12.2
- 11. 11. Dispose of records and equipment containing personal information in a secure manner.
 - a. See ISO 27002 9.2.6 and Toolkit DOC 9.11
- 12. Review your security plan at least annually or whenever there is a material change in business practices that may reasonably implicate the security of personal information.
 - a. See ISO 27002 clause 5.1.2 and Toolkit DOC 5.2
- 13. If you are a health plan or health insurer, provide patients with regular explanation of benefits statements.
 - a. This requirement is not covered by ISO 27002, but it is a sensible one!
- 14. Preparation for Notification, and incident response plan, which addresses security incidents including unauthorized access to or acquisition of higher-risk personal information – this requirement of SB1386 is addressed in ISO 27002 section 13 and in the Toolkit's section 13.