



Driving Value with Information Security Compliance

Presented to: 2015 COV Information
Security Conference

April 2015

northhighland[®]

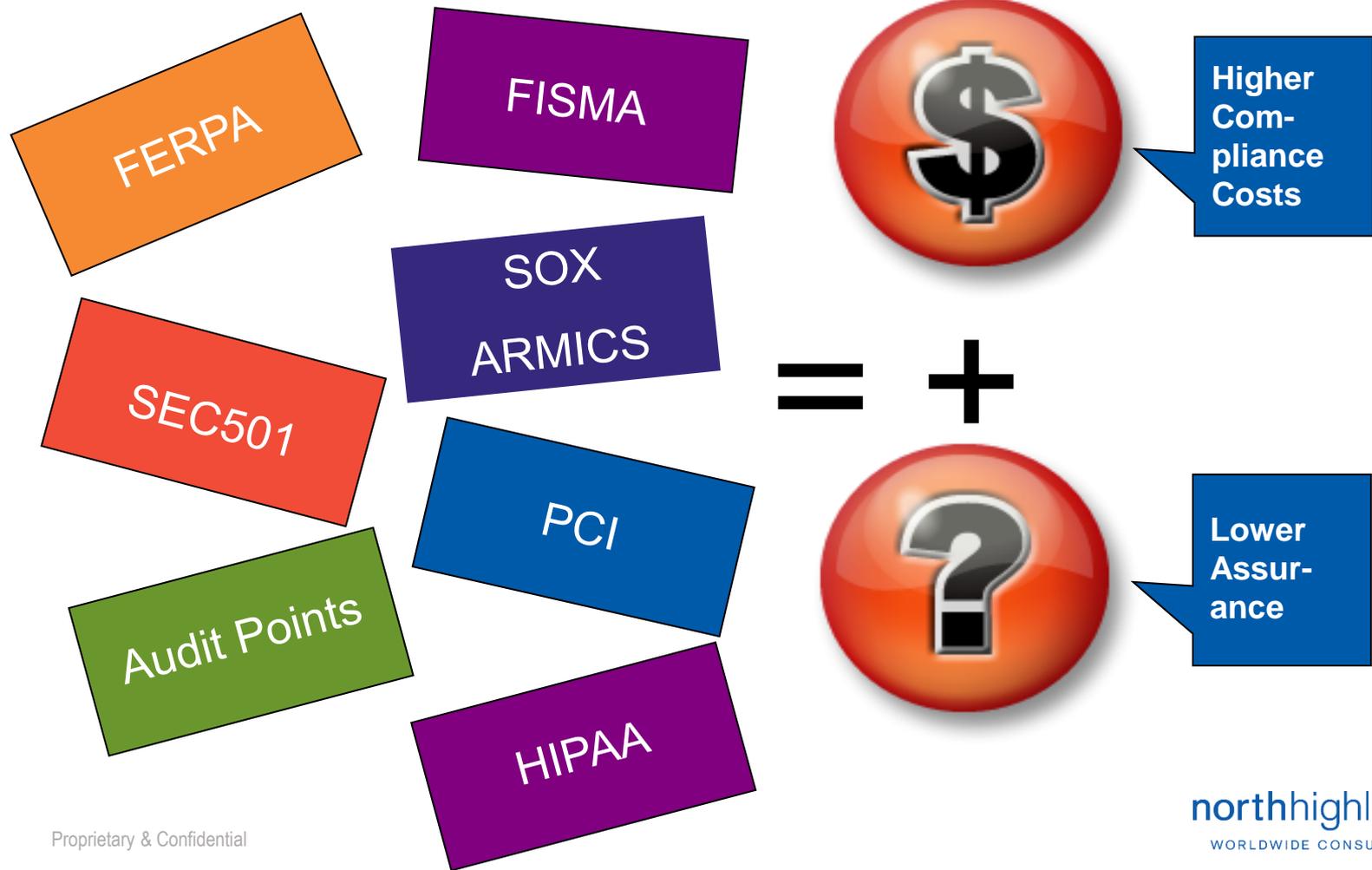
WORLDWIDE CONSULTING

Compliance Requirements are a:

- 1 Distraction from the value-add portions of the security program.
- 2 Necessary evil (emphasis on the evil).
- 3 Key component of moving the security program forward.
- 4 Compliance requirements? I thought this was the “Dancing with the Stars” auditions!

