SECURITY 2012

20. ročník konference o bezpečnosti v ICT

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.

The Language of GRC

- 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.)

	IT	Finance	Operations	Legal
Control	strong passwords	segregation of duties	product testing	trademark
Risk	unauthorized access	fraud	unsatisfied customers	brand dilution
Incident	data breach	missing money from cash drawer	high error rate	infringement
Threat	hacking	theft	ineffective tests	competitive
Asset	information	cash	quality	brand

eGRC Theme: Enterprise Risk

IT	Operations	Finance	Legal/Compliance
InfoSec		Fraud	
Data Center	Environmental	Market Risk	Liability
IT Security			
App Mgmt.			Litigation
	Health & Safety	Credit Risk	HR
	BCP		
SDLC		Liquidity Risk	Privacy
	DR		
Applications	Geo-Political	Financial Reporting	




eGRC Solutions

Security Management | **Business Continuity Management** | **Information Governance**

Trusted Cloud | **Enterprise Risk & Compliance**

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

- 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

Bez rizika nelze vyhrát …

„Neumím si představit žádný problém, který by mohl tuto loď zastavit, žádnou katastrofu, která by se nám mohla přihodit. Moderní lodě již překonaly všechna rizika.“

Captain E.J. Smith, Commander of Titanic

Známé poslední hlášky

Digitální fotoaparáty nemají budoucnost

Čára není zeď …

Neznámý

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

Vždyť jsme tady předloni měli audit …

Proč by nám někdo kradl naše data ? …

Jarda by to přece neudělal …

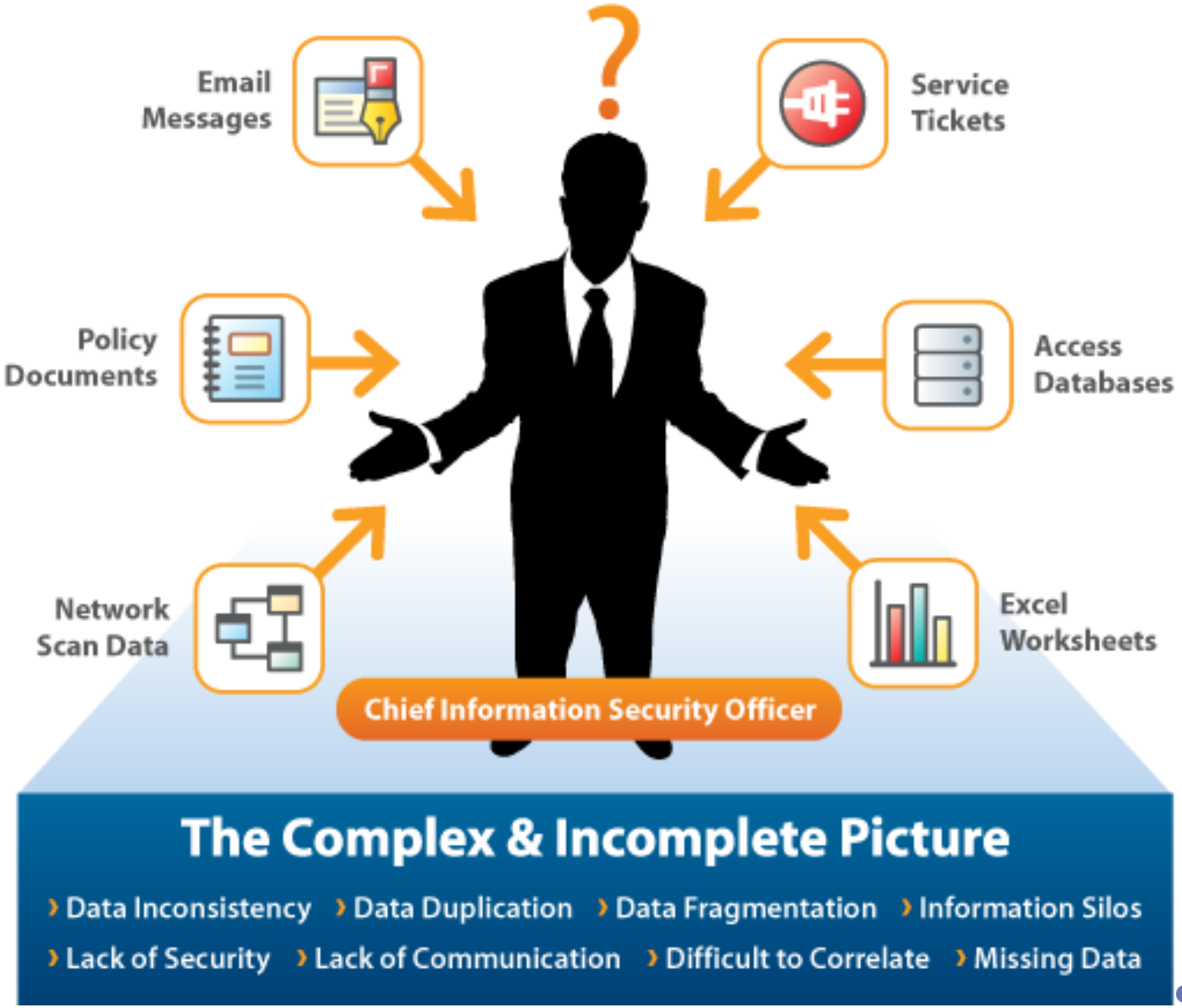
Jé hele užovka …

V pohodě hoši, tohle je nulák …

Brzdy jsou hotový. Jedu to vyzkoušet!

