ISACA®
Trust in, and value from, information systems
San Francisco Chapter

P12 – GRC: Ecosystem In The Cloud

Presented by:

Tony Buffomante & Dhawal Thakker

Agenda

- Understanding GRC
- Metamorphosis of GRC – Stage 1
- Metamorphosis of GRC – Stage 2
- Approach for implementing GRC
- Metamorphosis of GRC –Stage 3
- GRC – Ecosystem in the Cloud (Metamorphosis of GRC – Stage 4)
- GRC in Cloud – Pros & Cons
- Case Study
- SaaS offerings by GRC vendors
- Key Questions for SaaS provider

Understanding GRC

Governance, Risk & Compliance (GRC)

GRC typically encompasses activities such as corporate governance, enterprise risk management (ERM) and corporate compliance with applicable laws and regulations.

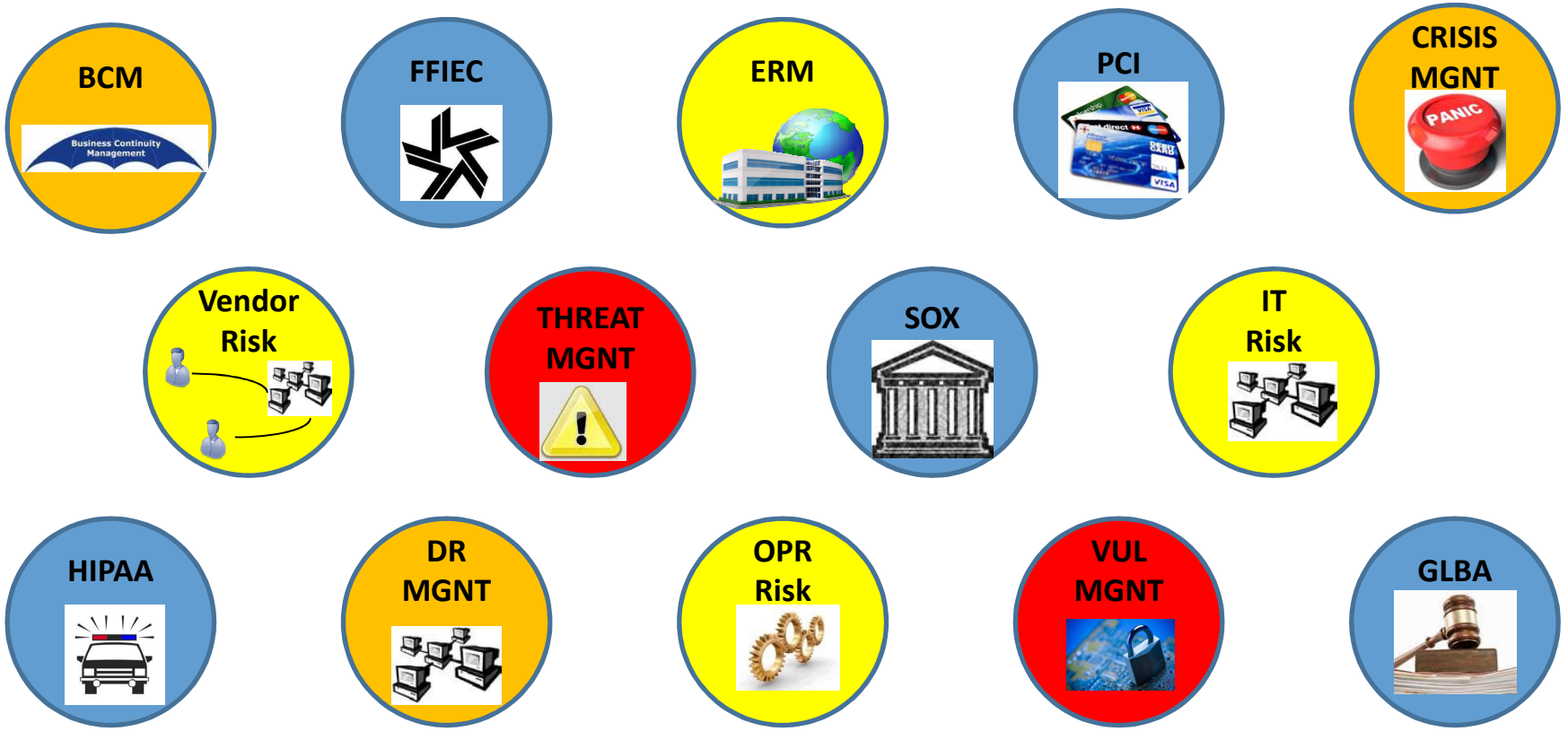
Governance describes the overall management approach through which senior executives direct and control the entire organization, using a combination of management information and hierarchical management control structures.

