

Inputs to Archer

Feeds

- Audits – Findings
- CMDB – Devices
- App Scans – Findings
- Risk Assessments – Findings
- ISO / Agency Head – Exceptions
- CETR / PARS – Technologies
- ISO / Helpdesk – Incidents
- Dell Secure Works – Vulnerabilities

Application Info

- Audits
- Risk Assessments
- All Policies
- Risk Treatment Plans
- Business Plans
- Scans
- Control Procedures
- Applications
- Risk Register
- Security Exceptions
- RTP
- Data Sets
- Quarterly Updates

Data In

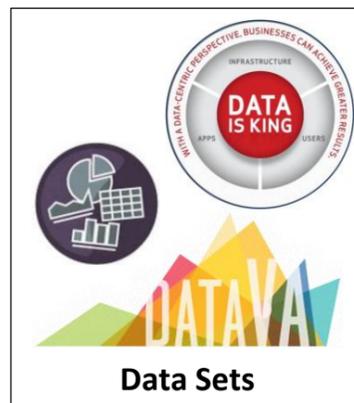


VITA

Archer



Archer is the commonwealth's governance, risk, and compliance tool. It is the system of record for maintaining information on agency apps, associated business processes, devices, and data-set names. RSA Archer GRC provides IT security risk and compliance features. RSA Archer GRC solutions allow building an efficient, collaborative **enterprise governance, risk and compliance (GRC)** program across IT, finance, operations and legal domains. With RSA Archer GRC, one can manage risks, demonstrate compliance, automate business processes, and gain visibility into corporate risk and security controls.