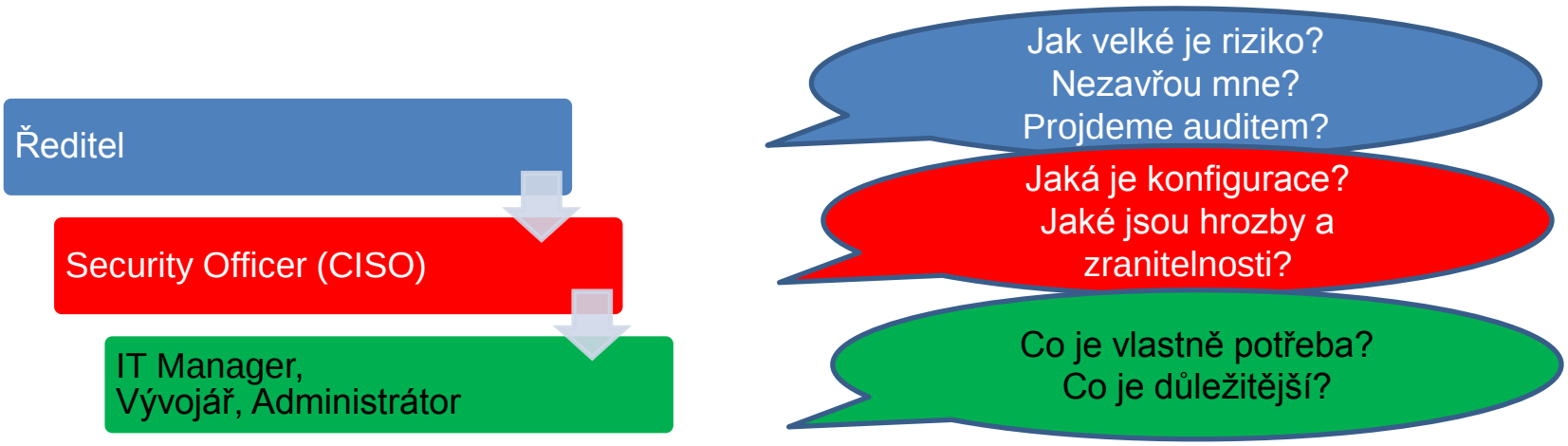
Pusť mě k tomu, já tomu rozumím…

Why GRC Platform ?



Je to bezpečné ? (Je to v souladu ?)

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, … ?

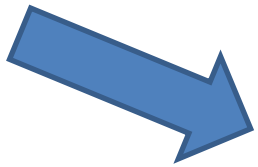
Integrated Risk and Compliance

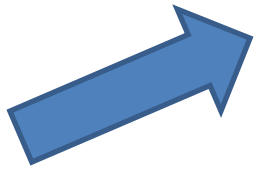
Identify Risks:

– 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





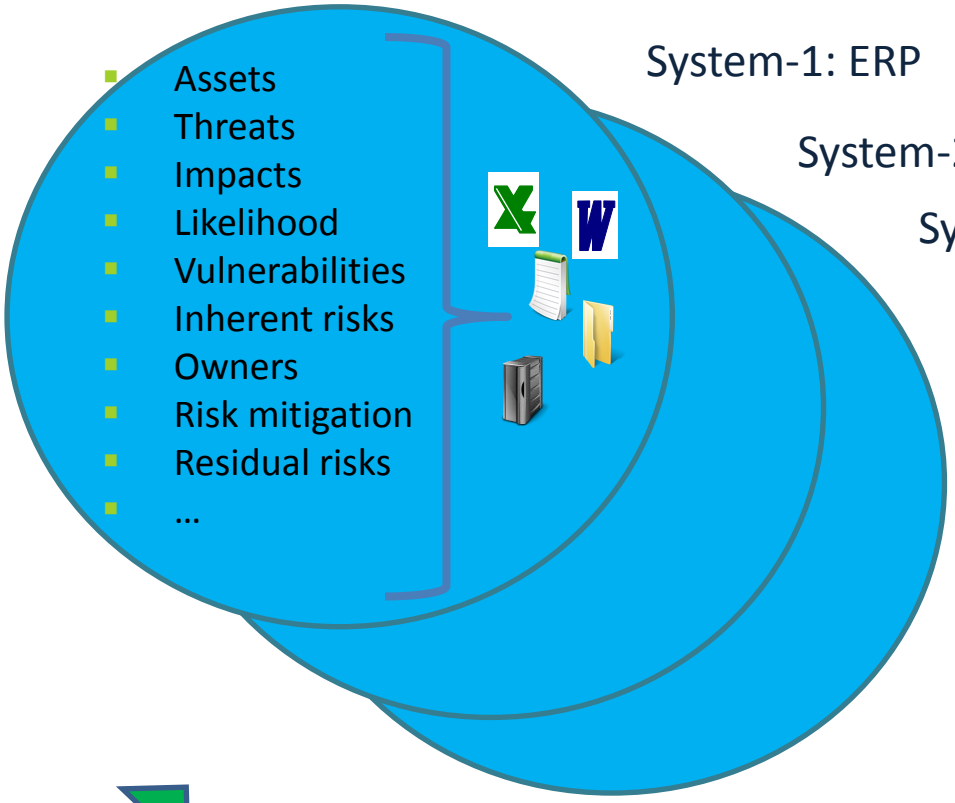
Risks ??
Compliance ??

Traditional approach

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

Asset	Threat	Impact	Likelihood	Vulnerability	Inherent risk	Owner	Risk mitigation	Residual risk
DB-1	xxx	zzz	yyy	yyy	yyy	yyy	yyy	yyy
DB-2	xxx	zzz	yyy	yyy	yyy	yyy	yyy	yyy
CRM	xxx	zzz	yyy	yyy	yyy	yyy	yyy	yyy
ERP	xxx	zzz	yyy	yyy	yyy	yyy	yyy	yyy
Router	xxx	zzz	yyy	yyy	yyy	yyy	yyy	yyy
FW	xxx	zzz	yyy	yyy	yyy	yyy	yyy	yyy
XY	xxx	zzz	yyy	yyy	yyy	yyy	yyy	yyy
XY	xxx	zzz	yyy	yyy	yyy	yyy	yyy	yyy

Traditional approach (2)



