

## Essential Questions for Evaluating IT GRC Solutions

The Leader in Integrated Security, Risk & Audit Management

eIQnetworks, Inc. • 31 Nagog Park • Acton, MA 01720 • t. +1 978.266.9933 • f. +1 978.266.0004 • [www.eIQnetworks.com](http://www.eIQnetworks.com)



## Table of Contents

<b>Introduction</b> .....	<b>3</b>
<b>Question 1: Data Sources</b> .....	<b>4</b>
<b>Question 2: Compliance Support</b> .....	<b>5</b>
<b>Question 3: Integration</b> .....	<b>6</b>
<b>Question 4: Correlation</b> .....	<b>7</b>
<b>Question 5: Dashboards</b> .....	<b>7</b>
<b>Question 6: Reporting</b> .....	<b>8</b>
<b>Question 7: Data Archival</b> .....	<b>9</b>
<b>Question 8: Architecture and Scalability</b> .....	<b>9</b>
<b>Question 9: Performance and Scalability</b> .....	<b>10</b>
<b>Question 10: Total Cost of Ownership</b> .....	<b>11</b>
<b>Summary</b> .....	<b>12</b>
<b>Exhibit A: IT GRC Solution Checklist</b> .....	<b>13</b>



## Introduction

eIQnetworks has developed this document as an evaluation guide to help ease the process of evaluating IT governance, risk and compliance (IT GRC) management solutions for your enterprise. By using the questions offered in this guide as a baseline for evaluating different solutions, you will be able to quickly identify the requirements for IT GRC products and platforms that are best suited to your organization.

### ***IT GRC Evaluation Fundamentals***


Effective IT GRC management solutions allow you to strengthen control of your enterprise's compliance with regulations, standards and best practices such as PCI DSS, COBIT, GLBA, ISO 27002, HIPAA, CA 1386, FISMA, GLBA, NERC, SOX, NIST SP 800, and others. It is likely that you also need to monitor compliance with your own proprietary IT criteria, such as service level agreements or business partner agreements.

In a nutshell, you need to:

- Identify and track organizational compliance against criteria from multiple regulations, standards and best practices, both public and proprietary
- Establish a compliance baseline and monitor it continuously
- Detect and analyze compliance gaps promptly as they occur
- Mitigate compliance gaps quickly and efficiently
- Generate audit reports for each regulation, standard and best practice
- Do all of the above cost-effectively

Most IT GRC solutions advertise that they can help you execute these essential tasks. However, upon closer inspection, you will discover important differences in how effectively, completely and efficiently they are able to help you. To make the most appropriate and justifiable solution selection, you should establish an understanding of these important differences including:

- The range of data sources collected and correlated
- The range and depth of support for regulations, best practices and propriety business drivers
- The degree of integration with an enterprise security management (ESM) solution
- The effectiveness of the data correlation
- The utility of dashboards
- The availability and utility of out-of-the-box reports
- The cost-effectiveness and efficiency of data archiving

- 
- The scalability of the solution architecture
  - The overall performance and scalability
  - The total cost of ownership

---

NOTE: [Exhibit A](#) presents these key difference areas in a handy checklist that you can use as a reference during your IT GRC solution evaluation.

---

## Question 1: Data Sources


*Does the IT GRC solution provide comprehensive monitoring of all your environment's information assets out of the box without developing custom connectors?*

Most regulations, standards and best practices require that organizations monitor a wide and diverse range of IT assets including operating systems, hardware devices, network traffic, applications and databases. This requirement helps provide a level of insurance against costly re-engineering that may result from continually evolving mandates. As regulations, standards and best practices evolve, the number of required data sources may well expand. Consequently, it is better to support a diverse set of data sources upfront than to have to re-engineer or replace the solution as requirements evolve and new criteria emerge.

Data sources also impact how quickly organizations can address compliance gaps. That is, if rapid compliance gap detection and mitigation is important, a complete set of environmental data needs to be collected and analyzed non-stop in real time. Rapid analysis of compliance problems is harder to achieve when working with a limited set of data points; multiple data points are needed to provide a broader picture and a more complete context for the compliance gap. To be specific, the solution should continuously collect and correlate data from a range of data sources, including:

- **Log** data, fundamental for security event detection and analysis
- **Configuration** data with periodic snapshots across network devices and hosts
- **Asset** data on all devices and hosts including hardware and software system specifications, applications and processes
- **Performance** data such as network traffic, data flow and CPU utilization
- **Vulnerability** data across network devices and hosts
- **NetFlow, C-Flow and other network traffic pattern** data to detect anomalous network behavior by users

Some IT GRC solutions can support more than just log and vulnerability data but at some cost. If support for data collection from all the important data sources is not included with a solution out of



the box, it must be either purchased as an add-on module or developed in a custom connector engineering project that can add hundreds of hours—and thousands of dollars—to the cost of deployment.