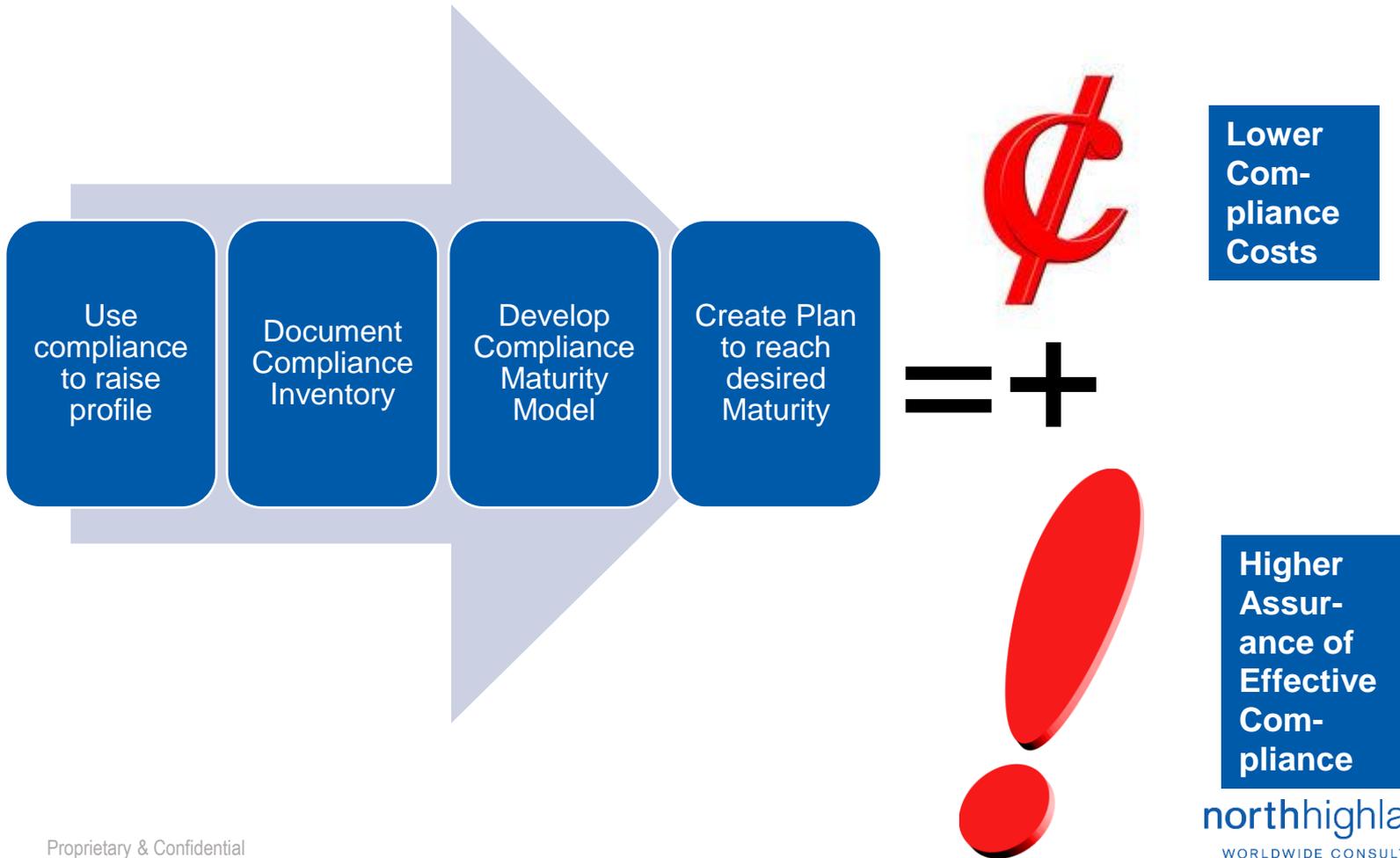
Add Value by Aligning Compliance Efforts