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

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

Workflow:
-Approvals
-Exceptions, …

History tracking

Adding context:
-Business Process, …

Customer Challenges

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

"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

SECURITY 2012

GRC Platform: Approach to Risk Management

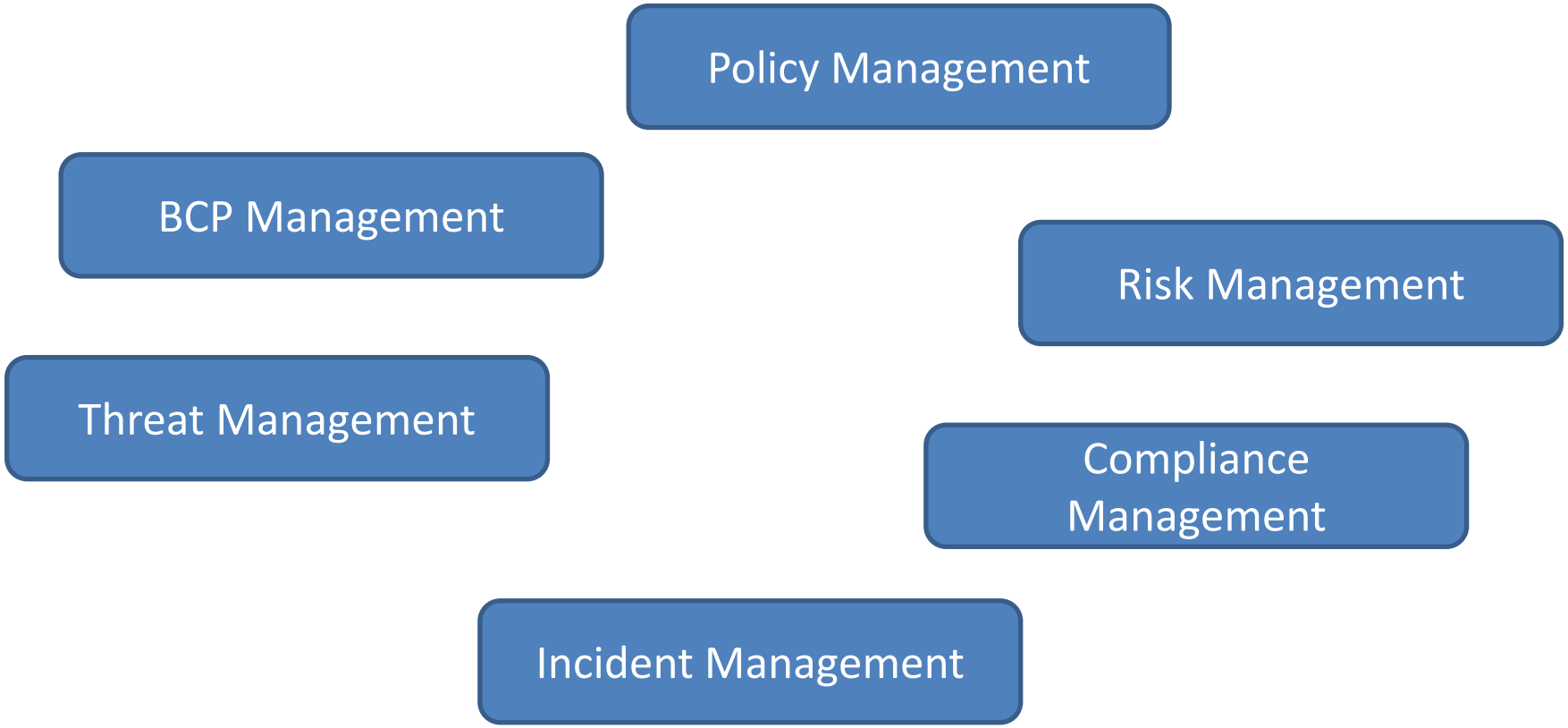
Why GRC Platform Risk Management

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.

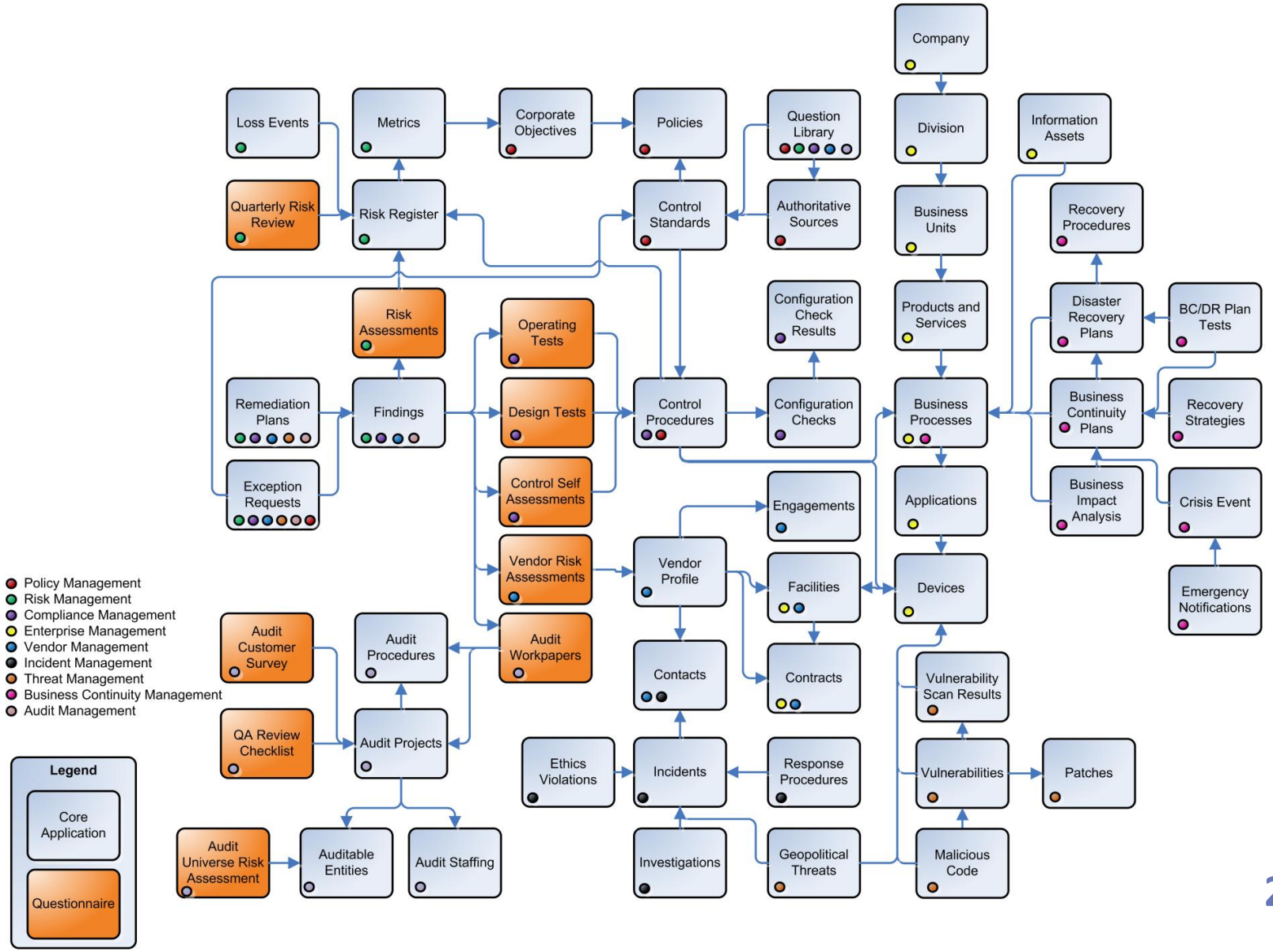
Central platform to transform isolated, manual processes into an **integrated, automated** risk management program

