



# 8 Keys to a Successful GRC Program

Phil Aldrich, CISSP, CISM, CISA, CRISC, CIPP  
Sr. Manager, GRC Program Office  
EMC

Jennifer Anderson, PMP  
GRC Program Director  
Verterim, Inc.

RSA Archer Webcast  
Jan 30, 2014

# Introductions

- Phil Aldrich

[philip.aldrich@emc.com](mailto:philip.aldrich@emc.com)

- Archer customer since 2007 (Iron Mountain)
- 2 year Tour of Duty at RSA managing Archer PMM team
- Currently GRC Program Manager for EMC

- Jennifer Anderson

[janderson@verterim.com](mailto:janderson@verterim.com)

- Former GRC Program Director at a large financial services company
- Currently GRC Program Director at Verterim, Inc.



**“My presentation lacks power and it has no point.  
I assumed the software would take care of that!”**

# Presentation Objectives

*Share our experience as it relates to best practices and effective GRC Programs*

- **DEFINE** the 8 Key of Successful GRC Programs
- **UNDERSTAND** the application of the keys
- **HIGHLIGHT** the keys that were most impactful for us
- **OUTLINE IMPLEMENTATION** tips for GRC programs



# Taking the Leap...to an Enterprise Focus

## Optimized

- Program Managed
- Strategic
- Senior Executive support



## Basic

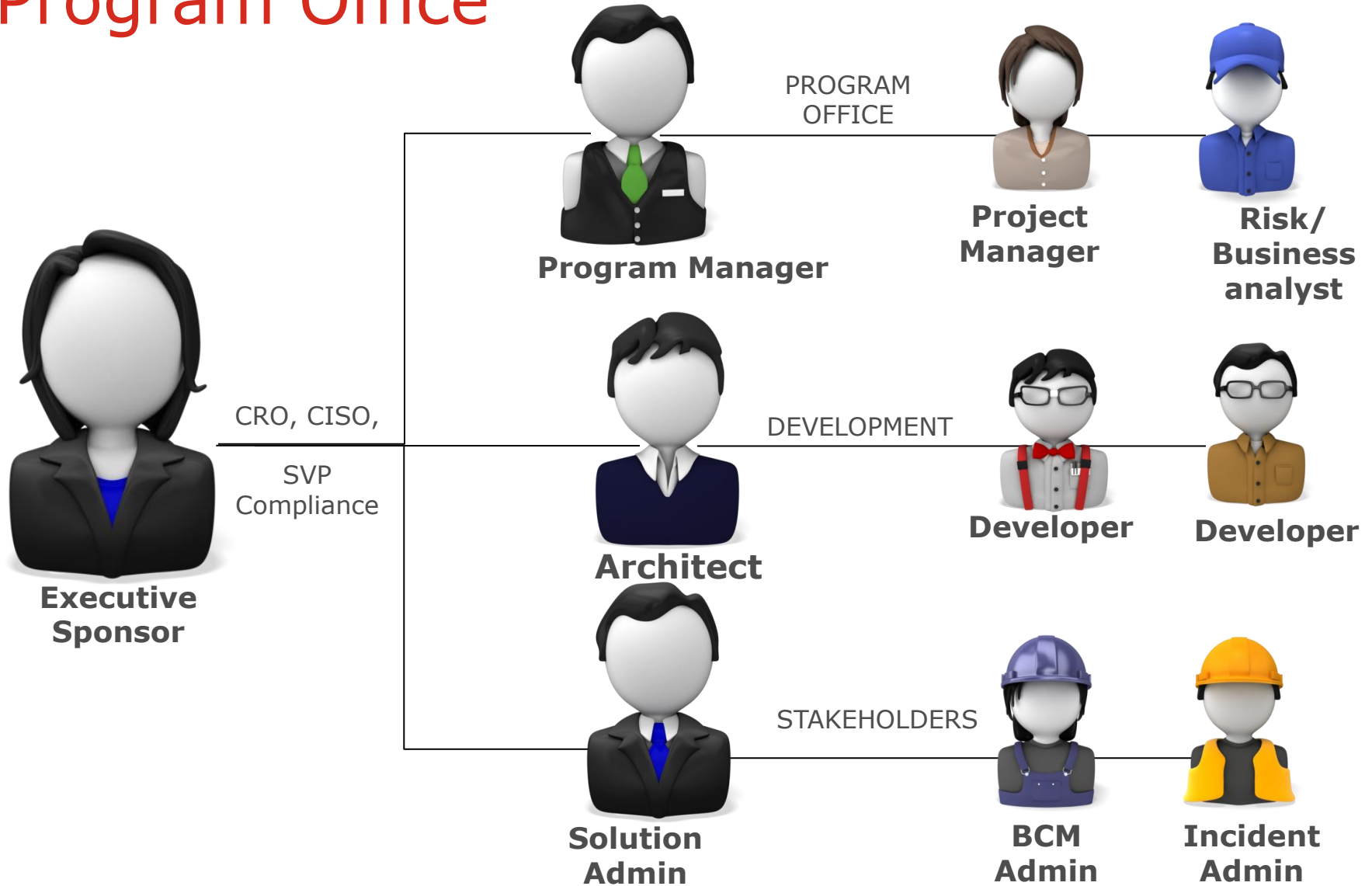
- Department Led
- Use case focused
- Limited Executive support