Organizations frequently approach compliance in a piecemeal manner



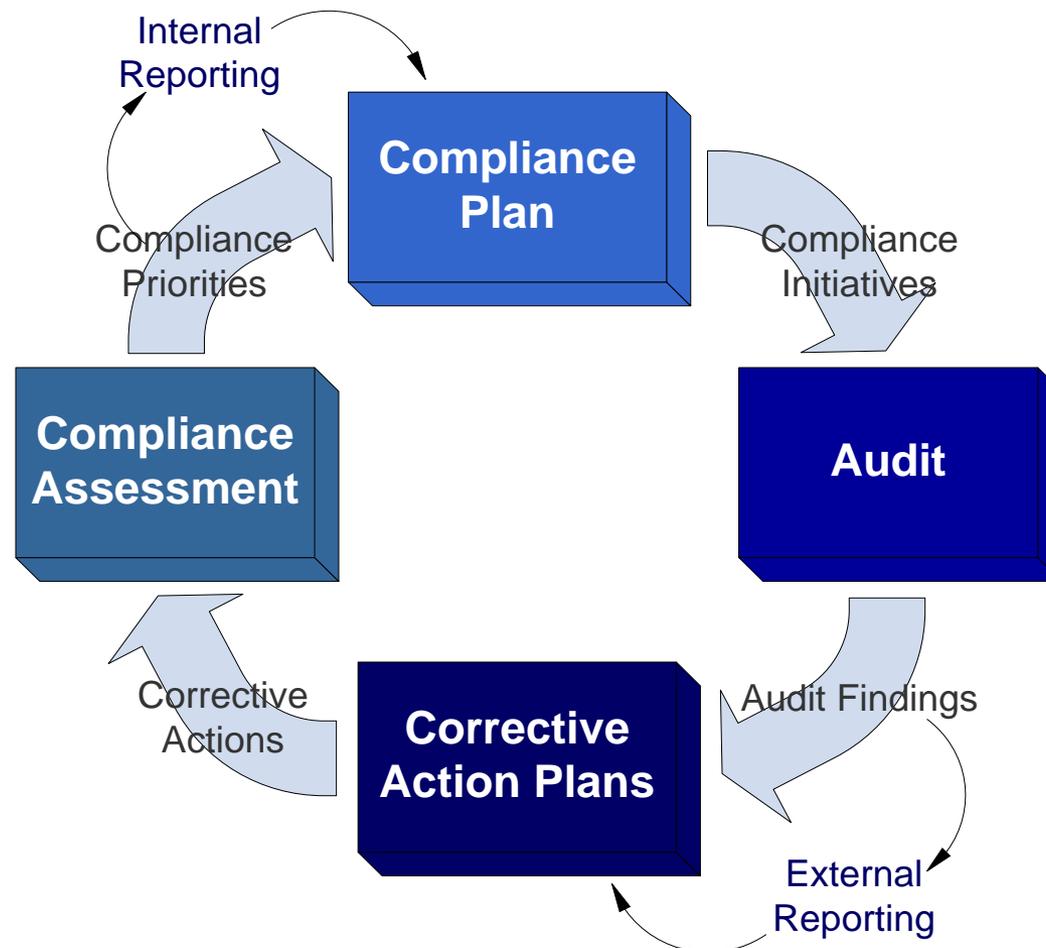
Add Value by Aligning Compliance Efforts

Aligning compliance efforts drives higher value

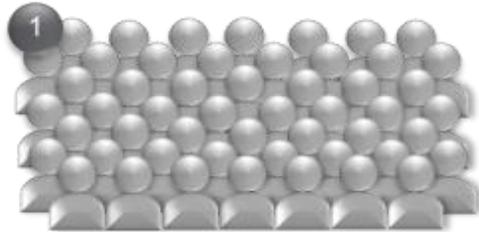


Use compliance to raise profile

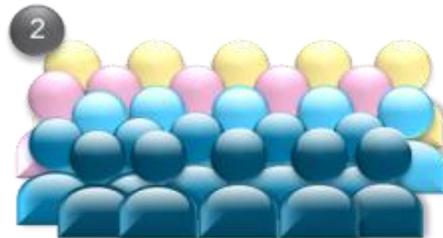
“There’s never budget until there’s an audit point” – use it to your advantage!



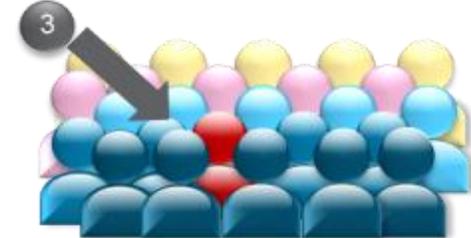
Start by documenting a compliance inventory



Document Requirements



Cluster like Requirements



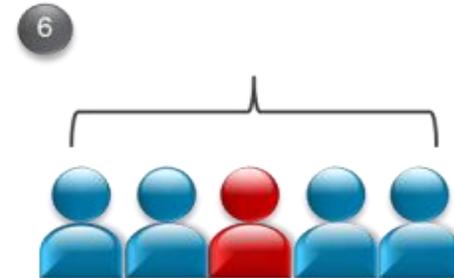
Select Requirements to Assess



Assess Compliance



Report Results



Quantify Results



Develop Dashboard



Communicate Results



Results are input to Maturity Model

Use inventory as input to Maturity Model

Increasing Maturity

Level 5: Optimized

- Process is pervasive, consistent and meets all operating and service level requirements
- Continuous process improvement is enabled and is aligned with business objectives
- High degree of automation exists within and between processes and/or services