Integrated GRC Approach



Integrated GRC Approach

Integrated GRC Data Model



Policy Management Process

Control Procedures

Control Standards

Authoritative Sources

Polices

PCI DSS v1.2 - 9.2.5 Prevent Stored

Data Protection Encryption Keys

07.1.03 Key Management

Managing Encryption Keys

Windows Vista Managing Encryption Keys Procedure

- Key owners may not print out private keys and should password protect digital files containing private keys
- Private keys should be 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

Set the "Configure TPM platform validation profile" policy setting by performing the following steps:

1. Open Group Policy Editor focused on the appropriate object
2. Navigate to the following subtree location:
Computer Configuration\Administrative Templates\Windows Component\BitLocker Drive Encryption
3. Set "Control Panel Setup: Enable advanced startup options" to Disabled
4. Click OK to confirm changes; and5) Close the group policy editor

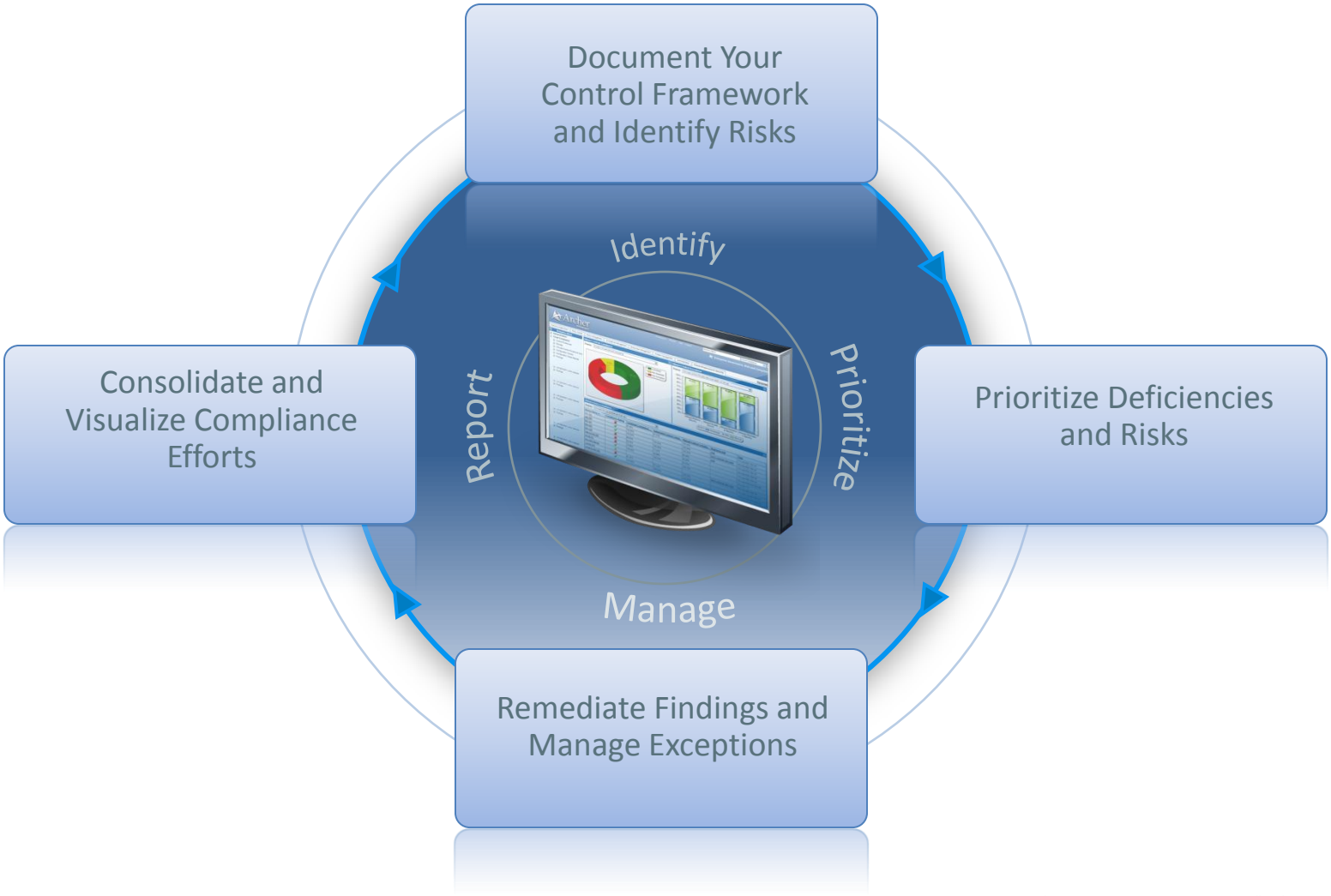
Policy Management Content

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



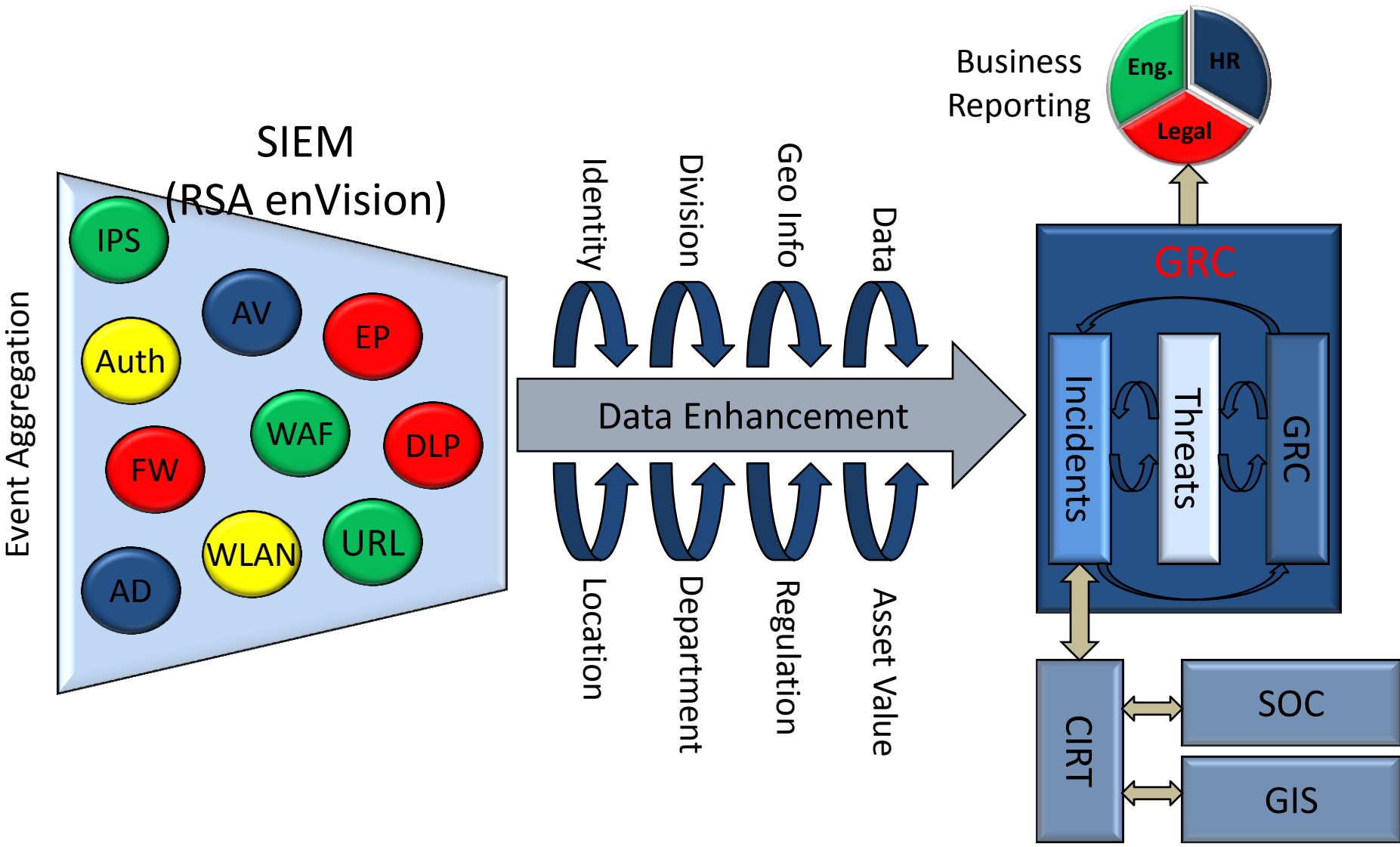
Integrated Approach for Enabling GRC

GRC Success Metrics

# regulatory requirements met	Time to demonstrate compliance with new regulations	# closed findings	Time to prepare monthly reporting	Cost of regulatory audit fines

"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