# 1<sup>st</sup> Key - Establish GRC Program Governance

- **Strong Executive Sponsor**
  - Influence a Strategic Vision
  - Align other GRC Functional Teams
- **Dedicated Program Manager**
  - Accountable for Program growth
  - Primary point of contact with business
- **Establish a Core GRC Committee**
  - Enterprise Risk focused
  - Govern Common Archer Components



# Recommended roles for the GRC Program Office



# 2<sup>nd</sup> Key – Manage the Program

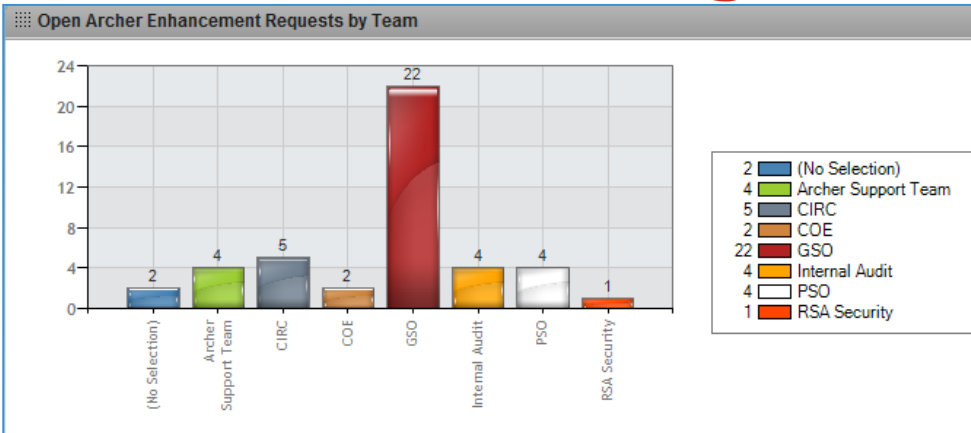
**Programs coordinate multiple related projects and operations to achieve a common, strategic objective.**

## **How do we cultivate a GRC program?**

- Scale your program
- Dedicated GRC team
  - Strong Program Manager
  - Skilled configuration and business analysts
- Anticipate and manage demand and change management
- Develop and maintain a program communication plan
  - Communicate success



