Využití GRC řešení pro řízení rizik

Ivan Svoboda
RSA, The Security Division of EMC
Agenda

- Defining GRC
- The Language of GRC
- GRC Processes
- Importance and Benefits of GRC Platform
- Risk Management
- Integrated GRC approach
- Success Examples: GRC ROI, Case studies
- The GRC Technologies by Analysts
- Q&A
Defining GRC

Governance: The culture, objectives, processes, policies, and laws by which companies are directed and managed.

Compliance: The act of adhering to, and demonstrating adherence to, external laws and regulations as well as corporate policies and procedures.

Risk: The likelihood and impact of something happening that will have an effect on achieving objectives.

Heat maps
Control
- Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature

Risk
- Combination of the likelihood of an event and its impact; Risk is inherent and residual

Incident
- Unwanted events that could compromise business operations

Threat
- Potential cause of an unwanted incident

Asset
- Anything that has value to the organization
The Language of GRC (cont.)

<table>
<thead>
<tr>
<th>Control</th>
<th>IT</th>
<th>Finance</th>
<th>Operations</th>
<th>Legal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>strong passwords</td>
<td>segregation of duties</td>
<td>product testing</td>
<td>trademark</td>
</tr>
<tr>
<td>Risk</td>
<td>unauthorized access</td>
<td>fraud</td>
<td>unsatisfied customers</td>
<td>brand dilution</td>
</tr>
<tr>
<td>Incident</td>
<td>data breach</td>
<td>missing money from cash drawer</td>
<td>high error rate</td>
<td>infringement</td>
</tr>
<tr>
<td>Threat</td>
<td>hacking</td>
<td>theft</td>
<td>ineffective tests</td>
<td>competitive</td>
</tr>
<tr>
<td>Asset</td>
<td>information</td>
<td>cash</td>
<td>quality</td>
<td>brand</td>
</tr>
</tbody>
</table>
What’s the big deal?

Here’s why GRC is an imperative in today’s business world:

- Demands on corporate governance
- Multi-faceted risk environment
- Growing regulatory requirements
- Disappearing boundaries in the extended enterprise
- Corporate social responsibility
Governance processes include:

- Identify leadership and organizational structure
- Formulate company objectives
- Create policies
- Identify controls
- Training and awareness
- Manage exceptions
Compliance Processes

- Compliance processes include:
  - Document control procedures and test plans
  - Identify business processes and assets
  - Perform continuous control monitoring
  - Perform routine assessments/testing
  - Identify and manage exceptions
  - Provide reporting to management
Risk Processes

Risk processes include:

- Identify threats to company objectives
  - Financial
  - Regulatory
  - Business
  - Reputational
  - Strategic
  - Security
- Evaluating the likelihood and impact of risks
- Determine the inherent risk
- Designing mitigating controls
- Prioritize risk reduction measures
- Monitoring residual risk
„Neumím si představit žádný problém, který by mohl tuto loď zastavit, žádnou katastrofu, která by se nám mohla přihodit. Moderní lodě již přeconaly všechna rizika.“

Captain E.J. Smith, Commander of Titanic
Známé poslední hlášky

Digitální fotoaparáty nemají budoucnost

President Kodaku

Čára není zeď ...

Neznámý

Vždyť jsme tady předloni měli audit ...

Proč by nám někdo kradl naše data ? ...

Jarda by to přece neudělal ...

Jé hele užovka ...

My přeci máme firewall (VPN, SSL, ...) ...

V pohodě hoši, tohle je nulák ...

Brzdy jsou hotový. Jedu to vyzkoušet!

Pusť mě k tomu, já tomu rozumím...
Why GRC Platform?

The Complex & Incomplete Picture

- Data Inconsistency
- Data Duplication
- Data Fragmentation
- Information Silos
- Lack of Security
- Lack of Communication
- Difficult to Correlate
- Missing Data
Je to bezpečné? (Je to v souladu?)