Level 4: Managed

- Process metrics have been identified and are routinely collected
- Process measures have been baselined and are routinely collected
- Tools / automation is leveraged to add efficiency to process functions

Level 3: Defined

- Processes and/or services are documented and standardized
- Process has been communicated and is pervasive across the organization
- Some automation is in place for process related activities

Level 2: Repeatable

- Stakeholders involved in performing process and/or service activities have been identified
- Some agreement exists relative to a more consistent approach to process activities
- Documentation exists relative to the process and/or services

Level 1: Ad-Hoc

- Agreement on how to achieve consistent process performance is not in place
- Redundant activities and manual efforts are prevalent within the process and/or service lifecycle
- Documentation is lacking, outdated, or non-existent

Document specific maturity characteristics

Example: Development and maintenance of BIA, RA, CP, etc.

Increasing Maturity

Level 5: Optimized

- Plan development and maintenance activities are consistent across the organization
- There is a plan for improving plan development and maintenance activities at each iteration
- Plan development and maintenance activities are highly automated

Level 4: Managed

- Metrics for plan development and maintenance have been identified and are routinely collected
- Schedule and budget for plan development and maintenance is baselined and updated
- Collection and population of plan data has been automated to increase efficiency

Level 3: Defined

- There is wide organizational acceptance of plan roles and responsibilities
- The process for plan development and maintenance is documented and communicated
- Development and maintenance of plans has been consolidated to eliminate repetition

Level 2: Repeatable

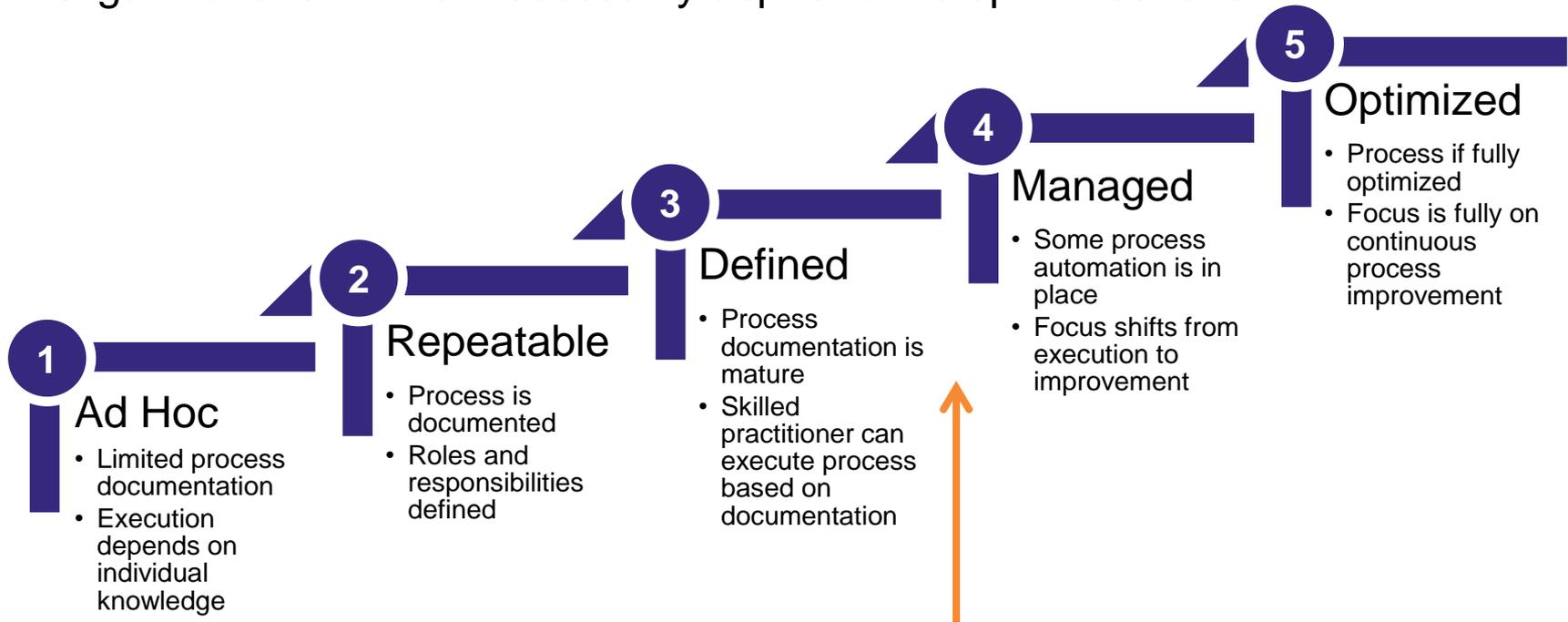
- Roles and responsibilities for developing and maintaining plans have been identified
- There is an informal process in place for documenting and updating plans
- Plans are documented and up to date