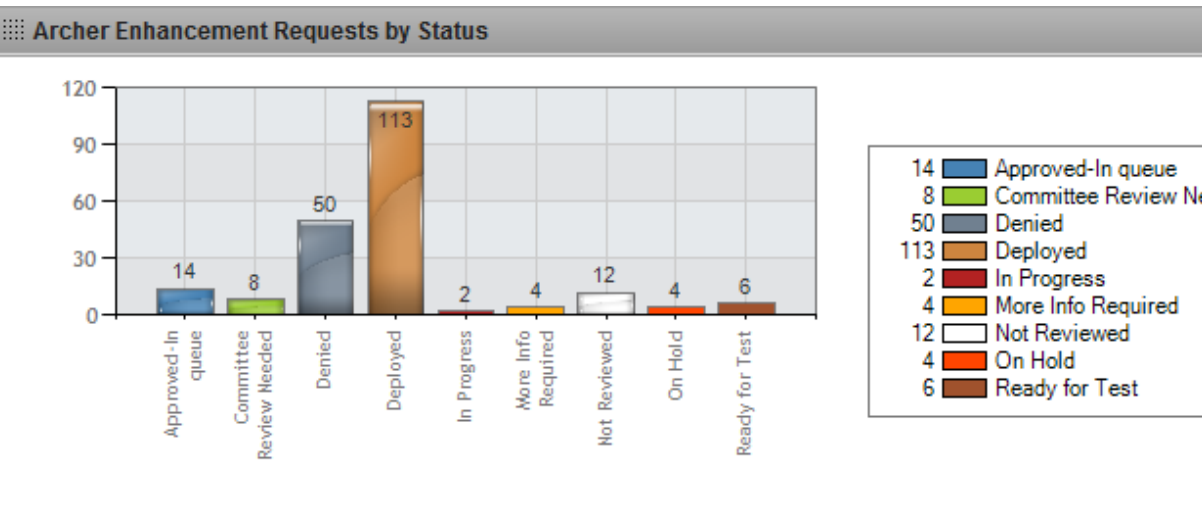
# View to the Kingdom: Managing Demand through On Demand



### FAQ's

#### Frequently Asked Questions

- [Submit an Archer Business Request \(New GRC Use Case\)](#)
- [Submit an Archer Enhancement Request](#)
- [Submit CCI - Charitable Contribution Request](#)
- [Email the GRC Program Team](#)
- [Report an Observation](#)



### Business Workspaces

- GSO
- CoE
- CIRC
- Enterprise Risk
- Internal Audit
- PriSM
- Legal
- Supply Chain





# Communicate, Communicate, Communicate

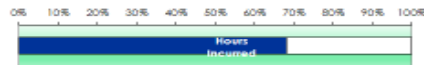
## GRC Implementation Project Status Report – week ending 1/31/14

Project: GRC Implementation  
 Client Executive: Phil Aldrich  
 Veritem Project Manager: Jennifer Anderson  
 Veritem Consultant(s): Kelley Boutelle,  
 Monica Basile

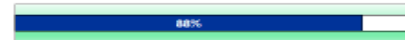
GREEN



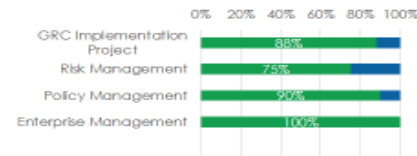
D. BUDGET TO ACTUAL TO DATE: 170 BUDGET, 250 ACTUAL,  
 BURN RATE = .85 (<1 = under budget, 1 = on budget, >1 = over budget)



E. GRC Project Implementation COMPLETION:



F. WORK PLAN STATUS UPDATE BY PROJECT: OVERALL PROJECT IN GREEN, ON SCHEDULE TO COMPLETE 2/14/14



### A. KEY ACTIVITIES FOR WEEK ENDING 1/31/14:

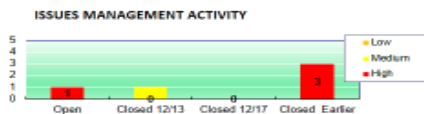
- COMPLETED THE BUILD OF RISK MGT
- MIGRATED ENTERPRISE MGT TO PROD
- COMPLETED 90% OF POLICY TESTING