Ředitel

Security Officer (CISO)

IT Manager, Vývojář, Admin

Jak velké je riziko?
Nezavřou mne?
Projdeme auditem?

Jaká je konfigurace?
Jaké jsou hrozby a zranitelnosti?

Co je vlastně potřeba?
Co je důležitější?
Je to bezpečné? (Je to v souladu?)

• Jaká je naše bezpečnostní politika?
• Jaká rizika jsou pro nás přijatelná?
• Jakou hodnotu mají naše data, aplikace, procesy, …?
• Jaké hrozby jsou u nás reálné?
• Jak má být systém správně nakonfigurován?
• Jaká je důležitost incidentů, výjimek, …?
Integrated Risk and Compliance

**Identify Risks:**
- Risk analytics
- Loss events
- Whistle blower reports
- eDiscovery
- Configuration scan results
- Security event logs
- Sensitive data discovery
- Document and records retention data
- Threat intelligence
- Vulnerability scan results

**Prioritize Risks:**
- Business impact
- Business hierarchy
- Responsibilities and leadership
- Products and services
- Business processes
- Technology and information assets
- Facilities
- Employee, partner and vendor contacts

Risks ??
Compliance ??
Traditional approach

- Assets
- Threats
- Impacts
- Likelihood
- Vulnerabilities
- Inherent risks
- Owners
- Risk mitigation
- Residual risks

<table>
<thead>
<tr>
<th>Asset</th>
<th>Threat</th>
<th>Impact</th>
<th>Likelihood</th>
<th>Vulnerability</th>
<th>Inherent risk</th>
<th>Owner</th>
<th>Risk mitigation</th>
<th>Residual risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB-1</td>
<td>xxx</td>
<td>zzz</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
</tr>
<tr>
<td>DB-2</td>
<td>xxx</td>
<td>zzz</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
</tr>
<tr>
<td>CRM</td>
<td>xxx</td>
<td>zzz</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
</tr>
<tr>
<td>ERP</td>
<td>xxx</td>
<td>zzz</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
</tr>
<tr>
<td>Router</td>
<td>xxx</td>
<td>zzz</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
</tr>
<tr>
<td>FW</td>
<td>xxx</td>
<td>zzz</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
</tr>
<tr>
<td>XY</td>
<td>xxx</td>
<td>zzz</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
</tr>
<tr>
<td>XY</td>
<td>xxx</td>
<td>zzz</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
<td>YYY</td>
</tr>
</tbody>
</table>
Traditional approach (2)

- Assets
- Threats
- Impacts
- Likelihood
- Vulnerabilities
- Inherent risks
- Owners
- Risk mitigation
- Residual risks

System-1: ERP

Different requirements:
- ISO 27k
- PCI
- Basel
- xxx

System-2: CRM

Changes:
- Owners
- Threats
- Mitigation
- Vulnerabilities
- Systems

System-3

Workflow:
- Approvals
- Exceptions, ...

History tracking

Adding context:
- Business Process, ...

SECURITY 2012
What are the top two barriers to achieving your organization’s GRC-related goals?

1. Lack of resources - 52%
2. Lack of cooperation and collaboration - 44%
3. Complexity of existing technologies - 31%
4. Lack of clear leadership - 20%
5. Organizational change - 19%
6. Inability to set priorities - 19%
7. Lack of C-level support - 15%
8. Difficulty in hiring skilled personnel - 11%
9. Inability to get started (inertia) - 4%
10. Inadequacy of existing technologies - 3%
11. Complexity of the program - 3%
12. Lack of organizational maturity - 2%

“Siloes are the enemy of eGRC programs.”
- Dr. Ponemon
Solving Risk Management Challenges

GRC Platform Risk Management:
Centralized, automated and proactive approach to risk assessment, management and reporting
GRC Platform: Approach to Risk Management