Risk Management is the set of processes to responds appropriately to risks that might adversely affect realization of the organization's business objectives.

Compliance Management means conforming with stated requirements (internal, industry, state, federal, clients etc)

Metamorphosis of GRC: Stage-1

- Initial years where each team operated within their own SILO / independent environment.



Metamorphosis of GRC: Stage-2

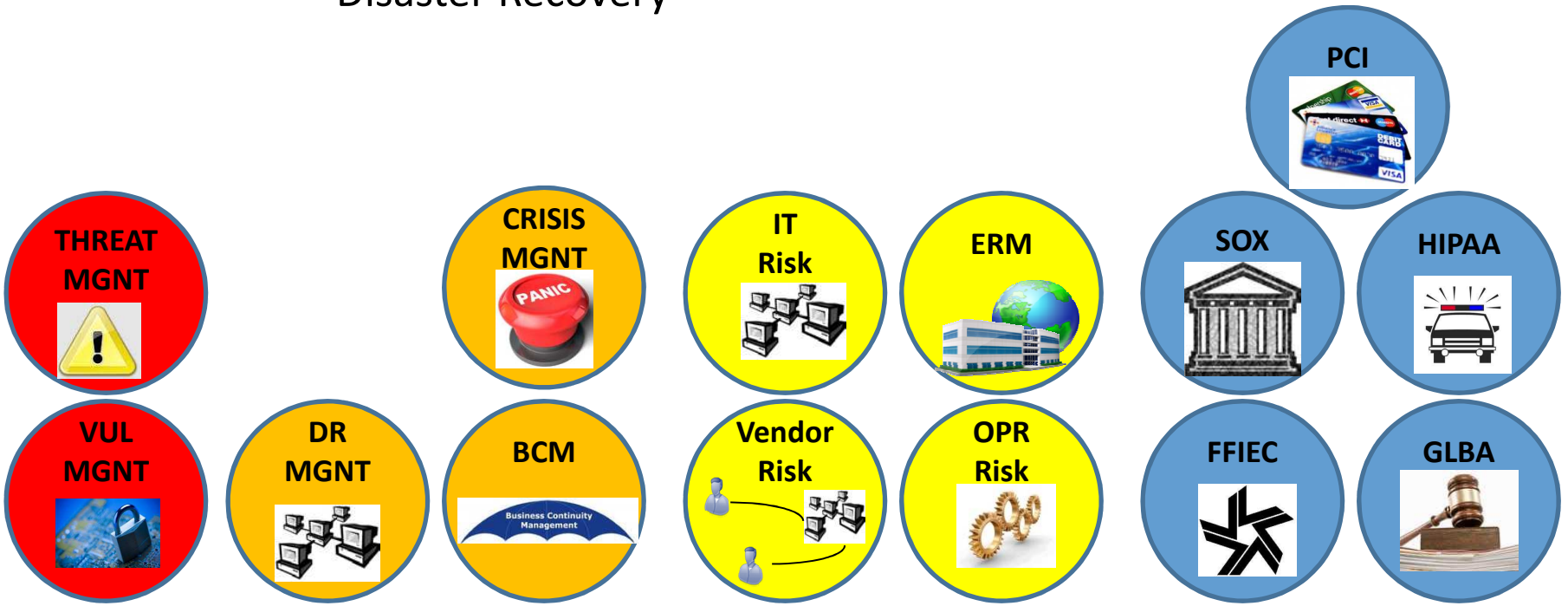
- Stage-2: Limited collaboration between similar teams

Threat & Vulnerability

Business Continuity & Disaster Recovery

Risk Management

Compliance Management



Why GRC – Key Drivers

Organizations, faced with increasing competitive challenges in the market place, are driven towards adopting technology to address their governance, risk and compliance needs.