Level 1: Ad-Hoc

- There is not clarity regarding roles and responsibilities for plan development and maintenance
- There is not a consistent, repeatable process for documenting and updating plans
- Documentation of plans is incomplete and plans are out of date

Identify the appropriate maturity level

Organizations will not necessarily aspire to the optimized level



Many organizations will find a point between “Defined” and “Managed” strikes the best balance between cost and value added

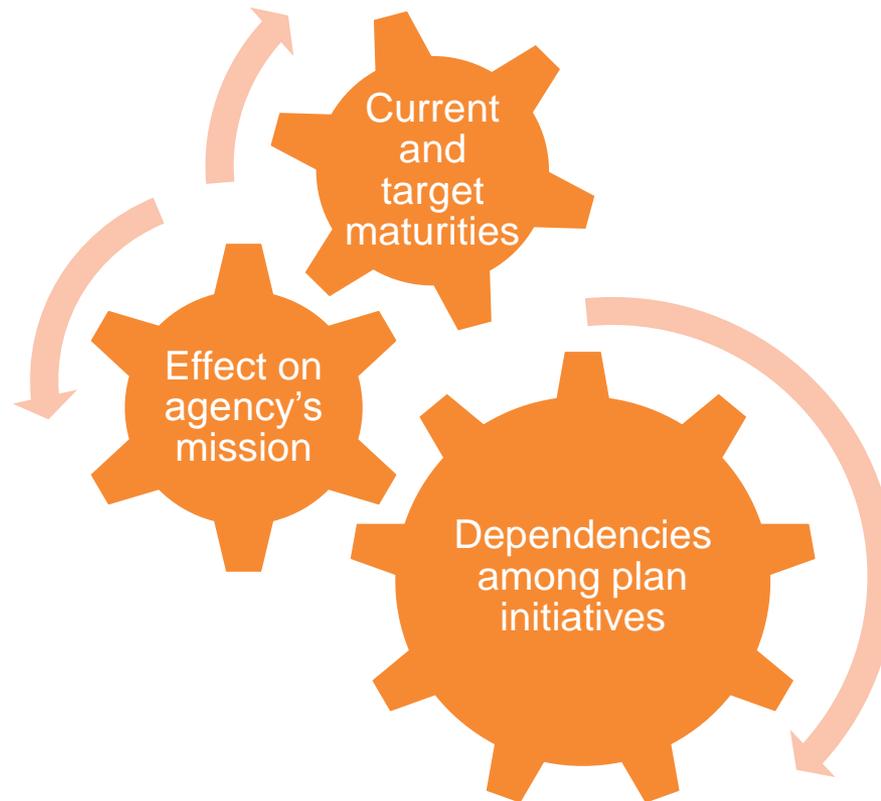
Determine current and target maturity for each compliance area

Example: SEC501 Control Families

Section	Section Name	Current	Target
8.1	Access Control	Ad Hoc	Managed
8.2	Awareness and Training	Repeatable	Managed
8.3	Audit and Accountability	Defined	Optimized
8.4	Security Assessment and Authorization	Repeatable	Defined
8.5	Configuration Management	Managed	Optimized
8.6	Contingency Planning	Ad Hoc	Managed
8.7	Identification and Authentication	Repeatable	Managed
8.8	Incident Response	Managed	Optimized
8.9	Maintenance	Ad Hoc	Managed
8.10	Media Protection	Repeatable	Managed
8.11	Physical and Environmental Protection	Managed	Optimized
8.12	Planning	Managed	Optimized
8.13	Personnel Security	Ad Hoc	Managed
8.14	Risk Assessment	Repeatable	Managed
8.15	System and Services Acquisition	Managed	Optimized
8.16	System and Communications Protection	Ad Hoc	Managed
8.17	System and Information Integrity	Repeatable	Managed