### B. UPCOMING ACTIVITIES FOR NEXT WEEK

- CONFIGURE RISK DASHBOARDS / REPORTS
- COMPLETE UAT POLICY TESTING, MIGRATE TO QA & PROD
- COMPLETE UAT RISK TESTING

### C. KEY ISSUES:

- TECHNICAL ISSUES
  - HIGH – THE DEV SERVER IS HAVING ISSUE



4



## Sample (Archer) Incident Management Project Charter

### Background

Define the business background and problem statement to be resolved with this charter. As an example; information security incidents are currently recorded through Excel workbooks and SharePoint. These have little capability for automated reporting and all escalation is manual

### Project Objective:

Automate the information security incident process through the implementation of RSA Archer Incident Management. Create automated workflow, escalation, dashboards for security analysts, director, vice president and internal 'customers', support the key performance indicators and metrics.

### Benefits:

- Estimated process efficiencies of 100 hours per month or \$120,000 annually
- Provide ability to correlate data which was previously unavailable.

FOR EXAMPLE PURPOSES ONLY

### In Scope for the project:

- Automate the incident management process
- Integrate with the current live reporting system, organizational structure and applications / devices
- Dashboards, metrics (KPIs, KRIs)

### Out of Scope for the Project

- The integration with policy is out of scope for this project

### Estimated Schedule

Project Phase	Start Date	Complete Date
Analyze	1/13/14	1/24/14
Design	1/22/14	2/7/14
Build	2/10/14	3/7/14
Test	2/20/14	3/18/14
Deploy	3/20/14	3/27/14

EMC GRC Program Office

Volume 1, Q12013

March 2013

# EMC GRC Quarterly

Newsletter Q12013



### INSIDE THIS ISSUE:

- EMC Program office opens 2
- Other Projects Completed 2
- Other Project Kicked off 3
- few BU Requests submitted 3
- EMC Risk Taxonomy Workshop 4
- Other Environment Linerize 4

## NEWSLETTER SUMMARY & HIGHLIGHTS:

- ❖ GRC Program office opened in January
- ❖ Archer Projects Completed in Q1
  - Issues Management
  - Archer Environment Refresh
  - Archer Enhancement Requests
- ❖ Archer Projects Initiated in Q1
  - GSO: Risk as a Service
  - GSO: Controls Assurance Program
  - PSO: Source Code Assessment
  - Data Center Services: Disaster Recovery Management
- ❖ New Business Requests for Archer GRC Program
  - Global Services: SOW Management (UK)

# 3<sup>rd</sup> Key – Conduct a Strategic Plan

- Be a Leader & Define the Vision
  - Set & Communicate GRC Program Goals
  - Partner with key GRC Stakeholders
- Prioritize Business Use Cases
  - Interview Business Stakeholders
  - Understand Requirements
  - Assess BU readiness

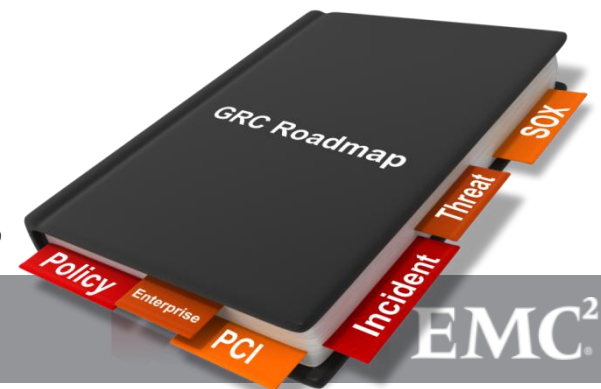


# Example GRC Business Request Form






1. What is your business unit?
2. What part of the company do you support?
3. Who are the key stakeholders for this GRC request?
4. Do you have a clearly defined process you wish to implement?
5. Do you have detailed business requirements ready?
6. Please describe your current process (outside of Archer)
7. What the primary drivers are influencing this request? (choose all that apply)
8. How many Full Time Employees currently manage your process?
9. Please describe your desired GRC use case (using Archer)
10. Please explain how does this request will help manage risk at our company?
11. What are your metrics to define success for this use case (i.e. Decommission software costs of \$150K/year, decrease report creation by 50%, reduce manual labor by 100hrs/month)?
12. How critical is automating this use case within Archer?
13. What are you willing to spend to fund the initiative?