Example: DLP Risk Remediation

Day 3
1200 Owners
in 43 Countries
Identified

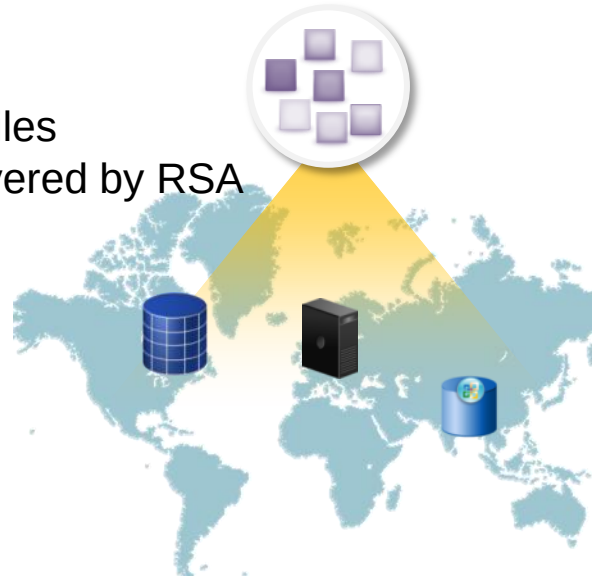
Day 40
90% of files remediated

Repeatable and
continuously monitored

Analyst work space and
executive metrics in
RRM.

Day 10
RRM sends initial
questionnaire to
data owners

Day 1
30K files
discovered by RSA
DLP



"The new process was more than 4 times faster and much less disruptive to business."

In Action: GRC in CIRC

EMC Critical Incident Response Center, Bedford, MA

Business Context

Process Automation

Visibility

Integrated Approach

GRC ROI Realized

Realized Value	Organization	Proof Point
Process Efficiency	Fortune 100 Pharmaceutical Company	$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
Collaboration	Fortune 100 Insurance Company	97% cost savings in IT-GRC due to collaboration and consolidation of assessment processes with several risk functions in the organization.
Speed and Agility	Fortune 100 Retailer	Initial store assessment implementation in February 2008; 1,000 assessments completed by March 2008 and over 3,500 by September 2008
Visibility	Fortune 1000 Bank Holding Company	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.”

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."

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"

