

## Network-wide compliance scores at a Glance

Imagine that each morning, when you reach the office, a customized, color-coded compliance spreadsheet awaits you!

With the information provided by Compliance Evaluator, you can easily determine the overall compliance status of your systems, and, if necessary, ask your IT Manager to investigate specific compliance-related issues.

**iSecurity Compliance Evaluator** provides managers, auditors and systems administrators a quick, yet comprehensive overview of their IBM i's level of compliance with PCI, SOX, HIPAA and other national, industry or enterprise-related regulations.

Using Compliance Evaluator, managers can:

- produce any number of compliance checklists
- select the contents of individual checklists
- structure the report to be produced
- attach varying weights to each report

Compliance Evaluator can be scheduled to run automatically, and its results can be emailed directly from your IBM i to the relevant persons in your organization.

### Features

- Built-in compliance checks for PCI, SOX, HIPAA etc.
- Easy to define site-specific compliance checks
- Color-coded Excel spreadsheet can be emailed directly from IBM i
- Schedule periodic compliance checks
- Produces single score per system and specific scores per topics
- Each item & topic can be allocated individual importance
- All scores displayed as percentages
- Several report templates provided, with different levels of detail
- Unlimited number of reports
- Compliance data presented in both detailed and/or summary format
- User-friendly GUI

Monday, October 26, 2009 Report Filter: T..... Summary (NonBlanks) Exceptions

**iSecurity Compliance Evaluator**  
**Sample PCI Compliance Report**

System: **S720**      **SPROD**  
 Compliance Rating: **65%**      **89%**

Item	Topic	Name	Relative Importance	Current Value	Optimal Value	Rank for Topic	Current Value	Optimal Value	Rank for Topic
<b>User Profile Attributes</b>			<b>44%</b>			<b>40%</b>			<b>94%</b>
User Profiles with *ALL QBJ authority				7	0-5		5	0-5	
Users with no password				4	0-10		2	0-10	
Powerful Users				12	0-10		12	0-10	
<b>All System Values Information</b>			<b>35%</b>			<b>68%</b>			<b>73%</b>
Previous end of system indicator *SYCTL QABNDPMSW				0	1		0	1	
Allow object restore option *SEC QALWOBJRST				*ALL	*ALL		*ALL	*ALL	
Require digit in password *SEC QPwDRQDDGT				0	1		1	1	
Minimum Password Length *SEC QPwDMINLEN				5	6-128		0	6-128	
<b>Network Activity</b>			<b>21%</b>			<b>88%</b>			<b>83%</b>
FTP Requests to Production Libraries				4	0-4		2	0-3	
FTPLQIG - FTP Server Logon (*)				12	0-10		4	0-5	
FILSRV - File Server (*)				2	0-10		4	0-3	
Native Access to Production Libraries				2	0-5		2	0-3	

## Compliance Evaluator Reports

Compliance Evaluator reports provide an overall compliance score, as well as specific ratings for topics comprising the compliance standard being evaluated. Individual topic scores are based upon the relative importance of the items comprising the topic and, of course, the item values themselves. Status checks are provided for items such as System Values, Network Attributes, User Profile Attributes and Object Authorities.

The result is a colorful, user-friendly Excel spreadsheet which provides three different views: general (detailed), summary and exception-only displays.

Compliance Evaluator reports are based upon both static system data and time-sensitive data covering actual network transactions. Together, these can highlight unexpected changes in user or system activity, such as how often users access production or system files, how many objects of a given type were accessed during a specific time range, etc. The reports include operational information from QAUDJRN and from actual network activity. Virtually any type of information can be included.

A number of pre-defined compliance checks relating to PCI, SOX, HIPAA and other common security regulations are supplied with the product. Each report can relate to a single server, selected servers or all servers in the enterprise. In addition, site-specific compliance checks can be defined by users through an advanced Eclipse-based GUI.

The results of queries are automatically saved, and can serve as the basis for historical comparisons of compliance status over time.

The image displays three overlapping screenshots of the Compliance Evaluator software interface. The top window shows the 'Checks' section with a tree view on the left and a list of checks in the center. The middle window shows a 'System Values' report with a table of system values. The bottom window shows a 'System Values' report with a table of system values.

Name	Type	Description	System	Importance
QPRTRMT	*MSG	Print text	*ALL	10
QPWDCHEGRLK	*SEC	Minimum time between password changes	*ALL	1000
QPWDEXPTY	*SEC	Password expiration interval	*ALL	1000
QPWDCPWRN	*SEC	Password Expiration Warning	*ALL	1000
QPWDLTATZ	*SEC	Limit adjacent digits in password	*ALL	1000
QPWDLTCHR	*SEC	Limit characters in password	*ALL	1000
QPWDLTREP	*SEC	Limit repeating characters in password	*ALL	1000
QPWDLVL	*SEC	Password level	*ALL	1000
QPWDMXLEN	*SEC	Maximum password length	*ALL	1000
QPWDMNLEN	*SEC	Minimum password lengths	*ALL	1000
QPWDPDSDF	*SEC	Limit password character positions	*ALL	1000
QPWDRQDGT	*SEC	Require digit in password	*ALL	1000
QPWDRQDQD	*SEC	Require password control	*ALL	1000
QPWDRULES	*SEC	Password Rules	*ALL	1000
QPWDLDPGH	*SEC	Password validation program	*ALL	1000
QPWRDUNLMT	*SYSCTL	Maximum time for PWRDWHNSYS *DIRAED	*ALL	1000
QPWRKSTPL	*SYSCTL	Automatic IPL after power restored	*ALL	1000
QRQDDEGREE	*SYSCTL	Parallel processing degree	*ALL	1000
QRQYTLMT	*SYSCTL	Query processing time limit	*ALL	1000
QRCLPLSTG	*ALC	Retain spool storage	*ALL	1000
QRRTBNSSEC	*SEC	Retain server security data	*ALL	1000
QRMTPL	*SYSCTL	Remote power on and IPL	*ALL	1000
QRHTSIGN	*SEC	Remote sign-on control	*ALL	1000
QRMTSKVATR	*SYSCTL	Remote service attribute	*ALL	500

Sample Compliance Evaluator Screenshots