CDOs Should Use IT Governance and Risk Compliance Management to Advance Compliance

Barry Runyon

Care delivery organizations (CDOs) are well aware of the threats to the privacy and security of their protected health information (PHI — see Note 1). With the likelihood of increased proactive auditing this year by Centers for Medicare and Medicaid Services (CMS) under the Health Insurance Portability and Accountability Act (HIPAA), healthcare provider CIOs must consider a more comprehensive approach to compliance as characterized by IT governance, risk and compliance management (GRCM) systems to help them determine the effectiveness of their security and compliance planning and spending.

Key Findings

- Gartner believes that, starting in 2008, the U.S. CMS will be more aggressive and proactive in auditing HIPAA compliance by CDOs.
- IT GRCM is an emerging category of products that can improve a CDO's audit posture, reduce associated reporting costs and help the organization more regularly assess its risk and real compliance levels.
- A CDO that has implemented sound vulnerability management (that is, those processes and technologies used to discover and address security weaknesses before they are exploited, including patch management, security configuration management, and security information and event management [SIEM]) should be well positioned to implement IT GRCM technology.

Recommendations

- Revisit the enterprise security plan to ensure that current security requirements, along with the corresponding policies and technical controls that support that plan, remain appropriate to truly anticipated threats and vulnerabilities.
- Plan to use IT GRCM to determine the efficacy of the enterprise security plan, and to develop the capacity to demonstrate compliance with HIPAA's privacy and security rules, as well as The Joint Commission's Information Management specifications.
- Investigate IT GRCM systems that have received a positive or strong positive rating in Gartner's "MarketScope for IT Governance, Risk and Compliance Management, 2008" — ideally, finding one that has an established healthcare provider vertical with active references.
WHAT YOU NEED TO KNOW

IT GRCM includes the management, measurement and reporting of IT policies and controls put in place to address risk, and to ensure privacy, security and regulatory compliance. IT GRCM solutions offer a core set of functionality to assist the CDO in defining its IT policies, managing policy content, mapping policies to the various technical controls, and automating the auditing and regulatory reporting process.

ANALYSIS

CDOs are in urgent need of a systematic approach to compliance management. CDO leadership must be able to determine their compliance posture at any point in time, retrospectively, or in near real time, by reviewing compliance reports and dashboard output that looks at realistically anticipated threats, the policies that are currently in force, and the technical controls that are being used to protect important infrastructure and information assets.

IT GRCM encompasses the workflow, content and technologies that assist with risk management and compliance requirements. Without a holistic approach that automates the collection, analysis and presentation of policy, process and control data — the proof of due diligence and a standard of due care — more CDOs will suffer damage to their reputations, accreditation status and bottom lines, as compliance lapses, such as those outlined later in this document, become more commonplace (see Note 2).

What Is a Control?

A control is a policy, process, procedure or technology that addresses a reasonably anticipated risk. Firewalls, secure e-mail, content filters, intrusion detection and protection systems, log monitoring systems, virtual private networks, and network access control appliances are examples of IT security controls that address the risk of unauthorized access to enterprise systems and information.

The HIPAA mandates that certain types of technical controls be in place in the CDO to control logical and physical access, user authentication, and authorization as well as for auditing purposes. An enterprise security plan and the various guidelines, standards, policies, and procedures that support and implement the plan are also considered controls.

The term "policy" can have a couple of different meanings. It can serve as an all-encompassing term for documents that set forth corporate intent, or it can refer to a set of detailed corporate mandates. An organization typically has many policies on the books on how business is done and what activities are considered appropriate or inappropriate. Privacy and security policies in CDOs generally outline the behavior expected of the users of enterprise business and clinical systems — particularly those that house PHI.

GRCM seeks to bridge the gaps that exist between the risks the plan addresses, its associated policies, and the technical controls that monitor and manage the various enterprise systems and infrastructural components.