Solution Outcomes

The 2011 Forrester Wave - GRC

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

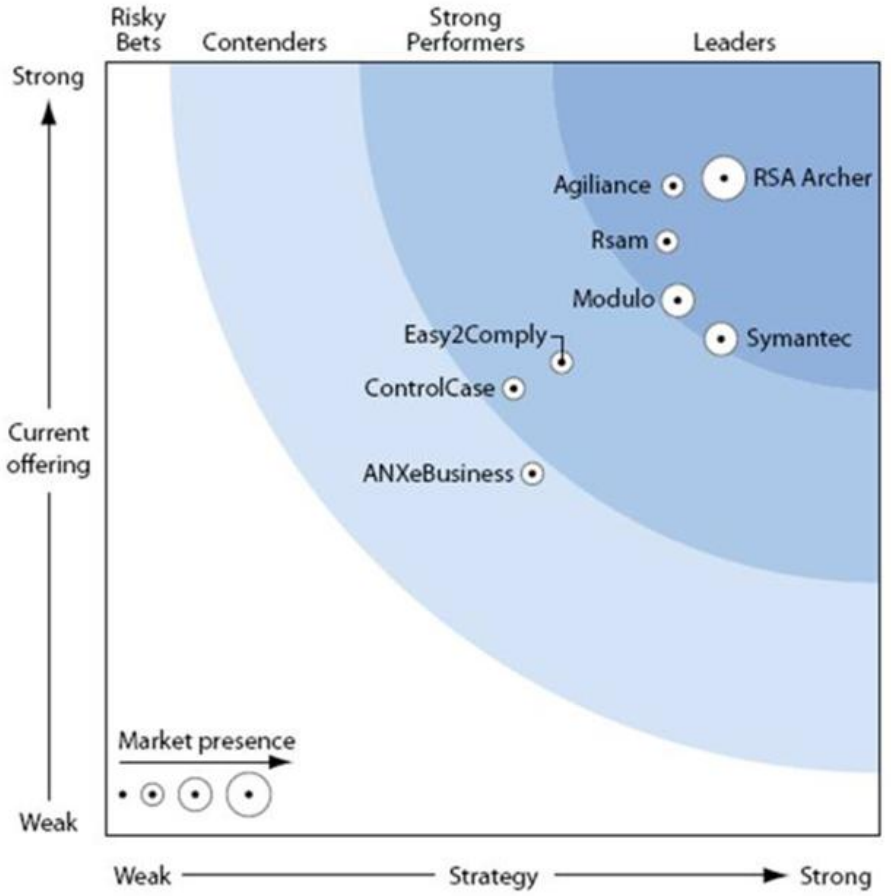
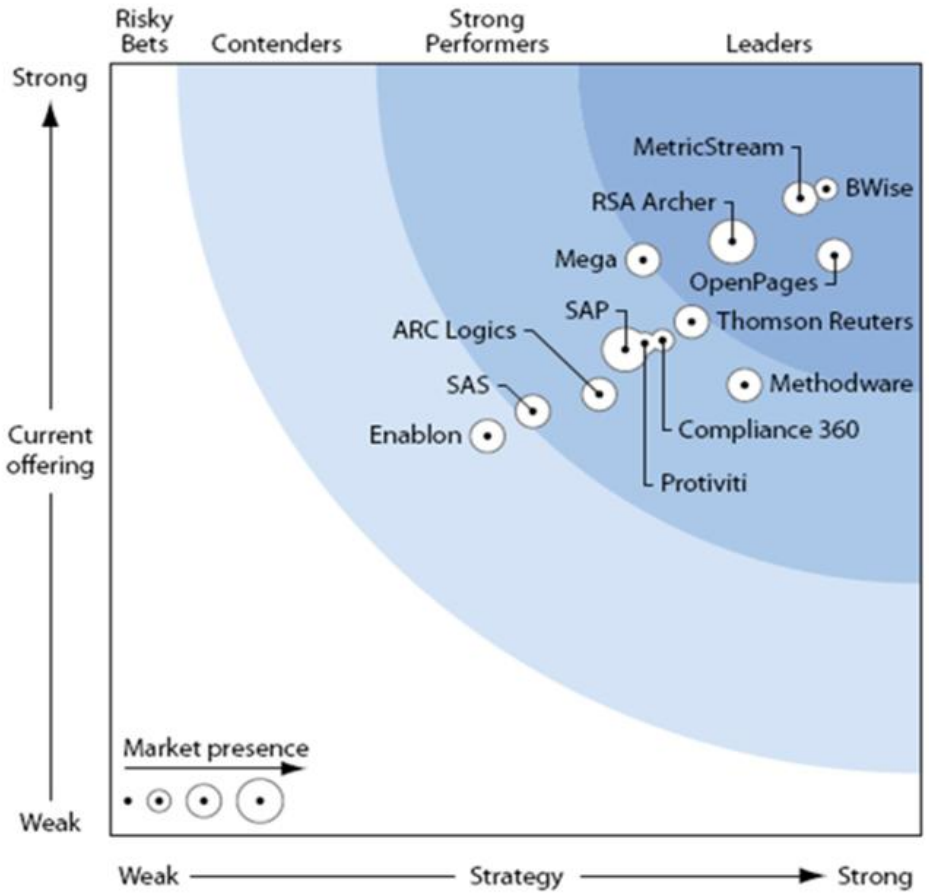
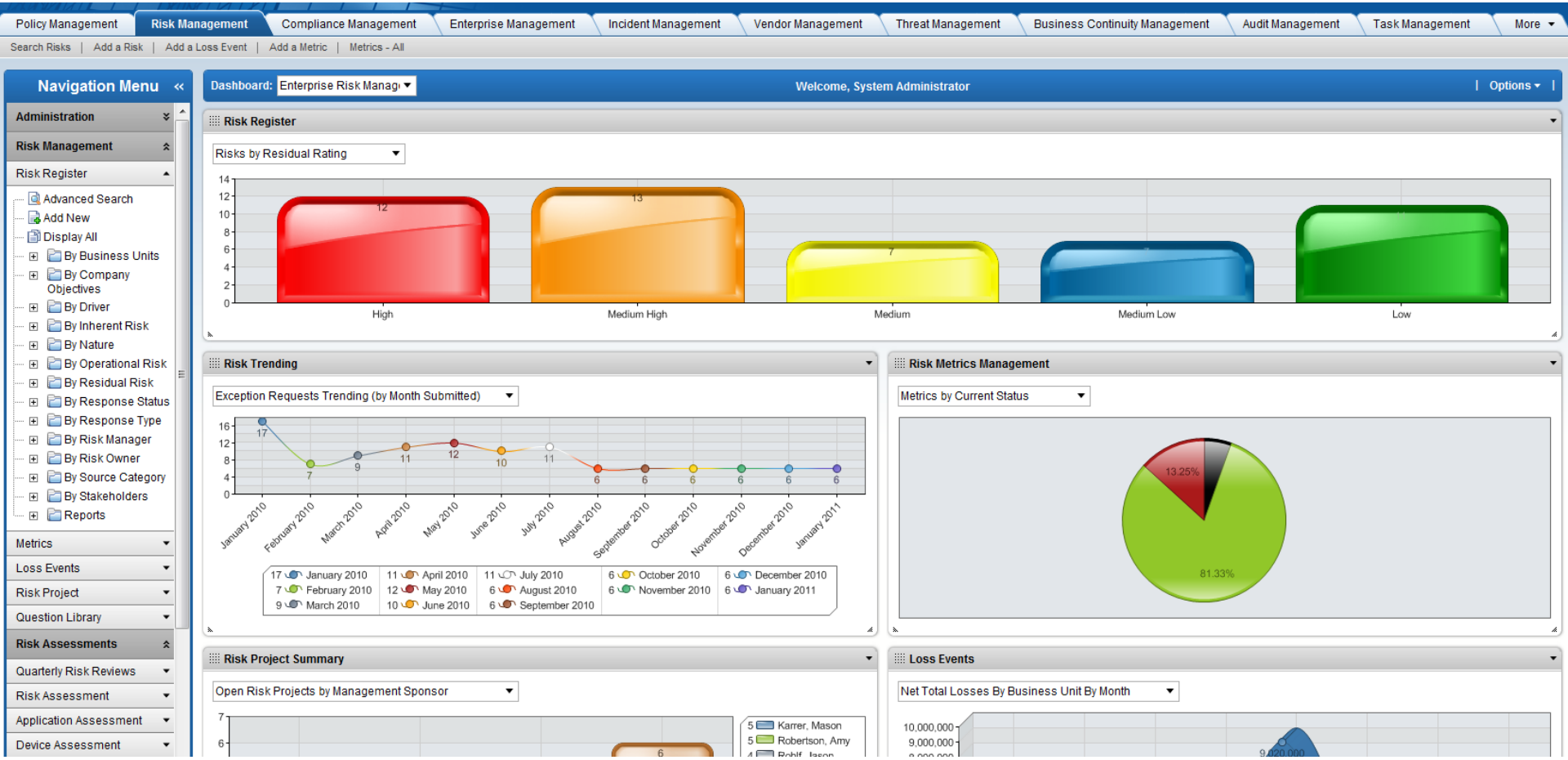