- Create a Holistic GRC Plan
  - 12-18 month Roadmap
  - Communicate to Stakeholders



# 4th Key – Implement Engagement Model

PROJECT PHASE	KEY ACTIVITIES / DELIVERABLES	ACCOUNTABILITY			WORK EFFORT	ENVIRONMENT
		Contractor	GRC Office	BUSINESS		
 <p><b>Initiation</b> Initial consultation between the business customer and GRC Office to determine if RSA Archer provides a solution both strategically as well as tactically.</p>	<ul style="list-style-type: none"> <li>Project Request Record</li> <li>Readiness Assessment</li> <li>General Requirements</li> <li>Prioritization of Project</li> <li>Creation of SOW</li> </ul>	CONSULTED	OWNS REVIEWS REVIEWS OWNS APPROVES	INITIATES COMPLETES DOCUMENTS CONSULTED APPROVES		Archer Business Unit use case requests are recorded in an on demand application in the EMC Archer Production environment.
 <p><b>Detailed Requirements/Design</b> Scope of the project is defined (Business Requirements) and the solution to be implemented (Project Application Binder – technical requirements).</p>	<ul style="list-style-type: none"> <li>Business Requirements</li> <li>Project Plan</li> <li>POCs created</li> <li>Design sign off</li> </ul>	DOCUMENTS OWNS OWNS	CONSULTED CONSULTED CONSULTED CONSULTED	CREATES CONSULTED APPROVES OWNS	50%	DEVELOPMENT
 <p><b>Build</b> With a clear definition of the project, the application is configured and presented to the customer for review and testing.</p>	<ul style="list-style-type: none"> <li>Configuration</li> <li>Build sign off</li> </ul>	OWNS	CONSULTED CONSULTED	CONSULTED OWNS	25%	DEVELOPMENT
 <p><b>Test</b> With a clear definition of the project, the application is configured and presented to the customer for review and testing.</p>	<ul style="list-style-type: none"> <li>Migration to QA</li> <li>QA Use Case Test Plans</li> <li>Remediate Issues</li> <li>Conduct Training</li> </ul>	CONSULTED CO-OWNS OWNS CONSULTED	OWNS CONSULTED CONSULTED CONSULTED	CO-OWNS CONSULTED CONSULTED OWNS	12.5%	TEST
 <p><b>Implementation</b> Properly tested and solid planning will result in a seamless production release. The project is closed out within an appropriate timeframe after it is released to production.</p>	<ul style="list-style-type: none"> <li>Migration to PROD</li> <li>PROD Test Plan Initiated</li> <li>Communication Plan Executed</li> <li>Post - Lessons Learned</li> </ul>	CONSULTED	OWNS CONSULTED CONSULTED OWNS	CONSULTED OWNS OWNS CONSULTED	12.5%	PRODUCTION

# Define Business Processes & Requirements Before Building Applications

- Identify the Business Problem
- Collaborate with the Business to define the 'as is' process and the 'future' Archer process
  - Identify key stakeholders & their role
  - Recognize the connection among the new and existing information
  - Take the opportunity to improve the process, enhance & mature the GRC environment
  - Capture meaningful process metrics





# 5<sup>th</sup> Key – Strengthen the Core Pillars of your GRC program

- **Define Risk Taxonomy and Risk Register**
  - Enterprise level Impact & Likelihood
  - Build your Catalog of Business Risks
- **Identify your control environment and potential relationships to risk**
  - Clarify your key controls based on regulatory requirement and risk posture
- **Identify your Critical Assets**
  - Understand what assets are High Value to your organization
  - Without Context, you will always live in the weeds