- Identify and Monitor Risks
- Capture Qualitative, Quantitative and Trending Metrics
- Perform Targeted Risk Assessments to Determine Inherent Risk
- Manage Findings through Remediation or Exceptions
- Auto-Calculate Residual Risk
- Report on the Organization’s Risk Profile
- Identify and Monitor Risks
Why GRC Platform Risk Management

**Standardized approach** with flexibility to adapt to your methodologies through point-and-click configuration.

**Ability to tie risks to mitigating controls**, corporate objectives, supporting metrics, etc.

**Central platform** to transform isolated, manual processes into an **integrated, automated** risk management program.
Integrated GRC Approach

- Policy Management
- Risk Management
- Compliance Management
- Incident Management
- BCP Management
- Threat Management
Integrated GRC Approach
Managing Encryption Keys

Key owners may not print out private keys and should:

- Ensure private keys are classified as Restricted and treated accordingly.
- Private keys should be transmitted through different channels to ensure proper separation from the information which is used to generate the encryption keys.

Control Procedures

Windows Vista: Implementation Procedure

1. Open Group Policy Editor focused on the appropriate object.
2. Navigate to the following subtree and its subnodes: Computer Configuration\Administrative Templates\Windows Component\BitLocker Drive Encryption
4. Click OK to confirm changes.
5. Close the group policy editor.

PCI DSS v1.2.0: Protect Stored Data Protection and Encryption Keys

07.0 Communication Management
07.1 Encryption
07.1.03 Key Management

Key owners may not print out private keys and should ensure private keys are classified as Restricted and treated accordingly. Private keys should be transmitted through different channels to ensure proper separation from the information which is used to generate the encryption keys.
Jaké jsou požadavky?
(ISO, COBIT, ITIL, CSA, PCI, SOX, Basel, ...)

Jak to máme udělat?
(MS Windows XY, CheckPoint, Oracle, SAP, Wmware, AIX, Cisco, ...)

Jaká je realita?
Enabling the Cycle of Risk and Compliance

- Document Your Control Framework and Identify Risks
- Prioritize Deficiencies and Risks
- Remediate Findings and Manage Exceptions
- Consolidate and Visualize Compliance Efforts
- Manage
- Prioritize
- Identify
- Report
Integrated Approach for Enabling GRC
“Where before we managed work in two or three places, with GRC Platform you have one place to manage all of your work. People are completing assessments and mitigating risks, not focusing on administrative tasks.”
Example: SIEM + GRC in CIRC

**SIEM (RSA enVision)**
- IPS
- AV
- EP
- DLP
- FW
- AD
- WLAN
- URL

**Event Aggregation**

**GRC**
- HR
- Legal
- Eng.
- Business Reporting
- Incidents
- Threats
- GRC
- CIRT
- SOC
- GIS

**Data Enhancement**
- Identity
- Division
- Geo Info
- Data
- Location
- Department
- Regulation
- Asset Value
Example: DLP Risk Remediation

Day 1
30K files discovered by RSA DLP

Day 10
RRM sends initial questionnaire to data owners

Day 40
90% of files remediated
Repeatable and continuously monitored
Analyst work space and executive metrics in RRM.

“The new process was more than 4 times faster and much less disruptive to business.”
- EMC CIRC
In Action: GRC in CIRC

Business Context  Process Automation  Visibility  Integrated Approach
## GRC ROI Realized