Business Transformation

- Companies are constantly going though changes to their organizational hierarchy
  - Mergers and Acquisitions
  - Restructuring
  - Globalization

Cost Reduction

- Abundance of pervasive legacy systems
- Manually intensive business processes and control systems.

Compliance Management

- Increase regulatory compliance needs
- Pressure to reduce cost of compliance
- Reduced headcounts requires employees to focus on core business.

Increase Efficiency

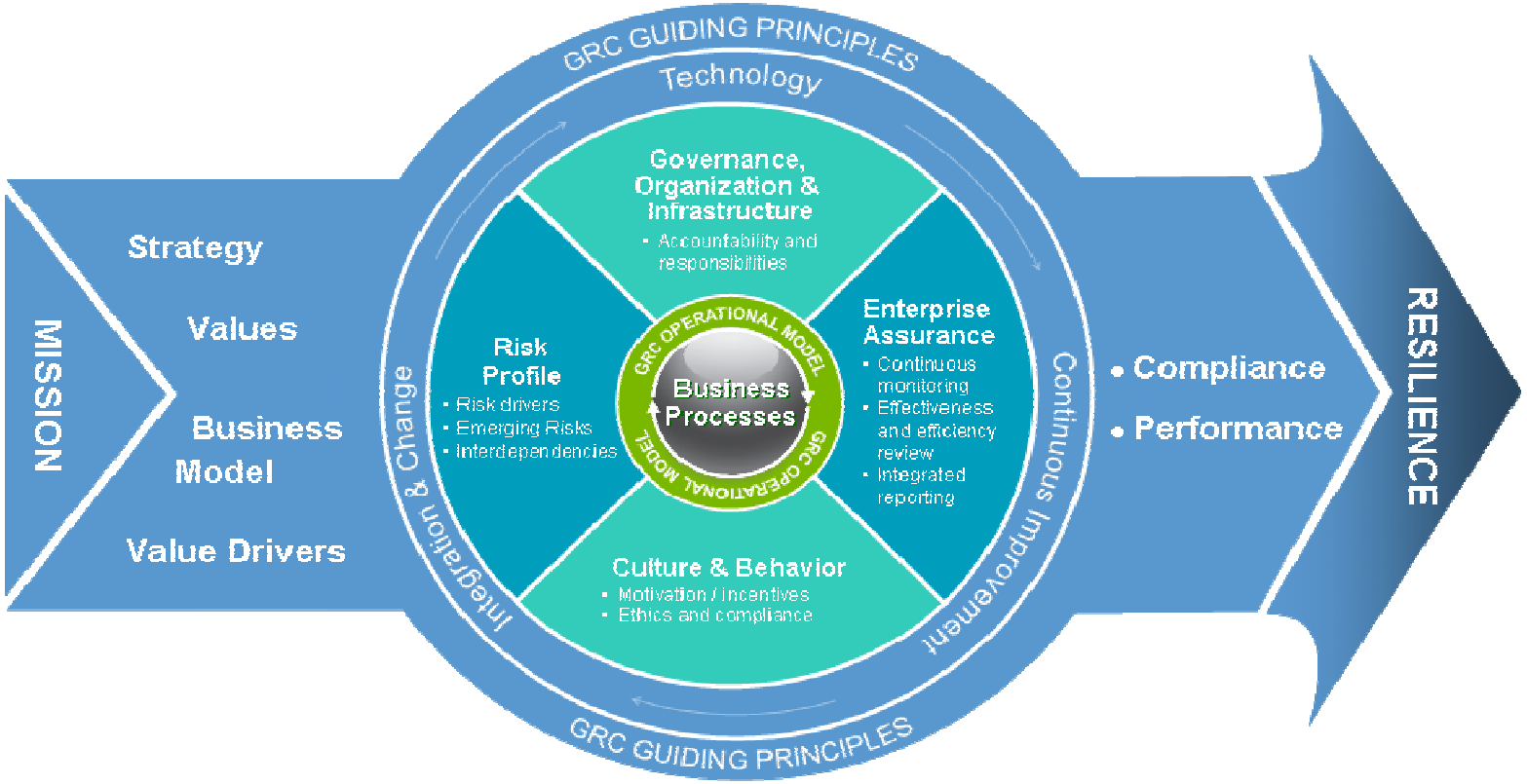
- Lack of visibility across the enterprise.