# 6<sup>th</sup> Key – Align or Fit GRC to Your Organizational Culture



Market your program internally, use common language and align to corporate directives

- Define Core GRC Pillars
- Develop and follow your strategic plan
- Explain GRC in common, business terms
- Promote Business Successes

# Company Culture is directly proportional to GRC Program Success

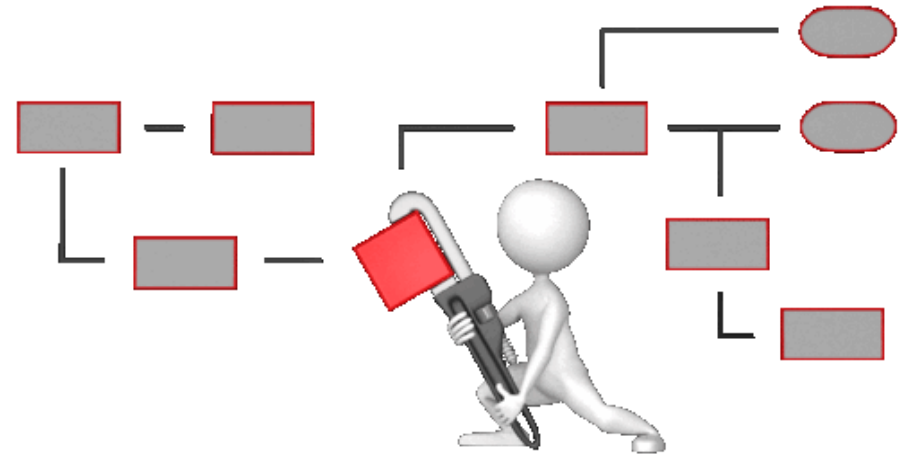


'DETENTION'

# 7<sup>th</sup> Key – Benchmark Your Program

- Seek Out GRC Best Practices

- Archer Community
- GRC forums / conferences
- Whitepapers & Webinars
- Analysts