<table>
<thead>
<tr>
<th>Realized Value</th>
<th>Organization</th>
<th>Proof Point</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process Efficiency</strong></td>
<td>Fortune 100 Pharmaceutical Company</td>
<td>$1.5 million annual savings due to reduced effort for Info Sec officers; $250,000 annual savings due to reuse of assessment questionnaires; reduction in time to complete assessment process from 2 months to 1 day</td>
</tr>
<tr>
<td><strong>Collaboration</strong></td>
<td>Fortune 100 Insurance Company</td>
<td>97% cost savings in IT-GRC due to collaboration and consolidation of assessment processes with several risk functions in the organization.</td>
</tr>
<tr>
<td><strong>Speed and Agility</strong></td>
<td>Fortune 100 Retailer</td>
<td>Initial store assessment implementation in February 2008; 1,000 assessments completed by March 2008 and over 3,500 by September 2008</td>
</tr>
<tr>
<td><strong>Visibility</strong></td>
<td>Fortune 1000 Bank Holding Company</td>
<td>Marshall Toburen, VP and operations risk manager: “Before we implemented our ERM system, silos of data were not used effectively. Now data may go into the system for one issue, but it can be cross-applied to all aspects of the business and aggregated for an overall view of risk rather than a variety of broken views.”</td>
</tr>
</tbody>
</table>
Business Outcomes

Business Impacts

- Compliance initiatives are tackled as individual projects
- Compliance reporting is stored in spreadsheets and represent one point-in-time
- Policy exceptions go untracked and pose risk to the business
- Compliance data scattered across multiple silos
- Managers struggle to prioritize threats by their potential impact to the business.

Solution Outcomes

- Efficiency: Ask once, Answer Many: Reduction or elimination of redundant assessments
- Automation: Isolated data is transformed into sustainable processes
- Accountability: Transparency and accountability: Knowing the status or exceptions and unresolved issues
- Collaboration: Partnerships and consistency across business silos
- Visibility: Threats are identified and remediation actions are easily prioritized and tracked

SECURITY 2012
The 2011 Forrester Wave - GRC

Figure 2: Forrester Wave™: IT GRC Platforms, Q4 ‘11

Figure 2: Forrester Wave™: Enterprise GRC Platforms, Q4 ‘11

- Risky Bets
- Contenders
- Strong Performers
- Leaders

- Current offering
- Market presence
- Weak — Strategy — Strong

- MetricStream
- RSA Archer
- B Wise
- ARC Logics
- OpenPages
- SAP
- Thomson Reuters
- Compliance 360
- Methodware
- Protiviti
GRC – Risk Management Example
Děkujeme za pozornost.

Živé demo RSA Archer GRC:
- salónek
- Petr Nádeníček, AEC

Ivan Svoboda
RSA, The Security Division of EMC
ivan.svoboda@rsa.com
GRC Customer Success
An Illustrative Example

Policy Management

Author Policies

Leverage Control Standards

Track Exception Requests

Map Authoritative Sources

Inform Employees

Document Control Procedures

SECURITY 2012
Effectiveness of GRC Deployment

Policy Management

• Created a consistent, automated process for managing the lifecycle of their policies and controls.
• Reduced the time and effort required to create, update and communicate policies company-wide.
• Greater end-user visibility into corporate policies through an easy-to-use portal.
• Consolidate control requirements for compliance processes.

“Our organization has experienced significant cost reductions in managing the policy review process.”

Advisor - Information Security & IT Risk Strategy
An Illustrative Example

Risk Management
Effectiveness of GRC Deployment

Risk Management

• Reduced effort for information security officers, resulting in $1,500,000 annual savings

• Reused assessment questionnaires, resulting in $250,000 annual savings

• Reduced time to track assessment completion from 2 months to 1 day

  “We’ve seen a huge reduction in resourcing [for compliance]. What used to take literally up to two months...it’s been reduced down to a day or two at most.”

  Information Security Manager
An Illustrative Example

Business Continuity Management

- Perform Business Impact Analysis
- Document Business Continuity Plans
- Document Disaster Recovery Plans
- Automate Plan Maintenance
- Track Crisis Events
- Test Plans
Enable protection for 350 applications, 80 of which are deemed critical

Able to recover 50% of the systems within 36 hours or less

Cost of resources required to perform vendor assessments down 50%

Risk assessment efficiencies save $20,000 per year

“The best thing is that we now have quick visibility into the important details without having to dig deep into all the information. We can validate that our risk and business-continuity data are accurate and complete and we can use the dashboards to quickly understand our situation,” said the CISO.