Business Decision-Making Support

- Lack of real time data.

Holistic Framework

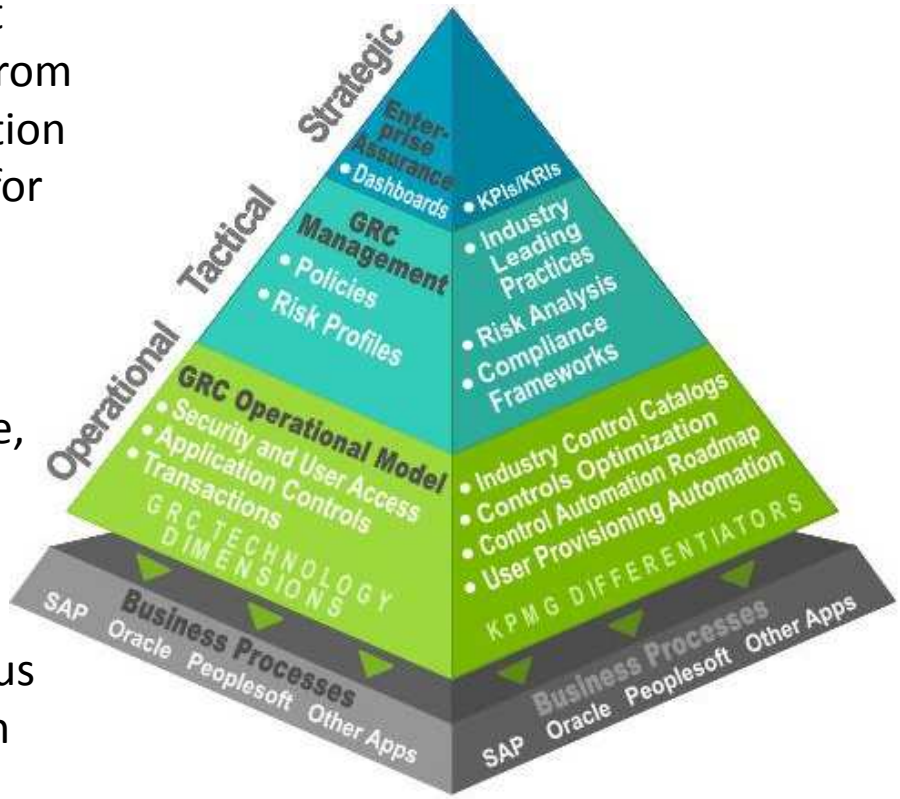
A holistic approach for establishing a successful and sustainable GRC Framework within the organization.