## Question 2: Compliance Support

***Does the IT GRC solution support the regulations, standards or best practices that are important to you, and does it support them in a robust fashion?***

This question may seem obvious, but you must have a complete answer to this question before proceeding with an evaluation. As implied in the question, there are both breadth and depth aspects to supporting regulations, standards and best practices. Since today's IT compliance environment is characterized by a broad array of regulations, standards and best practices, breadth refers to the range of criteria covered by an IT GRC solution. While vendors may claim support for a wide range of compliance drivers, your evaluation should primarily focus on those regulations, standards and practices that are critical to your organization. While some organizations may have a very broad range of compliance drivers, most organizations are impacted by one or two key drivers. For example, an online merchant most likely needs to comply with PCI DSS, but perhaps not with HIPAA. Likewise, a bank focused on attaining GLBA compliance may not need to be concerned with FISMA.

Once you have identified the solutions that claim support for the regulations, standards and best practices relevant to your organization, you should investigate the depth of the support. That is, you should determine to what degree—completely, partially or barely—the solutions support the relevant regulations, standards and best practices. To determine this, you need to first understand the relevant criteria and then ask vendors exactly how their solutions monitor, measure and report on these important criteria. For example, when the Sarbanes-Oxley (SOX) law went into effect, many vendors designed tools to allow SOX-impacted companies to automatically monitor and report on access controls within their financial software systems. Vendors of these tools claim their products are “SOX compliance solutions” but, in fact, they only support compliance management of ***one small part of the overall set of SOX requirements***. As this illustrates, you should determine whether a vendors' product is a true ***platform*** for IT GRC management or only a ***tool*** that partially supports a requirement and must work within the context of a larger framework provided by another solution.

It is also important to understand that there are two general types of controls specified by regulations, standards and best practices: ***technical*** and ***logical*** controls. Technical controls are those for which evidence can be automatically generated through a collection mechanism, such as log, configuration, asset, performance and vulnerability data. Logical controls, on the other hand, are not verifiable through technology because they generally specify the need for business processes such as security policies and procedures. Because compliance evidence is not automatically generated for logical controls, these controls must be manually attested to.



It follows then that a comprehensive IT GRC solution must support not only technical control evidence, but also manual logical control attestation across the enterprise. While you may be tempted to focus mostly or entirely on technical controls, do not overlook logical controls. A sound and complete IT GRC solution should offer robust features that enable the monitoring and reporting of both logical and technical controls.

Finally, investigate the method by which an IT GRC solution provides support for a regulation, standard or best practice. Support is most comprehensive if it is based upon a compliance library. The compliance library makes possible the comparison of the regulation's requirements with actual values collected from the enterprise. If the library contains both technical and logical controls that map directly to audit requirements for a regulation, the solution provides very robust support for monitoring and measuring an organization's compliance with that regulation.

### Question 3: Integration

***Does the IT GRC solution integrate with a robust ESM solution to the extent that built-in data feeds map directly to regulatory controls?***

An ESM solution collects and analyzes data from hosts, applications, network devices and security appliances to detect and mitigate security incidents. Most of these solutions collect, archive and analyze only log and vulnerability data from the infrastructure. While focusing on this data is, in fact, a great starting point for an ESM solution, it becomes vastly more meaningful and helpful when examined alongside the other security and compliance data listed in Question 1: asset, performance, configuration and NetFlow data. Thus, a very **robust** ESM solution also collects and correlates data from a broad range of data sources.

It is also important that the data be collected and analyzed in real time or near-real time. If data is collected and analyzed only periodically, valuable time that could be spent mitigating a security breach could be lost. Thus, a robust ESM solution provides round-the-clock, real-time data collection and analysis.