Figure 2 Forrester Wave™: Enterprise GRC Platforms, Q4 '11



GRC – Risk Management Example



SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Živé demo RSA Archer GRC:

- salónek
- Petr Nádeníček, AEC

Ivan Svoboda

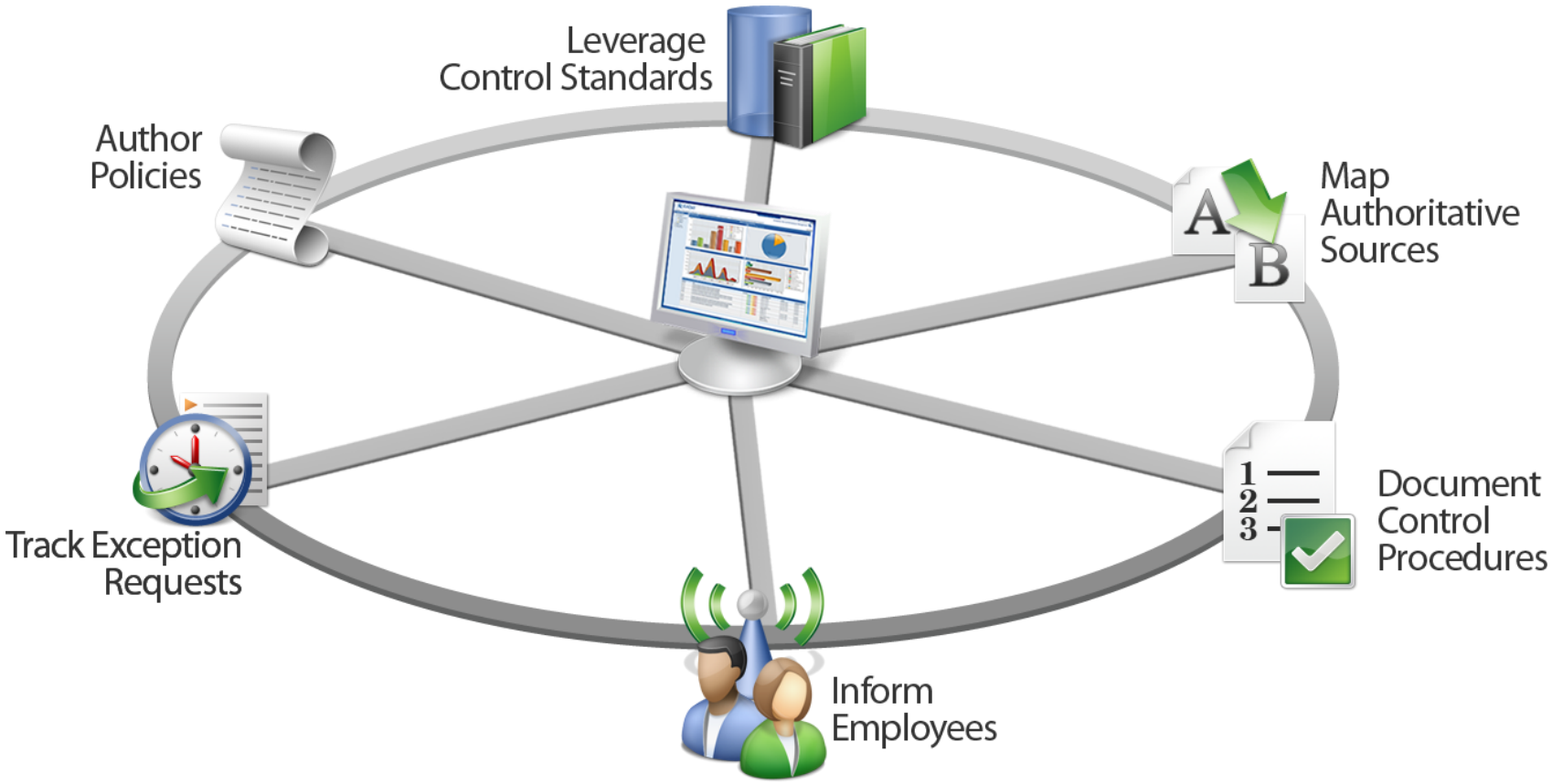
RSA, The Security Division of EMC

ivan.svoboda@rsa.com

GRC Customer Success

An Illustrative Example

Policy Management



Effectiveness of GRC Deployment

Policy Management

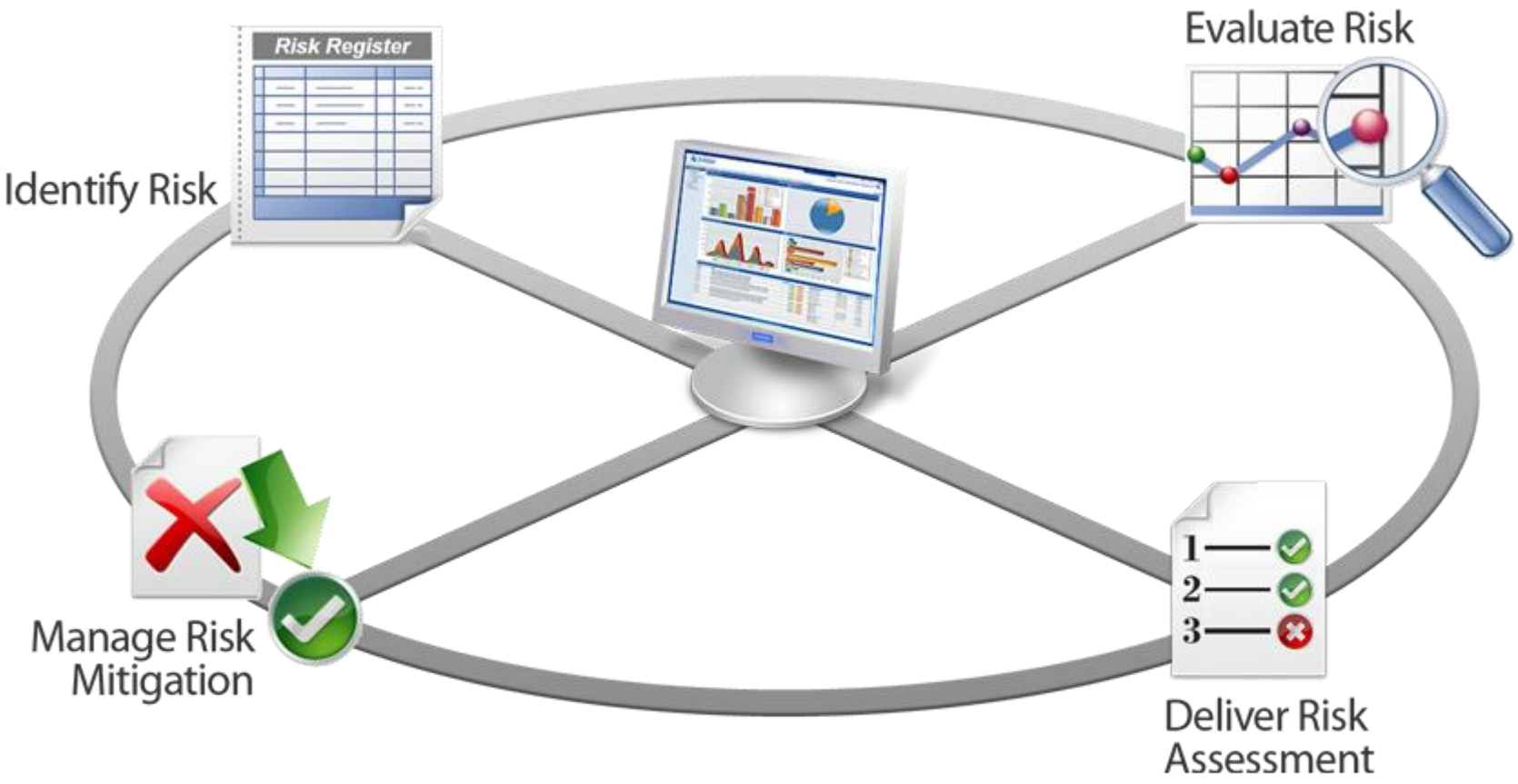
- Created a consistent, automated process for managing the lifecycle of their policies and controls.
- Reduced the time and effort required to create, update and communicate policies company-wide.