Application Information



Business Processes

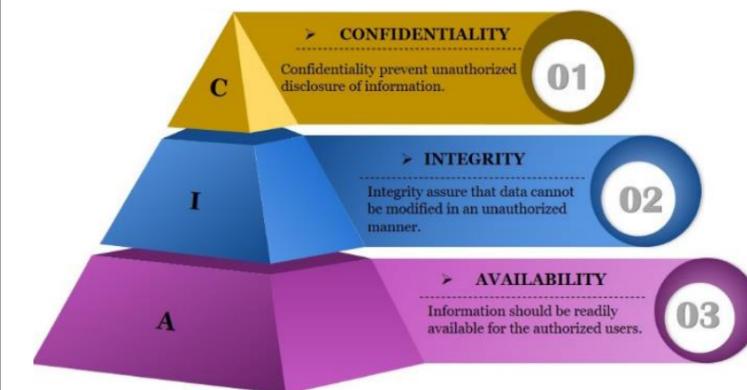
Risk Analysis Out



Agencies

Output

Operational Analysis

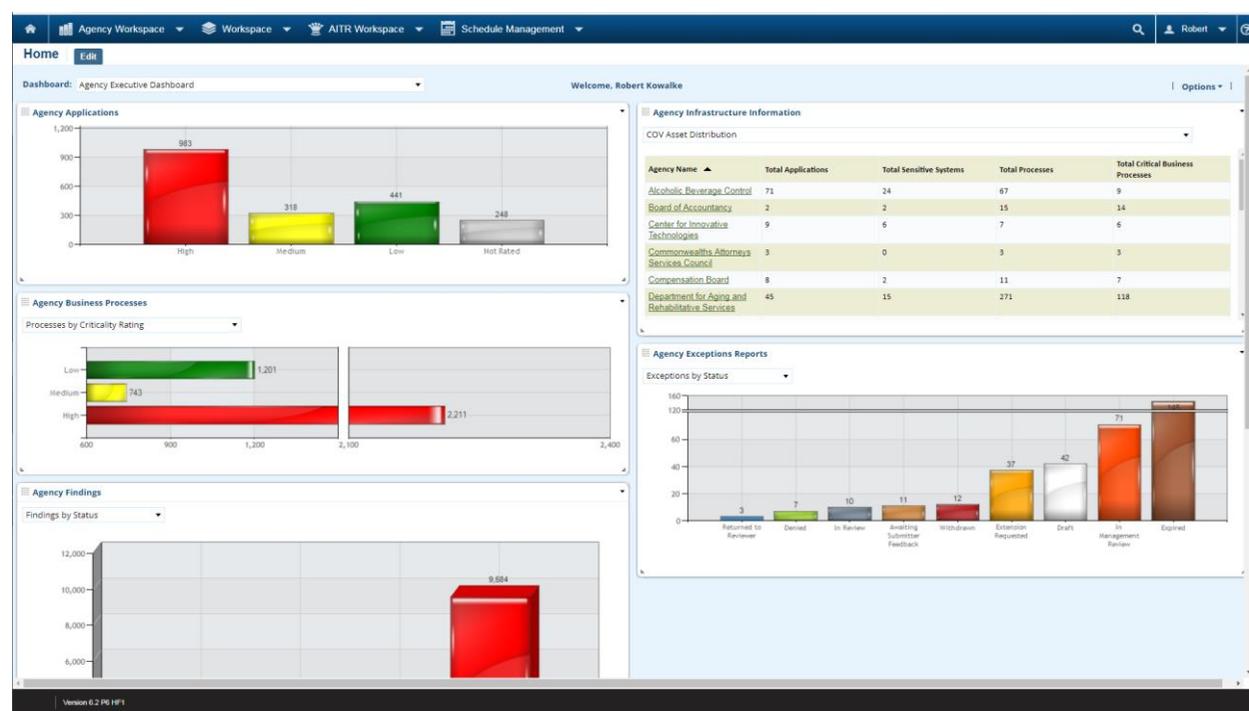


Confidentiality Integrity Availability (CIA)



Agency Consumable Risk Output





Organizations often also establish "risk tolerance" thresholds. These are almost always less than the related risk appetite and represent the level of risk the organization is willing to take on a day-to-day or transaction-by-transaction basis (Figure 1).

Introduction to the RSA GRC Reference Architecture

Governance, Risk and Compliance (GRC) represents a business oriented approach to establishing ownership and accountability throughout the organization to improve decision making.

Governance is the act of directing, controlling and evaluating the culture, policies, processes, laws, and institutions that define the structure by which organizations are directed and managed.

Risk is the negative effect of uncertainty on achieving objectives; **Risk Management** is the coordinated activities to direct and control an organization to realize opportunities while managing negative events.

Compliance is the act of adhering to, and demonstrating adherence to, external laws and regulations as well as organizational policies and procedures.

While these definitions may seem straightforward, establishing a GRC program within an organization is not a simple task. It is also not a new concept. Companies have been focused on improving compliance and managing risk for years. Since GRC programs have many moving parts, organizations are implementing an overarching vision of how things fit together to maximize value. This vision not only should clarify the objectives of a GRC program – but also give context to how the organization executes this strategic initiative.

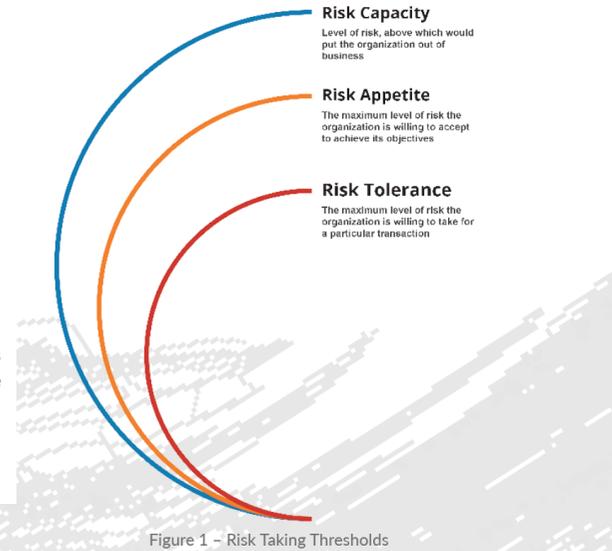


Figure 1 - Risk Taking Thresholds

Agency Executive Dashboard

- Agency Actionable Dashboard
- IT Security Audit Dashboard

Quick Links

- Applications that Need a Dataset
- List of Devices
- List of All Systems
- IT Security Audit Plans
- List of Business Processes
- Application Add/Update: CETR Register for ISOG Meeting
- CETR (if you have a CETR account)
- Review Business Processes not Ready for CSRM...
- Map data sets that aren't mapped to applications
- Review Applications Not Associated with Bus...
- Ensure All Sensitive Systems are Scheduled for update within the Quarterly Findings to be Updated
- View Applications Incomplete Datasets
- Applications without DEVICES Associated
- Data Sets that NEED A Questionnaire
- Sensitive Systems
- IT Risk Assessment Plans
- Register for IS Orientation