Create plan to reach desired maturity

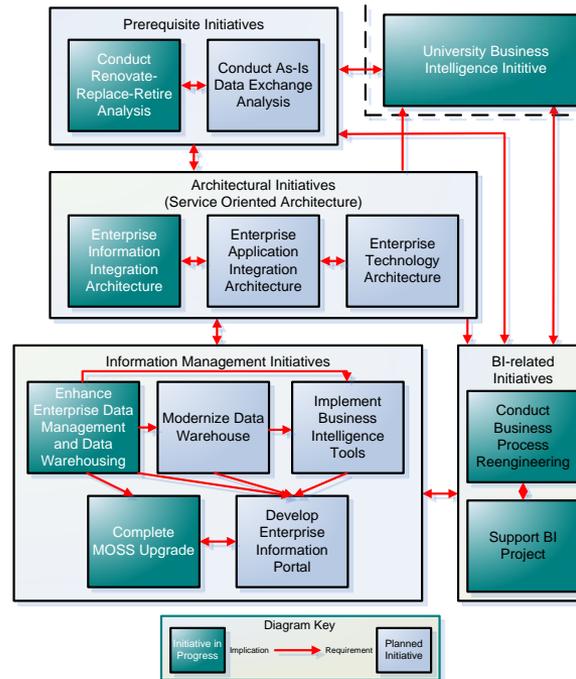
A number of factors will influence the maturity plan



Include narratives and roadmaps in plans

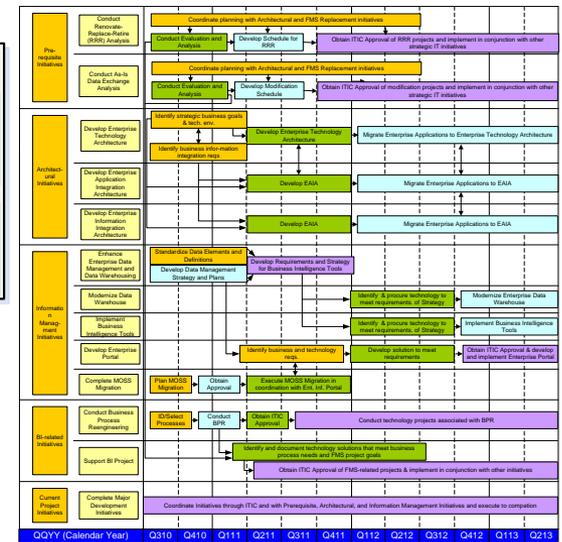
Conduct Renovate-Replace-Retire analysis of all VCU software applications to provide assurance their value is commensurate with associated support efforts and costs.	
Short Title	Conduct Renovate-Replace-Retire Analysis
Definition	Identify all currently-supported VCU software applications, evaluate the status of the technology on which they are based and their strategic and/or tactical value to VCU.
University Strategic Goals Supported	University Efficiency
Related Strategic Initiatives	Develop Enterprise Information Integration Architecture Complete Strategic Transportation System Projects Support FMS Replacement Project Complete Strategic Transportation System Projects
Requirements	<ol style="list-style-type: none"> 1. Conducting this analysis requires detailed information regarding each application. 2. Requires understanding of enterprise architecture goals. 3. Conducting this analysis also requires information from users of each application regarding their reliance on and use of the application. 4. Depends on Business Process Reengineering work to identify process/technology changes in advance of renovation, replacement, or retirement.
Implications	<ol style="list-style-type: none"> 1. All VCU enterprise applications will be affected, potentially including applications under development. 2. Replacement, renovation, or retirement of each application could affect other applications. 3. Replacement and renovation of applications will require significant commitment of funding. 4. Planning the replacement, renovation, and retirement of applications subsequent to this analysis will require significant investment of VCU staff time for planning and execution.
Component Projects	<ol style="list-style-type: none"> 1. Coordinate planning with Enterprise Information Integration Architecture initiative. 2. Identify applications, develop evaluation criteria, and conduct evaluation, including evaluation of in-progress projects. 3. Develop renovation, replacement, retirement schedule in coordination with other VCU strategic IT initiatives. 4. Obtain approval for renovation, replacement, retirement projects and execute projects in coordination with other VCU strategic IT initiatives.
Scheduling Dependencies	1. Must be coordinated with Enterprise Information Integration Architecture initiative.
Estimated Savings or Costs	1. Estimated net savings of \$850,000 in maintenance costs for applications that will be retired.

