ADISA

ASSET DISPOSAL & INFORMATION
SECURITY ALLIANCE

A comparison of ISO 27001 and ADISA

ISO27001 is a part of the 27000 family of Standards and covers information security management system. Disposal is mentioned only briefly in Section 4, Asset Management and also gets mentioned in 27002 Section 9. However, there is no explicit guidance as to how to achieve secure disposal. It is widely recognised as being the best information security standard available and has international recognition.

The ADISA certification program and standard were launching in 2010 and is a program specifically aimed at those companies provided ICT recovery services which encompass data sanitisation.

A quick comparison table is below:

Criteria	27001	ADISA	Notes
Continual Assessment	Annual Inspection	Twice a year	Depending on the accrediting body some ISO awards have up to 10 years validity. ADISA certification can be suspended any time
Independent Auditing	Yes	Yes	In addition to using UKAS accredited auditors ADISA also utilises independent forensic auditors for spot check audits.
Industry Specific	No	Yes	Any organisation can be ISO 27001 certified. Only expert IT asset recovery companies can become ADISA certification.
Specific to service rather than the business	No	Yes	The majority of ISO 27001 is regarding the business itself rather than the service it delivers. The scope of the certification can even have the service provision identified as being out of scope.
Unannounced audits.	No	Yes	ISO auditing is done by appointment. ADISA's spot check audit schedule happens at no notice to the member.
Forensic tests	No	Yes	Using University of South Wales forensics' teams, as part of the spot check audit formal forensic assessments are made on all media types to ensure no data is resident.
End user benefits	No	Yes	Free monitoring service for customers which enables them to receive copies of all audits at the same time as the member.
Government Recognised	Yes	Yes	The ADISA certification program has been formally recognised by DIPCOG. http://www.adisa.org.uk/Dipcog/
UK end user Recognised	Yes	Almost	ADISA certification is beginning to get built into vendor selection requirements which a number of tenders being released requiring certification.
Internationally recognised	Yes	Not yet.	ADISA will have members in 8 EMEA countries and the US by the end of 2013. It is hoped to have a complete global network in place by the end of 2015.

Summary

It is the view of ADISA that the two only have a very minor overlap with the scope of 27001 being far broader than ADISA. The ADISA program is very narrow in scope and focussed on each and every element of the IT disposal service which could impact on the level of risk being introduced by the company delivering these services. Also the ADISA program has more rigorous on-going auditing to show compliance which is underpinned by the unannounced audit schedule and forensic tests. This gives customers of our members' confidence that at any time their supplier may undergo auditing which is specific to the delivery of the service being provided and via the monitoring service they are able to receive updates of these audits for their own internal compliance requirements.