Now, if you consider how an effective IT GRC solution would work, you quickly realize that an IT GRC solution's effectiveness also depends directly upon the comprehensive collection and correlation of data from across the enterprise in real time. Therefore, the two solutions—IT GRC and ESM—are truly complementary and the close integration of the two solutions allows the IT GRC solution to perform considerably better across all key difference areas. This close integration should extend to having the built-in data feeds that map enterprise assets directly to regulatory, standard and best practice controls.



## Question 4: Correlation

***Does the IT GRC solution automatically and simultaneously correlate data both across multiple data sources and across time?***

Several IT GRC solutions collect data from multiple sources and may also automatically correlate current data with historical data. Correlation with historical data is important because to automatically detect changes in compliance, an IT GRC solution must be able to compare current information with historical information to determine that something has changed.

This can be simplified into two steps. First, a baseline compliance posture must be established. If the coverage of data sources is broad, the baseline compliance posture will be more comprehensive and will cover a greater the range of regulations, standards and best practices. Second, once the baseline is established, the detection of changes in compliance and the subsequent issuance of alerts come into play. Detection and alerting become significantly more sensitive and effective if the data is automatically and simultaneously correlated *across all sources over a period of time*. While some solutions do collect data from multiple sources and also correlate data over time, few solutions are able to simultaneously correlate data across multiple sources over time. Combining data source breadth with historical depth provides a more comprehensive, realistic baseline and sensitive gap analysis, both of which are of great value to compliance auditors.

## Question 5: Dashboards

***Does the IT GRC solution include dashboards that allow compliance auditors to visually track compliance trends over time and to drill down to compliance gap root causes quickly?***

An enterprise's compliance gaps and trends must be able to be viewed and, when necessary, investigated quickly. The ability to conduct these visual investigations is enabled by intuitive dashboard features such 3D visualization, drilldown and customization.

An effective IT GRC solution must also enable investigative analysis by multiple teams across all the data sources: log, vulnerability, configuration, asset, performance and NetFlow. In their investigative analysis of a deficit in compliance posture, the teams should also be able to move easily between these sources to view all related and relevant data in an at-a-glance dashboard. This requires data integration enabled by a single platform that collects, correlates and analyzes all relevant security and compliance data.

If information from all important security and compliance data sources is presented to multiple teams through a single console, efficient and effective collaboration can be achieved. In this case, solution console access can be granted based on the user's role—be they a network operations center (NOC), an information security operations center (SOC), or an audit team member. The console, in turn,



must present the data in a way that is meaningful for each of the different roles. This means that at-a-glance dashboards should be customizable to meet varying needs. For example, a NOC team member should be able to obtain operational metrics through the console while a SOC team member uses the same dashboard to view security metrics. In this way, different teams can effectively collaborate by viewing different metrics through the same interface. A solution that allows all teams to look at the same data collaboratively removes obstacles to resolving problems collaboratively and expeditiously.

## Question 6: Reporting

***Does the IT GRC solution deliver all the out-of-the-box reports that it advertises and do the reports provide useful, actionable information?***

As a fundamental component of any IT GRC solution, reporting should comprehensively meet the differing requirements of NOC, SOC and Audit teams. These teams typically mandate that GRC reports be useful and actionable, incorporate all important compliance data and be out-of-the-box accessible in different formats based on role. Let's briefly examine each of these requirements in more detail.

Reports should be useful and actionable, presenting a high-level summary of all compliance data so a manager or an analyst can immediately see the big picture and understand the context of any reported compliance gaps. The solution should then provide the ability to easily drilldown into more detail to quickly determine root cause of the gap.

To be cost-effective, the IT GRC solution should also provide a variety of reports right out of the box. Many vendors claim—often in obfuscating terms—that their solutions include a variety of reports. Their customers, however, soon discover only a small set of reports are provided out of the box and the generation of additional reports requires either a costly third-party reporting tool or, even worse, custom coding. This can prove both costly and timely as customers are often forced to write their own SQL queries or hire the vendor's professional services to get the reports they need.

As a complement to its ability to report data across all sources, an IT GRC solution should deliver reports based on user role, as it does with dashboards. That is, the solution should allow a user, regardless of team affiliation, to access the solution and obtain a report of data meaningful to them from anywhere at anytime based on the privileges assigned to the user's role. Finally, the solution should provide automated audit report generation with the flexibility to deliver reports in various formats such as HTML and PDF.