Initiative Narrative



Initiative Relationship Map

Initiative Implementation Map



Document initiative narratives

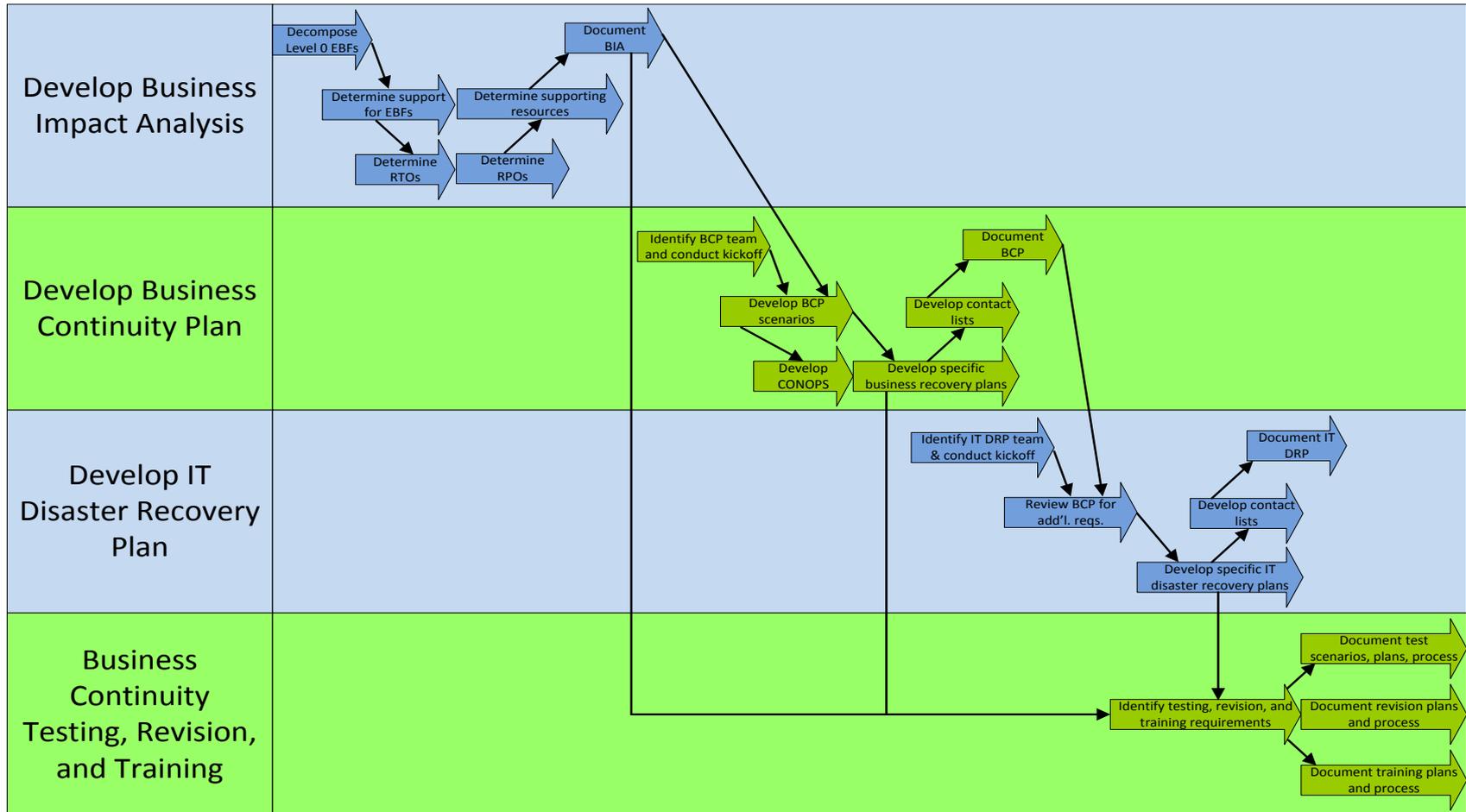
Using the list of Level 0 Essential Business Functions (EBFs) previously defined, develop a full Business Impact Analysis (BIA) that identifies business processes that support EBFs, delineates people, process, and technology resources that support these processes, and document requirements to recovery processes and supporting resources.

Short Title	Document Business Impact Analysis (BIA)
Definition	Identify and document all processes that support EBFs, people, process, and technology resources that support these processes, and requirements for their recovery in a disruption.
Requirements	<ol style="list-style-type: none">1. All CAI business continuity planning documentation completed to date will be required to support this initiative.
Implications	<ol style="list-style-type: none">1. The business continuity plan development initiative depends on this initiative to identify processes and supporting resources which require recovery.2. The business continuity plan development initiative depends on this initiative to identify recovery requirements in the form of recovery time objectives (RTOs) and recovery point objectives (RPOs).3. The testing, training, and revision initiative depends on this initiative as one of its inputs.
Component Activities	<ol style="list-style-type: none">1. Decompose Level 0 Essential Business Functions (EBFs) to constituent Level 1 and/or Level 2 business processes.2. Determine direct or indirect support for EBFs.3. Determine dependency among EBFs and supporting processes.4. Based on EBFs supported and dependency determine Recovery Time Objectives (RTOs) for business processes that support EBFs.5. Determine supporting resources (people, process, technology) for all business processes that support EBFs.6. Determine Recovery Point Objectives (RPOs) for processes that support EBFs.7. Document overall recovery requirements (people, process, technology, RTOs, RPOs) in BIA report.