GRC Tool Capabilities

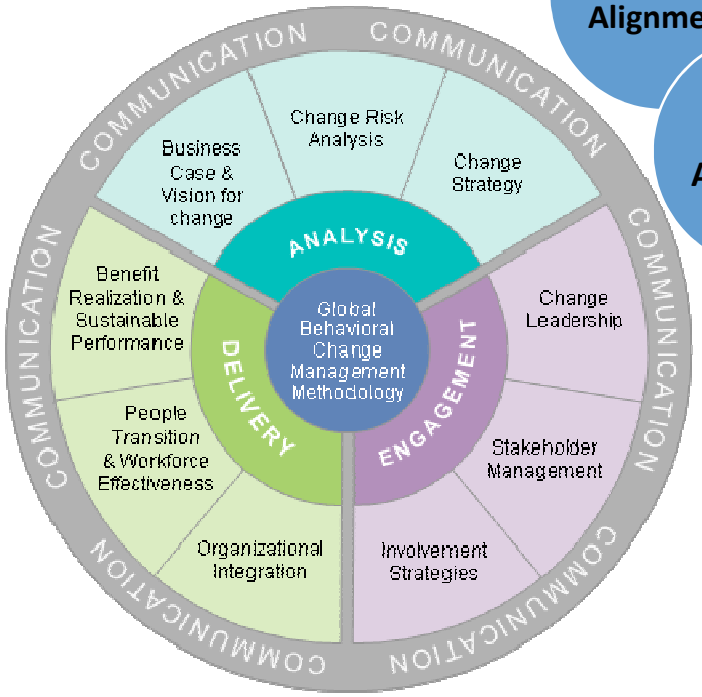
Governance, Risk, and Compliance (GRC) tool capabilities can be broadly classified into three major dimensions as follows:

- **Strategic** – The layer at which management monitors risk and enterprise governance. From a tools perspective, this includes the definition of Risk Monitors, Dashboards and Reports for providing strategic monitoring capabilities.
- **Tactical** – The layer at which an enterprise defines its governance structure, risks, and compliance needs. From a tools perspective, this is the layer where risk and compliance needs can be defined and automated for testing and monitoring.
- **Operational** – The layer at which continuous monitoring is performed by the tools within specific business processes.



Behavioral Change Management

Behavioral and culture change is very critical for enterprise wide GRC deployment. Key principles for managing behavioral & cultural change for GRC are:



Strategic Alignment — Senior leadership alignment critical to success of any change program

Systemic Approach — Behavioral Change is complex, impacting the whole organization

Involve Employee — People perform best in an environment they have been part of designing

Sustained Benefits — Sustaining change is the primary objective of any change program. Measuring the impact of change enables a sustainable approach.

Communications Strategies — Communications is a strategic lever to enhance awareness, buy-in and ownership across the organization

Approach to Implementing GRC

Client Triggers

Strategy, Governance Culture Pain Points

Reporting & Data Pain Points

Process & Systems Pain Points

1. Assessment

- Understand current state and GRC capabilities
- Determine client vision and culture
- Gap Analysis and key areas to enhance

2. Design & Build

- Develop detailed Road Map
- Determine approach and timeline
- Develop technology approach
- Set up project structure

3. Implement

- Implement modular or full approach
- Assist in IT implementation
- Project and Change Management