## Question 7: Data Archival

***Does the IT GRC solution archive all data, using existing SAN, NAS or DAS storage media, to support historical analysis?***

As discussed above, the real-time collection and archiving of data for historical comparison purposes is the hallmark of a comprehensive ESM solution which, in turn, is the foundation of a complete IT GRC solution. Because the collection of large quantities data across the enterprise can cause storage capacity issues, it is important that the IT GRC solution archive the collected multi-silo data *without* creating new storage management headaches. That means the solution should take advantage of the existing storage infrastructure by archiving data on any storage media whether it be DAS, NAS or SAN.

In a large enterprise network, the data generated over months and across thousands of nodes can be quite voluminous so, to save storage space and enhance data security, an ESM solution should support compression and encryption of all the data collected over long periods of time. In short, when evaluating an IT GRC solution's data archival features, you should look for the ability to:


- **Compress** data to use storage space efficiently
- **Encrypt** data transmission to maintain data integrity
- **Piggyback** on existing DAS, NAS and SAN infrastructures for data archival
- **Archive** data for long time periods

This set of archiving features allows your company to cost-effectively meet security, risk and audit management requirements.

## Question 8: Architecture and Scalability

***Can the IT GRC solution architecture scale to easily support an increasing footprint of compliance criteria?***

The footprint of IT compliance criteria will grow over time. In other words, as the regulations, standards and best practices evolve, they add new logical and technical criteria that must be met across the enterprise. A sound IT GRC solution, therefore, must be flexible enough to incorporate change. A comprehensive solution easily accommodates evolving criteria by offering tools such as wizard-based policy mapping which allow a user to add and modify regulations and best practices as they emerge and evolve. For example, as both internal and external auditors complete their evaluations, the IT GRC solution should be flexible enough to allow controls—both technical and logical—to be modified to adapt to the outputs of auditing efforts.



Moreover, this need for flexibility applies not only to externally-sourced regulations, standards and best-practices but also to the creation, approval and maintenance of dynamic *internal* compliance requirements such as those specified by service level agreements and business partner agreements. As organizations mature and business processes change, the need to support a broad range of truly customized criteria will change. New business partners will mandate specific controls as a condition of doing business with them and internal constituents will continually seek more defined service levels from IT. Both groups will then require evidence of compliance with these controls. An IT GRC solution must be flexible enough to define, track, and report on these proprietary compliance drivers as well as external drivers.

## Question 9: Performance and Scalability

***How is solution performance impacted by the physical growth of the network infrastructure and the logical growth of the historical evidence library?***

It is essential that an IT GRC solution deliver high performance out of the box because the demands on a successful solution will only increase over time. To support increasing demands, the chosen solution should be able to handle at least tens of thousands of correlated compliance requirements per second out of the box.

In addition, as the physical network infrastructure expands with organization growth, an IT GRC solution must be able to scale to support both compliance criteria footprint growth and physical network growth.

Some important measures of performance scaling for an IT GRC solution are:

- Distributed IT GRC server performance that scales effortlessly to reach required performance levels as the compliance footprint expands
- Real-time, multi-silo IT GRC performance scaling that handles the collection and analysis of data in real time from the organization's multiple data silos

Two final comments on IT GRC solution scalability:

- The solution's scalability should be cost-effective and not come at significant incremental expense as would happen, for example, if the solution required a dedicated DBA.
- As the scope of the IT GRC solution extends to new types of network devices, operating systems, applications and databases, the solution should have a built-in ability to adapt to new data formats and data structures in order to avoid the expense of custom programming.



## Question 10: Total Cost of Ownership

### *What is the true total cost of ownership (TCO) of the IT GRC solution?*

While initial purchase price is always a consideration, it is the ongoing maintenance costs that render a solution either cost-effective or a bad purchase decision. For an IT GRC solution specifically, there are four ongoing cost elements that can drive the TCO to unreasonable levels: the need to hire additional staff, the need for additional consulting services, purchasing third party applications and licensing per user. Be sure to ask both vendors and references about the following potential hidden costs:

