Using Enterprise Governance, Risk, And Compliance (EGRC) Tools For Improved Management Of Security And Privacy

June 23, 2015
What is eGRC?

- A management system for compliance requirements, policies, risk assessment, and remediation tracking, spanning across multiple domains.
Benefits to GRC

- Management via the traditional spreadsheet method does not scale well with a large decentralized environment, such as a multi-hospital enterprise.

- Benefits to GRC
  - Manage and centralize risk across the enterprise
  - Enable collaboration across different enterprise groups
  - Streamline business processes and workflows
  - Generate risk metrics and risk profiles for further insight
  - Ensure data integrity through access control
NYP’s GRC Story

NewYork-Presbyterian Hospital’s information security department acquired the RSAM GRC platform in 2010.

It sits on a server, unused, for all the same reasons other GRC projects never get off the ground.

An effort is currently underway to establish the consensus necessary for a true GRC program to be established, linking to existing organizational audit, finance, and compliance activities.

In other words, this won’t be another IT project . . . .
The Incident Response Problem

“Companies that select individual solutions for each regulatory challenge they face will spend 10 times more on IT portion of compliance projects than companies that take on a proactive and more integrated approach.”

—Gartner
The Incident Response Problem
The Incident Response Problem

<table>
<thead>
<tr>
<th>#</th>
<th>Security classification*</th>
<th>Incident category</th>
<th>Incident severity</th>
<th>Incident start details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Classification</td>
<td>Impact</td>
<td>Cause</td>
</tr>
<tr>
<td>5</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>6</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>7</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>8</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>9</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>10</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>11</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>12</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>13</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>14</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>15</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>16</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>17</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>18</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>19</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>20</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>21</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>22</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>23</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>24</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>25</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
<tr>
<td>26</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
<td>Choose</td>
</tr>
</tbody>
</table>
Steps in the Wrong Direction

In 2009 Partners HealthCare acquired RSA’s Archer Incident Response module.

- Professional services were not included;
- The project manager was responsible for the daily support of security infrastructure and responding to helpdesk tickets;
- The project did not report into the Partners Chief Information Security Officer; and
- No one outside of IT was aware of the project.
Putting on the Brakes

In summer 2010 the Partners Chief Information Security Officer made a decision was made to stop the deployment of Archer’s Incident Response module.

• Only a single workflow related to lost or stolen laptops had been implemented at that time.

• Business and technical ownership remained unclear.

• Initial discussions about implementing an GRC platform the “right way” began in fall 2010.
Deloitte Security Review

In 2012 Partners HealthCare engaged Deloitte & Touche LLP to evaluate the organization's information security and privacy program.

Deloitte’s recommendations included:

- The acquisition of a GRC platform to holistically manage compliance activity; and
- The establishment of a GRC Steering Committee to guide the project over multiple years; and

Deloitte’s review facilitated the establishment of the “enterprise mindset” necessary for the Partners GRC project to takeoff.
GRC Acquisition

Partners Healthcare began evaluating GRC vendors in 2013.

- A cross-organizational stakeholder group was established, representing compliance, IT, information security and privacy, finance, and clinical and research leaders.

- This process was critical – buy-in for the GRC program needed to exist amongst a diverse group of stakeholders, not just management.

- The RSA Archer platform was acquired in December 2013.
## Partners’ GRC Implementation Project

<table>
<thead>
<tr>
<th>GRC Applications</th>
<th>Key Focuses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enterprise Management</strong></td>
<td>• Import Partners enterprise data such as applications, servers, site locations, which are foundational for all other solutions.</td>
</tr>
<tr>
<td><strong>Risk Management</strong></td>
<td>• Implement risk management process to evaluate, communicate, and manage enterprise risks and associating findings.</td>
</tr>
<tr>
<td><strong>Policy Management</strong></td>
<td>• Implement enterprise solution to publish, approve, and manage policies. Migrate PHS &amp; PCC existing polices to GRC.</td>
</tr>
<tr>
<td><strong>Business Continuity Management</strong></td>
<td>• Implement process to create, access, and manage Disaster Recovery Plans. Replace the LDRPS system.</td>
</tr>
</tbody>
</table>
How did we get here?

• Project originally conceived in summer 2012
  – New CISO needed an IT security governance tool.
  – Due to the impending retirement of Lotus Notes, Compliance and clinical leaders were looking for a new home for over 6,000 policies stored in 50+ separate Notes databases.
  – No organization-wide governance for policies. Each entity created and managed their own, all in different ways with different formats.
  – There was an expressed desire to consolidate all policies into a single database, and to establish an organization-wide governance process for policies.
What we did...

• Issued an RFP during fall 2013
  – Initial focus was on a policy management tool, but broadened the scope to look at GRC products in order to meet a broader set of needs

• In the summer of 2013, purchased RSA Archer eGRC
  – Other finalist was a system that only did policy management – this was the preferred solution for some clinical leaders

• Implementation began in winter 2013/2014, with an initial focus on Policy Management due to the upcoming Lotus Notes retirement
  – Needed to migrate over 4,000 policies before July 2014
Duke Medicine's RSA Archer eGRC Evolution

- Enterprise
- Policy Management
- Vendor Management
- Risk Management
- FISMA (future)
- Business Continuity (future)

Focus for Today's Discussion
Vendor Management Goals

- Centralize Vendor Data
  - General vendor information
  - Contracts
  - Addendums
  - Business Associates Agreements

- Manage Vendor Contacts/Relationships

- Assess Vendor Risk

- Retire/replace current Vendor Management tools:
  - Legacy system
  - Spreadsheets
  - SharePoint
Vendor Design Considerations

• Contract Access
  – Governance concerns
  – Confidentiality/Non-Disclosure Agreement

• Assessments
  – Application/Service
  – Financial
  – Vendor

• Accommodate alias (also known as) and other vendor relationships to track mergers and name changes

• When to start tracking/managing a vendor?
  – Pre-purchase
  – Contract signed
Risk Management Goals

• Provide an integrated tool to assess, categorize, and quantify risks related to the security of system applications, facilities, devices, information assets and business units.

• Assign data classifications, risk categories, threats, business processes.

• Ensure that risk assessments are designed and conducted.
Duke Medicine Demo
Enterprise Management

• Business Hierarchy
  – Company
  – Division/Entity
  – Department

• IT Infrastructure
  – Applications
  – Devices

• Business Infrastructure
  – Processes
  – Business Impact Analysis
Duke Medicine Demo
Risk Assessments and Findings

• Questionnaires
  – Service Transition Readiness Assessment (STRA)
  – Critical Controls
  – PCI
  – Common Controls

• Exception Requests
  – Document risk acceptance

• Remediation Plans
  – Document risk remediation
QUESTIONS?