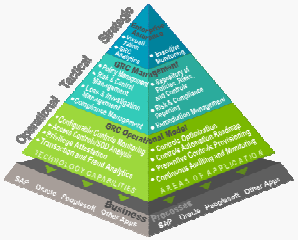
4. Sustain

- Establish process to support Continuous and Sustainable GRC

Established & Integrated GRC Framework

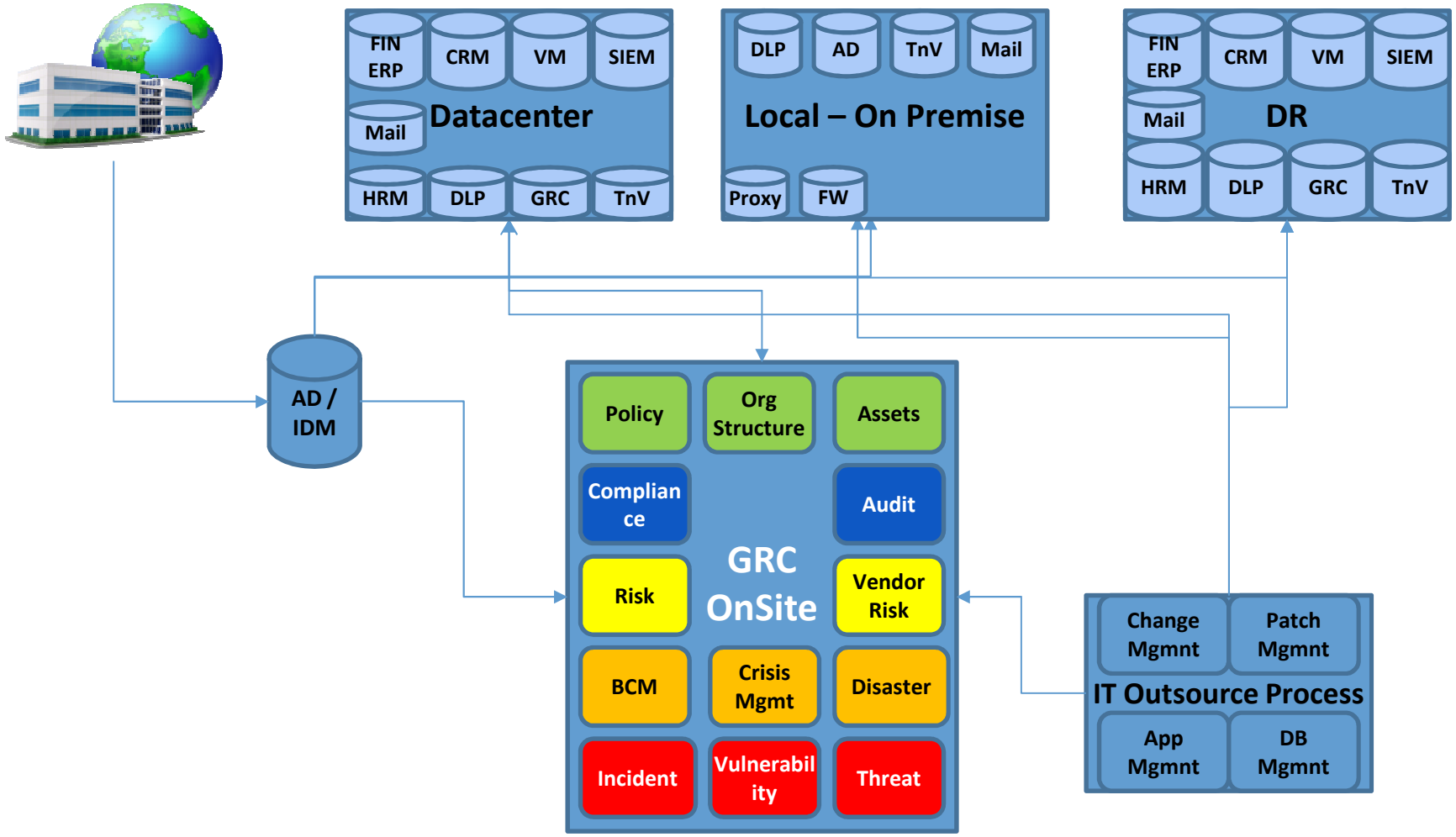
Guiding Principles and GRC Holistic Model

GRC Technology Framework



Change Management Communication Project Management

Metamorphosis of GRC: Stage-3



Benefits of GRC

Increased **consistency and transparency** from enterprise-wide alignment of GRC structures and processes.

Increased **efficiencies** from automated workflow and reporting of GRC processes.

A **centralized view of GRC** issues, events and unresolved findings and improved accountability and tracking.

Cost optimization from leveraging data and processes across departments (e.g., control testing data, risk data, etc).

Real Time reporting across organization level on risk exposure and compliance.