- **A dedicated DBA** – Many IT GRC solutions are based on a relational SQL database which may require a dedicated database administrator. What type of database is used by the solution and is a dedicated administrator required?
- **Additional management staff for new nodes** – Additional people may be required to manage the IT GRC component on new nodes as they are added to the network and to the scope of the solution. Are the node agents self-managing or do they require management?
- **Custom connectors** – Adding an unsupported device to an ESM network often requires that a custom collector be created to collect data from that device. Does adding an unsupported device require returning to the vendor for custom design work or can it be done in-house?
- **Additional applications** – Additional applications may be required to make an IT GRC solution truly useful across the enterprise. Examples of such additional applications include report server engines and applications to report on vulnerability, asset, configuration or NetFlow data drawn from across the network. Consider how your users will expect to deploy and use the application. Are any additional third-party applications required to make the solution effective and useful?
- **Additional licenses** – As nodes and associated users are added in the future, licensing cost can soar if they are licensed individually. Some IT GRC solutions charge a per-user fee. Are users licensed in tiers or separately?

To eliminate or minimize these hidden expenses, you need an IT GRC solution that takes a broader, more integrated platform approach: an approach that supports both your security and compliance needs with sufficient flexibility to accommodate enterprise IT growth without adding significant IT expense.



## Summary

This document has been designed to provide you, an IT GRC decision maker, with an explanation of key topics and questions to assist you in navigating the murky waters of an IT GRC solution evaluation. By following this guidance, your overall product analysis, understanding and recommendations should be more convincing and sound. The IT GRC solution that remains standing at the end of this evaluation should prove to be the best solution for your organization. With it, comprehensive security and compliance management will be achievable through end-to-end data collection and correlation, high performance and maximum scalability at a minimal TCO that enables you to:

- Establish a baseline compliance posture
- Continuously monitor for compliance gaps
- Promptly identify and mitigate gap root causes
- Deliver streamlined audit reports for each regulation, standard and best practice

---

### About eIQnetworks

eIQnetworks, Inc., a leader in integrated security, risk and audit management, enables enterprise, government and MSSP customers to effectively meet security and compliance challenges through a unified framework. More than 2,700 organizations worldwide rely on the power of eIQ's enterprise security management and IT governance, risk and compliance solutions to proactively detect security breaches, speed incident remediation and support evolving best practices and compliance regulations across the enterprise. For additional information, please visit [www.eIQnetworks.com](http://www.eIQnetworks.com) or call +1 877.564.7787.

## Exhibit A: IT GRC Solution Checklist

Evaluation Topic	Specific Questions	Notes
Data Sources	<ul style="list-style-type: none"> <li>• All information assets supported out of the box?</li> <li>• Log, vulnerability, configuration, asset, performance, NetFlow, C-Flow, etc.?</li> </ul>	
Compliance Support	<ul style="list-style-type: none"> <li>• Support regulations and best practices important to you?</li> <li>• Complete or partial support?</li> <li>• Platform or tool?</li> <li>• Both technical and logical compliance controls supported?</li> <li>• Compliance library?</li> </ul>	
Integration	<ul style="list-style-type: none"> <li>• Robust ESM and IT GRC solutions?</li> <li>• Real-time data collection?</li> </ul>	
Correlation	<ul style="list-style-type: none"> <li>• Simultaneous and automatic correlation across all sources and time?</li> </ul>	
Dashboards	<ul style="list-style-type: none"> <li>• Provide compliance trends over time?</li> <li>• 3D visualization, drilldown and role-based customization?</li> <li>• Single console for multiple teams?</li> </ul>	
Reporting	<ul style="list-style-type: none"> <li>• Reporting based on role?</li> <li>• High-level summary with drilldown?</li> <li>• Variety of reports out of the box?</li> </ul>	
Data Archival	<ul style="list-style-type: none"> <li>• NAS, DAS and SAN supported?</li> <li>• Encrypt and compress store?</li> </ul>	
Architecture and Scalability	<ul style="list-style-type: none"> <li>• Meet evolving regulations?</li> <li>• Ability to manage internal policies?</li> </ul>	
Performance and Scaling	<ul style="list-style-type: none"> <li>• Events per second?</li> <li>• Performance scales?</li> <li>• Adapts to new data formats?</li> </ul>	
TCO	<ul style="list-style-type: none"> <li>• Additional staff?</li> <li>• Third party applications?</li> <li>• Custom connector design?</li> <li>• Additional licenses?</li> </ul>	

© 2008, eIQnetworks, Inc. eIQnetworks and the eIQnetworks logo are registered trademarks of eIQnetworks, Inc. All other trademarks, servicemarks, registered trademarks or registered servicemarks are the property of their respective owners. All rights reserved.