

Automated configuration assurance, vulnerability assessment, change detection and compliance.

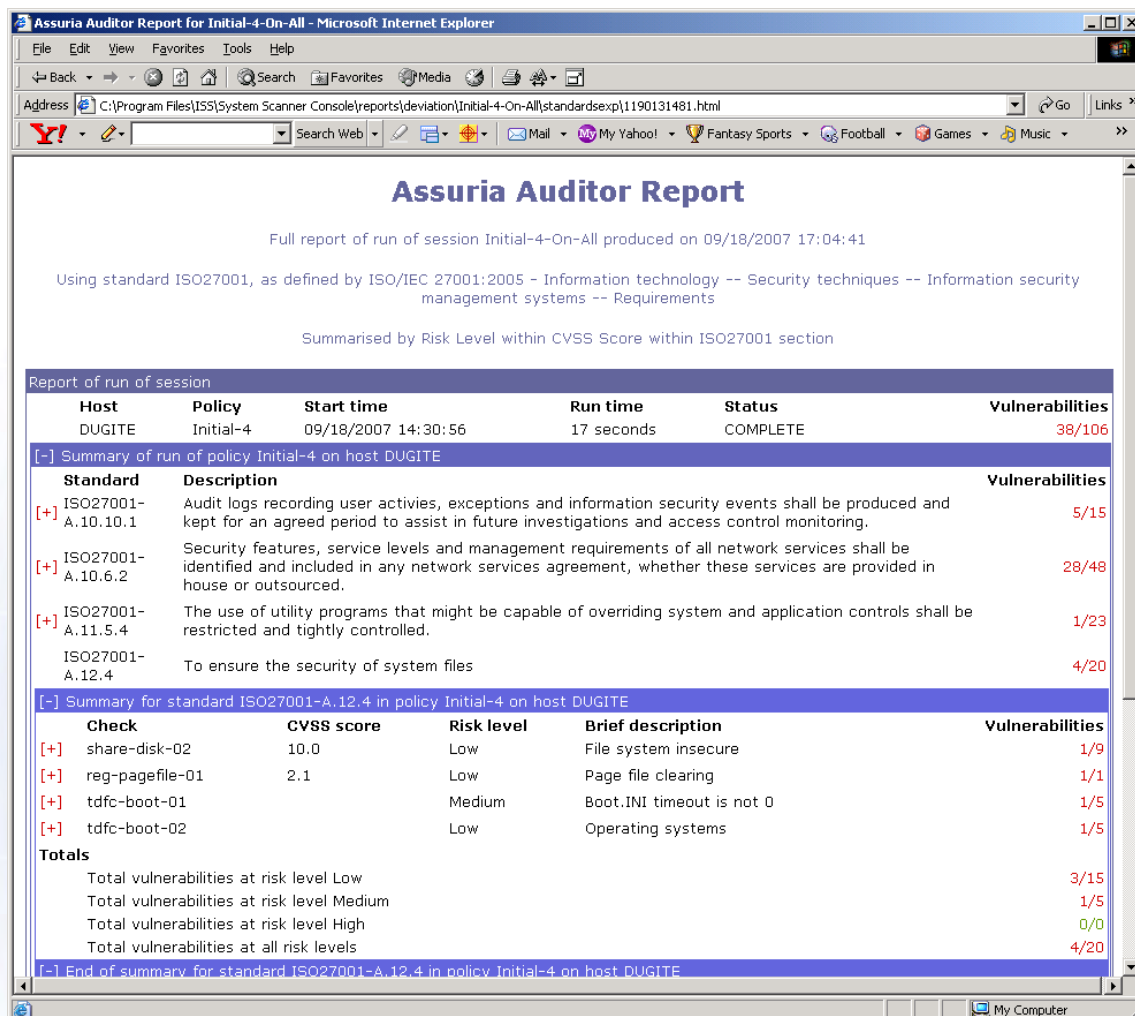
Assuria Auditor is deployed by hundreds of major enterprises in more than 45 countries and in a wide range of industries worldwide to provide vital information assurance and protection for critical business servers and to help maintain systems in a secure 'known state'.

For these organisations, Assuria Auditor provides a critical element of their IT security infrastructure, both physical and virtual.

Assuria Auditor is a market leader in countering the 'insider threat' to business integrity and a key solution for managing compliance to international regulatory standards such as ISO27001.

Through a flexible, distributed management framework, Assuria Auditor measures, manages and enforces server security policies and configurations using a host-to-network view of critical systems and servers, assessing host security, detecting and reporting system security weaknesses and recommending corrections.