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

GRC Ecosystem in the Cloud

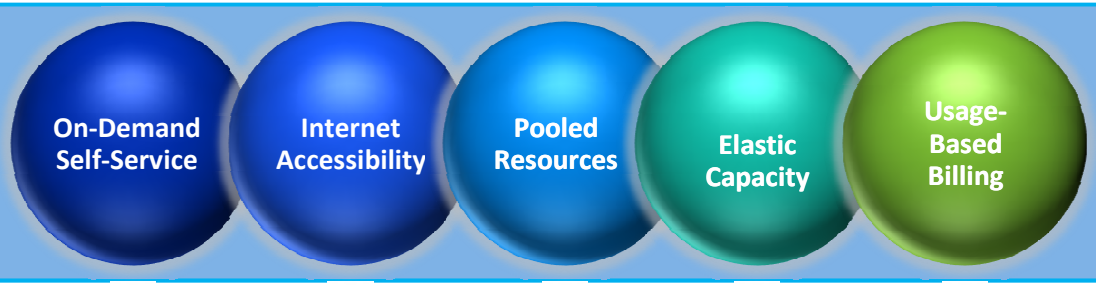
"SaaS is starting to shake things up in areas like CRM (customer relationship management) and human resources, where it is replacing on-premises systems. SaaS is also making some inroads in GRC (governance, risk and compliance) and application development"

-Forrester-

Understanding The Cloud Operating Environment

Cloud Environment	=	Internet-based data access & exchange	+	Internet-based access to low cost computing & applications

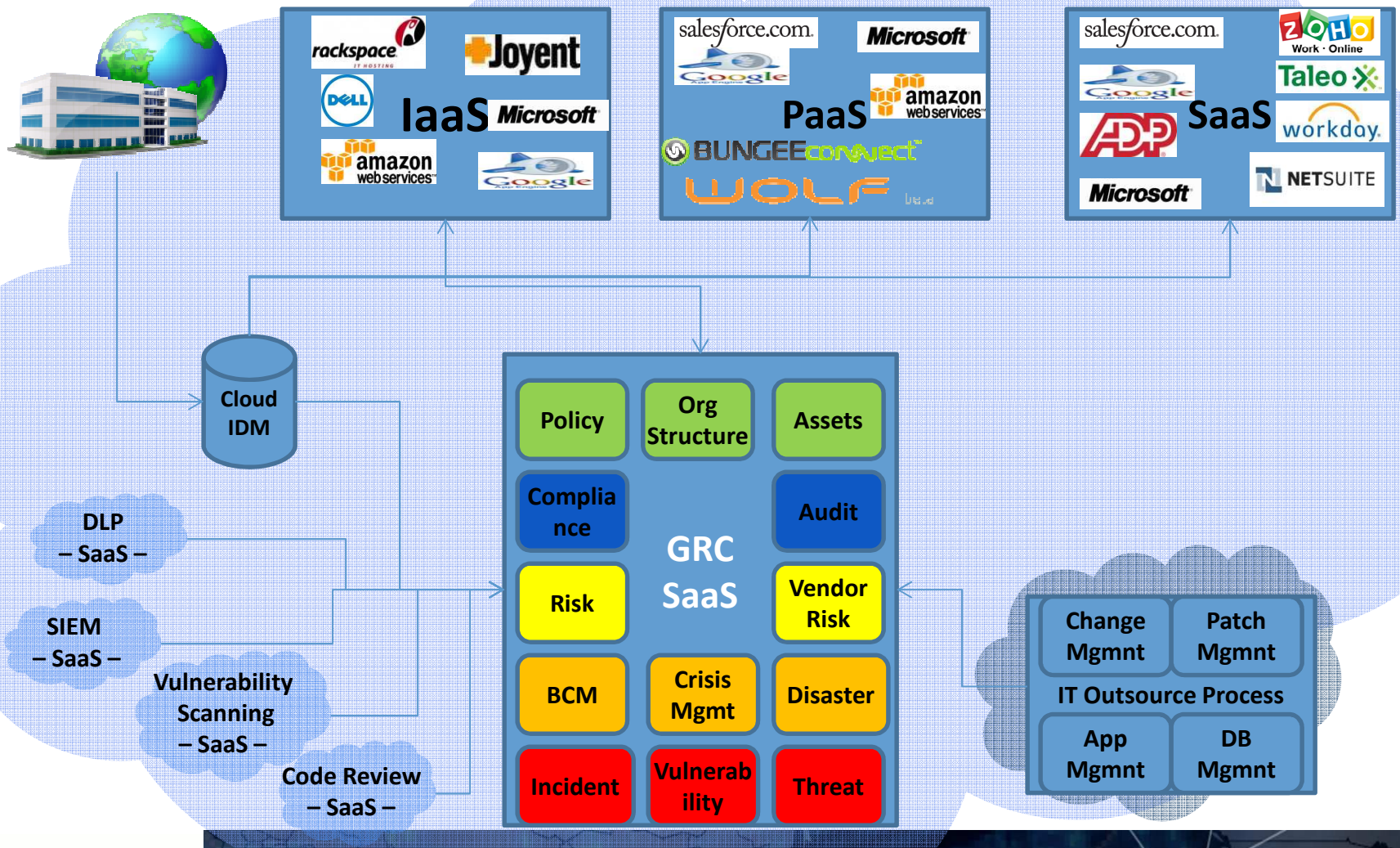
Cloud Environment Characteristics:



Cloud Service Models		
Software as a Service *Business operations over a network* ***"SaaS"***	**Platform as a Service** *Deploy* **customer-created** *applications to a cloud* ***"PaaS"***	**Infrastructure as a Service** *Rent processing, storage, network, other computing resources* ***"Iaas"***

Cloud Deployment Models	
Private	Operated for a single organization
Public	Available to the general public or large industry group, owned by an organization selling cloud services
Community	Shared by several organizations, supporting a specific community

Metamorphosis of GRC: Stage-4



ISACA
Trust in, and value from, information systems
San Francisco Chapter

Back to Business

GRC in Cloud – Pros & Cons

Pros

- Low cost of ownership:
- Low effort on maintenance of Infrastructure
- Standardization of Governance process
- Possible Replacement for Legacy Technologies
- Easy to Scale

Cons

- Integration with other applications
- Limited control over Access Management of Infrastructure
- Limited visibility of SaaS provider operations, data handling, security etc

Case Study

Onsite

Goal: To implement enterprise wide GRC solution to manage risk and compliance effectively.

Implemented following modules:

- Enterprise Asset management;
- Risk Management;
- Compliance Management;
- Exception Management
- Vendor Risk Management

SaaS

Goal: To implement enterprise wide GRC solution to manage risk and compliance effectively.

Implemented following modules:

- Enterprise Asset management;
- Risk Management;
- Compliance Management;
- Exception Management
- Vendor Risk Management
- Policy Management

Case Study

Onsite

Infrastructure required

- Primary site
- DR site
- Separate third party instance in DMZ

HW Maintenance required

- Primary site
- DR Site

Pricing

- Priced per module

# of users

- > 30000 (Active users <10,000)

SaaS

Infrastructure required

- None

HW Maintenance required

- None

Pricing

- Priced per user

# of users

< 500

SaaS offerings by GRC vendors

- **Normally GRC SaaS vendors provide following:**

Business Benefits
- Up and running instantly
- Quick time to market
- Low cost to get started

Infrastructure Maintenance
- Application Upgrades
- Hardware Installation
- Hardware Maintenance
- Operating System patches

Security
- Intrusion Detection
- Firewall
- Virus Protection
- Monitoring

Continuity
- Daily Backups
- DR Facility (may be)

Key Questions for SaaS provider

1. What will the service do?
2. How thorough is the vendor's service-level agreement?
3. How much will data backup cost, and how quickly can you get at data once it's been backed up?
4. How is intellectual property handled?
5. Do the vendor's policies and procedures map to mine well enough for me to comply with HIPAA, SOX and any other regulations that might apply?
6. Where is my data?
7. Is the data encrypted?
8. Is the vendor bound to give me physical access to the servers housing my data?

Questions

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

Thank You

Tony Buffomante

&

Dhawal Thakker