GRC, GRCM and IT GRCM

"Governance," "risk" and "compliance" (collectively known as GRC) are general terms that can apply to a host of business requirements, vendor products, and IT programs and initiatives. More often, GRC refers to the use of content management, reporting, workflow, and automation tools and technologies in support of corporate governance, as well as IT governance, risk management
and compliance. In the CDO, GRC requirements are determined by regulations, such as HIPAA; The Joint Commission; local, state and regulatory mandates; and — where appropriate — Sarbanes-Oxley.

GRCM is about the management, monitoring, measuring and reporting activities associated with the various policies, processes, procedures and technical controls that GRC encompasses. GRCM comes in two flavors: financial and IT. Financial GRCM refers to GRCM activities associated with enterprise financial systems, such as audits, segregation of duties, business rule management, operational risk management and so on.

IT GRCM is about management, monitoring, measuring and reporting — but also about IT controls versus financial controls. IT GRCM refers to software systems that have document management capabilities, workflow, survey and reporting capabilities, an asset repository, and dashboard functionality. IT GRCM may also include the policy content that is specific to IT controls, and support for the automated measurement and reporting.

The IT GRCM market is composed of vendors that provide software products that help organizations proactively measure and manage their IT technology and process controls. Typically, these software systems provide functionality needed to:

- Define IT policies, processes and controls (based on best practices)
- Manage policy content
- Map policies to process and technical controls
- Automate the measurement of process and technical controls
- Evaluate the risk of noncompliance
- Automate the auditing and regulatory reporting of these elements

IT GRCM solutions also may take input from controls automation and monitoring tools, such as configuration management tools, identity and access management, and SIEM monitoring and log management tools.

**IT GRCM Core Capabilities**

CDO IT professionals responsible for enterprise security, risk management and compliance will find IT GRCM tools and vendors challenging to identify and evaluate. Some control and compliance vendors claim to offer IT GRCM solutions. To make the selection process easier, Gartner has set forth nine core capabilities required to define, manage, measure and report on IT controls. They are:

1. **Controls and policy mapping** — This is fundamental to IT GRCM and refers to the ability of a system to map the enterprise's privacy and security policies as well as the manual and technical controls to best-practice security frameworks, such as the International Standardization Organization (ISO), Information Technology Infrastructure Library (ITIL) and Control Objective for Information and Related Technology (CobiT), and the control objectives outlined by HIPAA and The Joint Commission.

2. **Policy distribution and training attestation** — This refers to the distribution of privacy and security policies along with a method to validate that the policy was reviewed and understood and that the user intends to comply.

3. **IT control self-assessment and measurement** — This refers to the tool's ability to create, disseminate and manage control self-assessments in the enterprise.
4. **IT GRCM asset repository** — This describes the ability to discover, define, classify and group IT assets — servers, desktops, network components and the like.

5. **Automated general computer control (GCC) collection** — This refers to the ability of the tool to import, collect and measure configuration settings, vulnerability and identity auditing information as well as other general computer controls information.

6. **Remediation and exception management** — This refers to the ability to track the life cycle of identified gaps and authorized exceptions (in other words, residual risk).

7. **Basic compliance reporting** — This refers to the tool’s ability to create compliance reports that will satisfy in-house and industry auditors.

8. **IT compliance dashboards** — These make it possible to make better decisions based on up-to-date compliance information collected from key points within the enterprise workflow and key components of the enterprise infrastructure.

9. **IT risk evaluation** — This describes the tool’s ability to demonstrate the enterprise’s current state of process and technical control compliance, known vulnerabilities, residual risk and so on.

**Other IT GRCM Inputs**

External threats had the CDO’s attention earlier in this decade, but the focus will increasingly turn to internal threats. With that in mind, IT GRCM systems should also be used to import information from systems such as:

- **Incident management** — A system that implements a methodology or process for capturing and responding to privacy and security incidents.