System administrators and network management systems can also be alerted to Un-authorized changes to configurations, critical system elements and application components. Powerful change detection management features allow rapid assessment and reporting of suspicious or potentially troublesome changes.



Assuria Auditor Report

Full report of run of session Initial-4-On-All produced on 09/18/2007 17:04:41

Using standard ISO27001, as defined by ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements

Summarised by Risk Level within CVSS Score within ISO27001 section

Host	Policy	Start time	Run time	Status	Vulnerabilities
DUGITE	Initial-4	09/18/2007 14:30:56	17 seconds	COMPLETE	38/106
[-] Summary of run of policy Initial-4 on host DUGITE					
Standard	Description				Vulnerabilities
[+] ISO27001-A.10.10.1	Audit logs recording user activities, exceptions and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.				5/15
[+] ISO27001-A.10.6.2	Security features, service levels and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in house or outsourced.				28/48
[+] ISO27001-A.11.5.4	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.				1/23
ISO27001-A.12.4	To ensure the security of system files				4/20
[-] Summary for standard ISO27001-A.12.4 in policy Initial-4 on host DUGITE					
Check	CVSS score	Risk level	Brief description		Vulnerabilities
[+] share-disk-02	10.0	Low	File system insecure		1/9
[+] reg-pagefile-01	2.1	Low	Page file clearing		1/1
[+] tdfc-boot-01		Medium	Boot.INI timeout is not 0		1/5
[+] tdfc-boot-02		Low	Operating systems		1/5
Totals					
Total vulnerabilities at risk level Low					3/15
Total vulnerabilities at risk level Medium					1/5
Total vulnerabilities at risk level High					0/0
Total vulnerabilities at all risk levels					4/20
[-] End of summary for standard ISO27001-A.12.4 in policy Initial-4 on host DUGITE					



Assuria auditor

Assuria Auditor's methodology simplifies the creation of system security baselines for users, groups, shares, services and critical system files, and easily fits in with existing business processes. Fully scalable for enterprise installations, Assuria Auditor manages large agent populations.

The Assuria Auditor Advantage
Regulatory standards compliance. The comprehensive security database includes mappings of each of Assuria Auditor's 2500+ security configuration checks to appropriate references within international standards such as ISO 27001, ISO 17799, PCI and SOX. CVE and BID references are also provided, with CVSS scores where appropriate.

Configuration Policy Compliance. As well as monitoring compliance with external standards and accepted best practice in security configuration, Assuria Auditor can be tailored to specific requirements, allowing users to adjust checks and policies and write new checks to match the specific requirements of an organisation's security policy, thus ensuring full compliance.

Change Detection. Assuria Auditor allows the creation of system baselines and to monitor for any changes to those baselines, including changes to executables, data files and registry keys.

Vulnerability Assessment. Delivered with a comprehensive security knowledge base of more than 2500 checks and a library of best practice policies, Assuria Auditor detects potential vulnerabilities, assists with assessment of risk and recommends changes to mitigate those risks.

Distributed Management Framework. This framework enables operational access to the

Assuria Auditor agent community from anywhere on an enterprise network.

Fully Scalable. Large populations of agents can be managed from a single Assuria Auditor Console and agent-less scanning is available on some platforms, including MS Windows systems. Multi-layer management is also provided. Many Assuria Auditor installations comprise hundreds of servers.

Powerful and flexible Reporting. Standard reports, designed for both technical and managerial audiences, identify areas of security weakness or mis-configuration, the security implications and the possible consequences of security breaches resulting from such weaknesses, and appropriate remedies and solutions in detail.

Auto Updates Regular monthly security content updates ensure that hosts are protected from even the most recent vulnerabilities and exploits, also allowing rapid distribution of new product features.

Customisable Checks. Although a huge number of vulnerability, mis-configuration and other best practice checks are delivered as part of the comprehensive Assuria Auditor Knowledge Base, additional custom checks can easily be added via the Tcl scripting language.

Supported Platforms

Assuria Auditor Console Version 4.2.8:

- Windows Server 2003.

Assuria Auditor agents:

- Windows 2000, Windows Server 2003
- Solaris SPARC 7, 8, 9, 10
- AIX 4.3 and 5.1+
- HP-UX – PA-RISC and ITANIUM 11+
- Red Hat Enterprise Linux 3, 4, 5
- SuSE Enterprise Linux 10 X86
- SuSE Enterprise Linux 10 IBM Z series

Contact Assuria at:

Assuria Limited,
Science & Technology Centre,
University of Reading, Earley Gate,
Reading, RG6 6BZ, United Kingdom
W: www.assuria.com E: info@assuria.com
T: +44 118 935 7395 F: +44 118 926 7917

Assuria Partner