- Greater end-user visibility into corporate policies through an easy-to-use portal.
- Consolidate control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

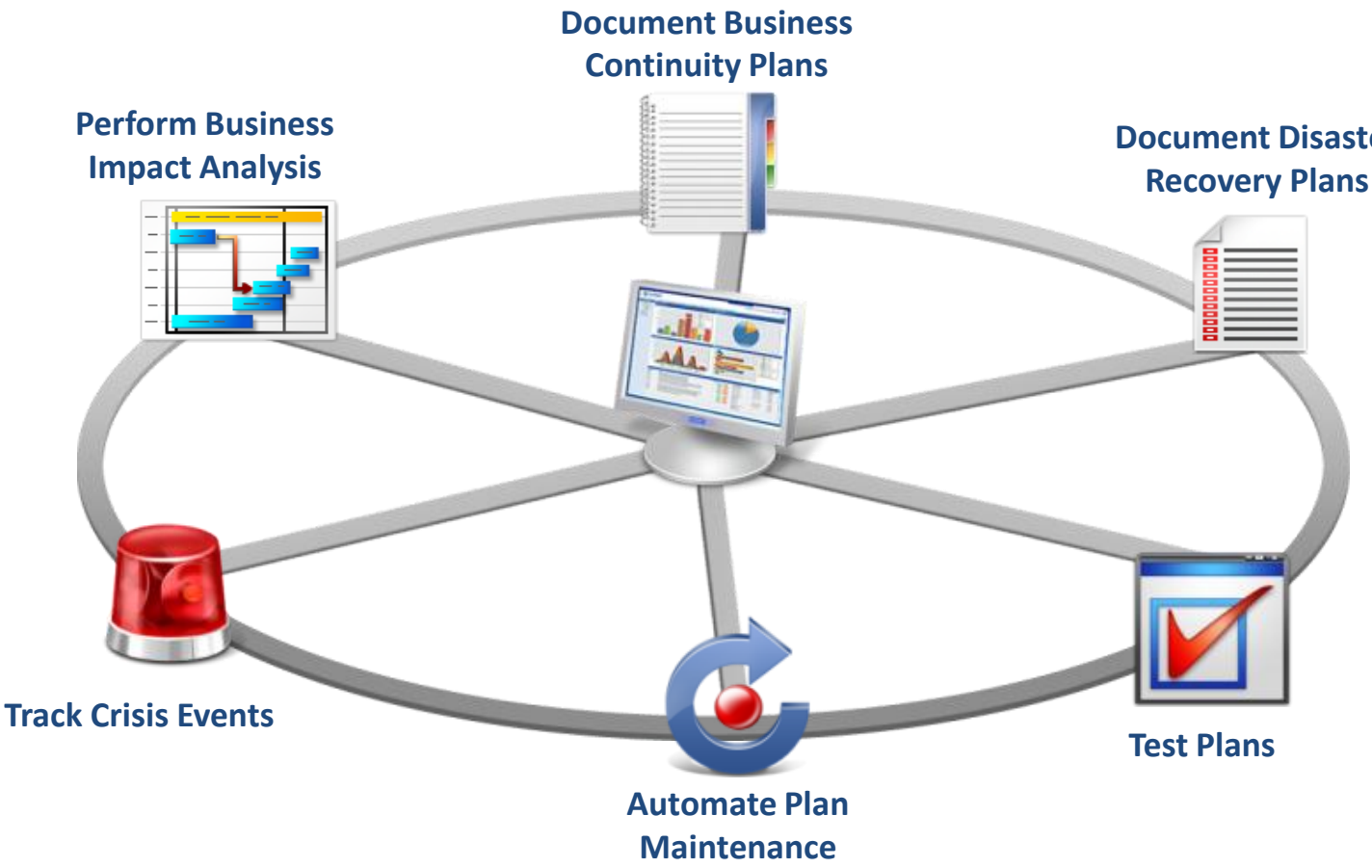
- Reduced effort for information security officers, resulting in **$1,500,000** annual savings
- Reused assessment questionnaires, resulting in **$250,000** annual savings
- Reduced time to track assessment completion from 2 months to **1 day**

"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



Effectiveness of GRC Deployment

- 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.

Compliance Management Process