- **Consent management** — A system or set of policies for allowing patients to determine what health information they are willing to permit a CDO to access and view.

- **Disclosure tracking** — A system to assist the CDO in maintaining and reporting on the history of PHI disclosures concerning a patient.

- **Log management** — CDOs should also adopt a more-deliberate log management approach. Security information and event management (SIEM) tools collect, aggregate and correlate data from disparate audit sources to support two main functions:
  1. Increasing enterprise incident response capabilities by providing situational awareness
  2. Providing security information management for long-term trending, analysis and regulatory compliance

**IT GRCM Vendors**

Based on the nine critical capabilities outlined above as well as the ability to support certain key IT GRCM use cases (self-assessment, audit support and automated GCCs), Gartner has identified the following vendors as important IT GRCM players:

- Agiliance
- Archer Technologies
- Brabeion Software
Despite substantial investments in time and capital, most CDOs struggle to find a systematic way to define, manage and enforce the privacy and security policies and controls that are required to address reasonably anticipated threats and to comply with HIPAA and other industry mandates. Like most things IT, there is no silver bullet in this area — IT GRCM involves people, processes, policy and technology.

The IT GRCM tools attempt to provide a framework to bring these areas together, and Gartner is attempting to influence these requirements. Gartner has defined IT GRCM core functionality at a high level in an attempt to clarify the marketplace.

CDOs should pilot or purchase an IT GRCM system that, at a minimum, integrates best with the enterprise's technical controls infrastructure, offers a flexible document management and workflow capability, and has HIPAA regulatory content and policy templates. IT GRCM tools can help the CDO to analyze and decrease security risk and determine the effectiveness of overall programs — and eventually, reduce the overall cost of compliance. IT GRCM can assist the CDO in determining, in more-concrete terms, how secure the enterprise is and whether it has the right practices, policies and controls in place.

RECOMMENDED READING

"IT GRCM Functions Defined"
"Critical Capabilities for IT GRCM Tools"
"Tutorial for Protected Health Information: Going Beyond Compliance"
"Refresh HIPAA Security Assessments to Prepare for More Proactive Audits"

Acronym Key and Glossary Terms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDO</td>
<td>care delivery organization</td>
</tr>
<tr>
<td>CMS</td>
<td>Centers for Medicare and Medicaid Services</td>
</tr>
<tr>
<td>CobiT</td>
<td>Control Objectives for Information and Related Technologies</td>
</tr>
<tr>
<td>GCC</td>
<td>general computer control</td>
</tr>
<tr>
<td>GRC</td>
<td>governance, risk and compliance</td>
</tr>
<tr>
<td>GRM</td>
<td>governance, risk and compliance management</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>ITIL</td>
<td>IT Infrastructure Library</td>
</tr>
</tbody>
</table>
SIEM  
security information and event management

Note 1
 Protected Health Information

PHI is considered any oral or recorded information relating to the past, present, or future physical or mental health of an individual, the provision of healthcare to the individual, and the payment for the healthcare of that individual. More specifically, PHI refers to individually identifiable health information that can be used to reasonably identify an individual. In the United States, HIPAA specifies 18 such identifiers, including name, birth date, telephone number, e-mail address, Social Security number and medical record number.

Note 2
 Security Breaches Announced in April 2008

- A New York Presbyterian Hospital employee was charged with selling patient information as a participant in a wide-ranging identity theft ring. The employee, a patient admissions representative, used his user login to improperly access the personal health information of nearly 50,000 patients. He began to access the files and sell the information in early 2006.

- Health insurer WellPoint confirmed that the Social Security numbers, pharmacy and prescription records, and other personal health information for approximately 130,000 of its customers were left unsecured on the public Internet.

- The University of Miami announced that a case of six computer backup tapes containing the personal health information of some 2.1 million patients was stolen from a vehicle on 17 March. The data included information on hospital patients dating back to 1 January 1999.
REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509