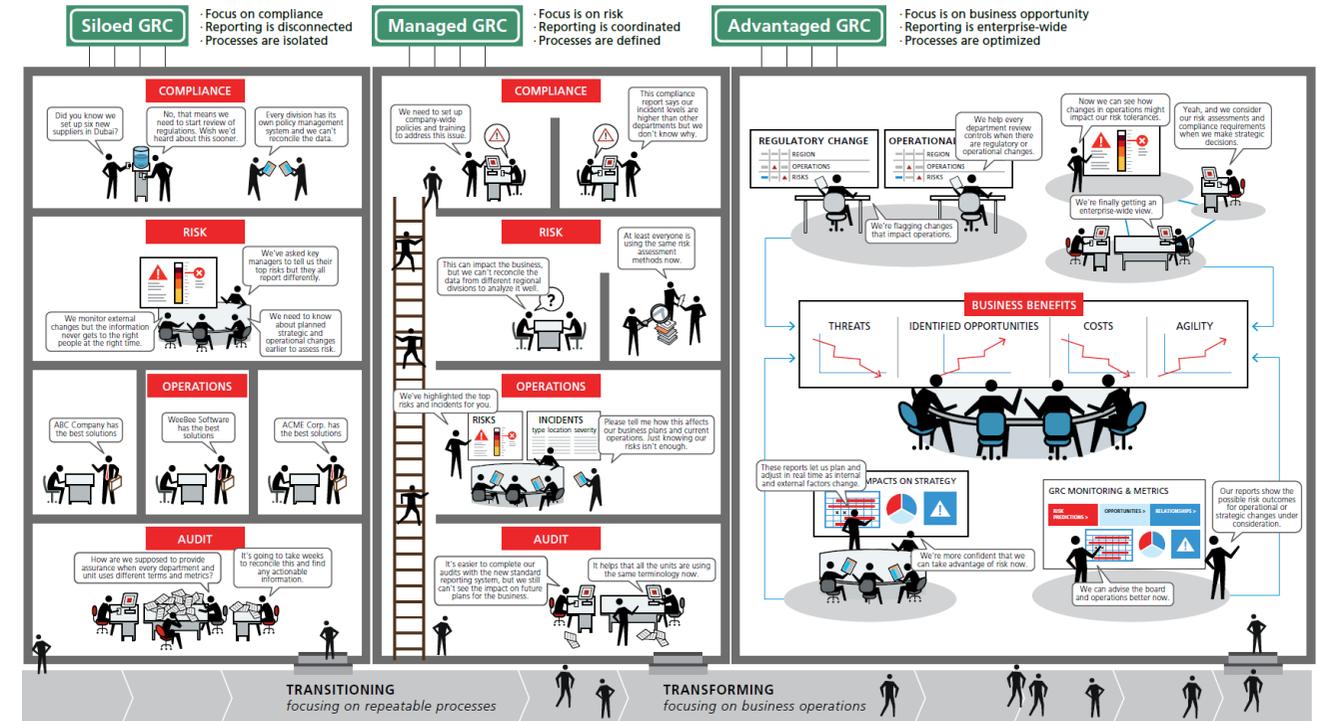
Solutions

- Agency Management
- IT Infrastructure
- Business Infrastructure



The Journey to Advantaged GRC

As organizations mature their approach to GRC, they transition from a structure of siloed departments and units to a fully engaged business operation where everyone has a part in managing risk, ensuring compliance and contributing to performance outcomes. This leads to greater confidence, agility and resilience - advantages that ensure success.



Contact info@ocgg.org for comments, reprints or licensing requests ©2016 OCGG for additional GRC illustrations and resources visit www.ocgg.org/resources

See other side for the model/diagram – this side is just the backpage for additional information.