- Perform Continuous Improvements based on company need and GRC best practices

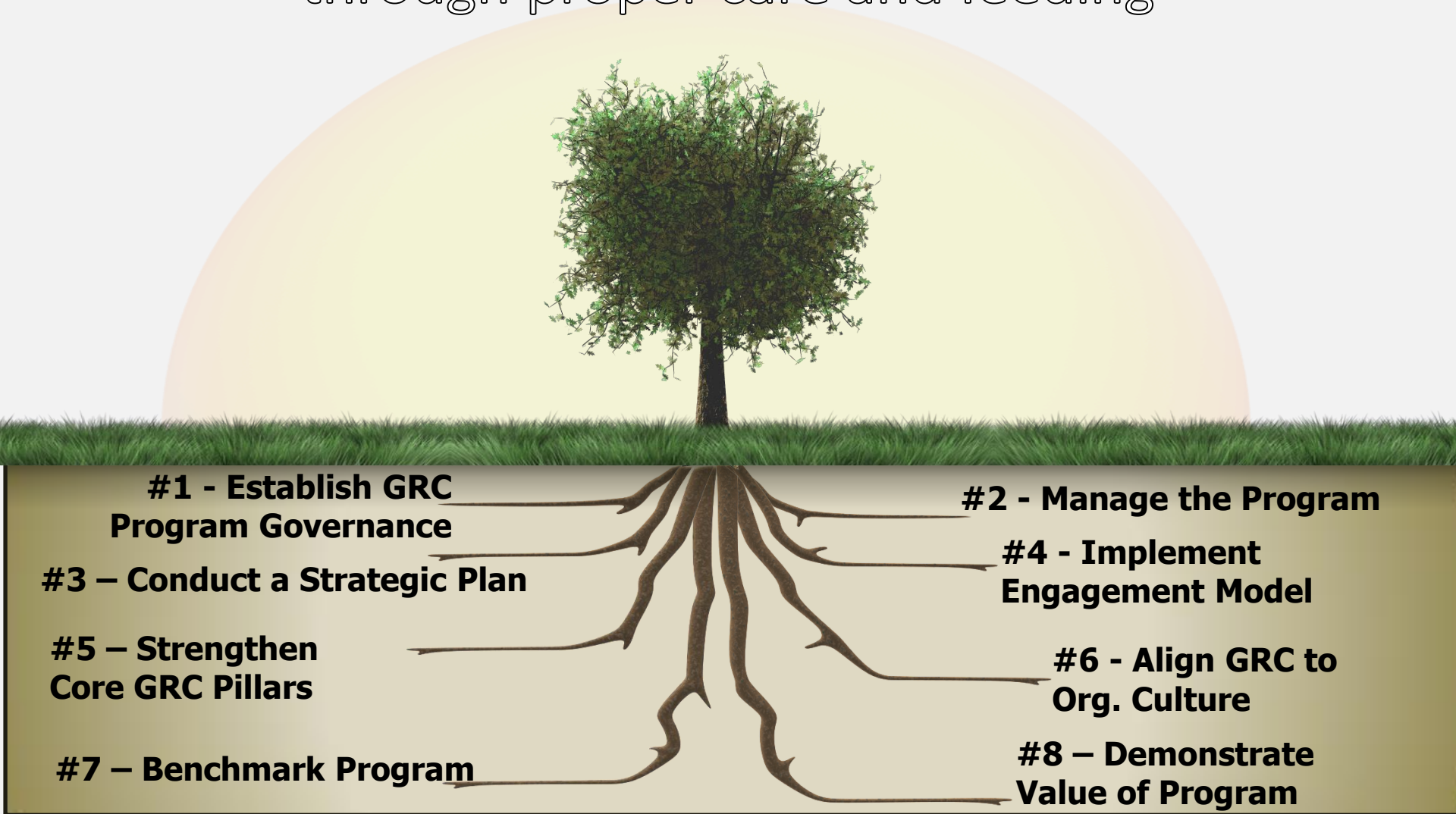
- Use metrics & measurements to improve your program
- Truly listen to the voice of the customer
- Refresh program engagement process
- Continually align the program actions with your governance committees expectations

# 8<sup>th</sup> Key – Demonstrate the Value of the Program

**How is the GRC program providing value to the organization?**

- Develop consistent quantitative and qualitative metrics, statistics and meaningful (business) information to measure the program
- Call out the specific actions / projects that :
  - ✓ Diminish or remediate risk
  - ✓ Strengthen controls
  - ✓ Generally improve the business environment
- Communicate consistently and concisely

# Grow Deep Roots for your GRC Program through proper care and feeding



# Questions?



# RSA Archer Resources

- RSA Archer public web site: [www.emc.com/security/rsa-archer.htm](http://www.emc.com/security/rsa-archer.htm)
- Weekly complementary webcasts on top GRC leadership topics  
[www.emc.com/campaign/global/rsa/rsa-webcast.htm](http://www.emc.com/campaign/global/rsa/rsa-webcast.htm)
- GRC leadership blogs from Archer's product SMEs  
[community.emc.com/community/connect/grc\\_ecosystem](http://community.emc.com/community/connect/grc_ecosystem) and [blogs.rsa.com/category/grc-3/](http://blogs.rsa.com/category/grc-3/)
- RSA Archer GRC Summit is June 10 - 12 in Phoenix, Arizona
- RSA Archer private Community and Exchange

# Thank you

- Phil Aldrich  
[philip.aldrich@emc.com](mailto:philip.aldrich@emc.com)
  
- Jennifer Anderson  
[janderson@verterim.com](mailto:janderson@verterim.com)



RSA Archer ■

# grc summit