Initiative narrative should include:

- Definition
- Requirements
- Downstream Implications
- Component activities

Reflect all initiatives in roadmaps



Roadmaps should reflect functional and schedule dependencies

We have templates to share!

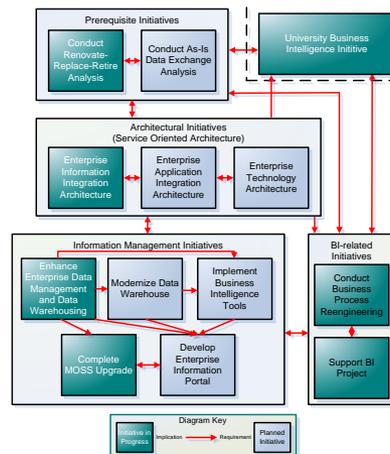
SEC501 Section Number	SEC501 Section Name	Applicable DGIF Policy Number(s)				
1	Introduction	3	14			
2	Information Security Roles and Responsibilities	3	4			
3	Business Impact Analysis	1				
4	IT System and Data Sensitivity Classification	14	17			
5	Sensitive IT System Inventory and Definition	11	17			
6	Risk Assessment	10	11			
7	IT Security Audits	13				
8.1	Access Control	14	15	22	23	25
8.2	Awareness and Training	2	26			
8.3	Audit and Accountability	13				
8.4	Security Assessment and Authorization	12				
8.5	Configuration Management	5	14			
8.6	Contingency Planning	6	25			
8.7	Identification and Authentication	7				
8.8	Incident Response	8				
8.9	Maintenance	20				
8.10	Media Protection	9	14	15		
8.11	Physical and Environmental Protection	23	24			
8.12	Planning	2	21			
8.13	Personnel Security	2	10			
8.14	Risk Assessment	11				
8.15	System and Services Acquisition	19	25			
8.16	System and Communications Protection	14	15	16	23	25
8.17	System and Information Integrity	18	23	25		

Governance	<i>Vision, Mission, & Values</i>	Current
		Target
	<i>Board Maturity & Compliance</i>	Current
		Target
Management	<i>Staff Capacity & Capability</i>	Current
		Target
	<i>Plan, Processes & Technology</i>	Current
		Target
Program Delivery & Impact	<i>Program Outcomes</i>	Current
		Target
	<i>Alignment to Strategy & Mission</i>	Current
		Target
Relationships & Collaboration	<i>Program Effectiveness</i>	Current
		Target
	<i>Funding & Development</i>	Current
		Target
Finance	<i>Communications</i>	Current
		Target
	<i>Organizational Collaboration</i>	Current
		Target
Finance	<i>Strategic Finance</i>	Current
		Target
	<i>Financial Leadership</i>	Current
		Target
Finance	<i>Financial Management & Reporting</i>	Current
		Target

Maturity Model

SEC501 Mapping

Narratives and Roadmaps



... Etc.

Further Discussion



For More Information

Scott Hammer, Principal Consultant

Scott.Hammer@northhighland.com

(804) 306-9685

The North Highland Company
7275 Glen Forest Drive, Suite 208
Richmond, VA 23226

About North Highland

North Highland is a full-service global consulting firm

northhighland.
WORLDWIDE CONSULTING



FOUNDED
in 1992 by three consultants who wanted to revolutionize consulting



OFFICES
58 locations around the world

GLOBAL HEADQUARTERS
Atlanta

AFFILIATIONS



a global management consulting group

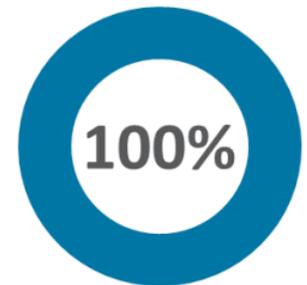
PROFESSIONALS

2,500+ Worldwide
1,000+ in the U.S.

Avg. 15+ yrs. Experience



PRIVATE FIRM
Employee owned



North Highland's Key Differentiators Help Us Drive Value For Clients

We are a smarter investment

- We guarantee our work
- 100% of our clients would recommend us
- Pragmatic, custom solutions that integrate well within your organization
- Proven record of producing great returns on our clients' investment
- Projects completed faster and with more measurable impact

We bring high caliber consultants

- We tackle clients' toughest, most complex business challenges
- We bring years of collective experience
- Our professional integrity instills trust over long-standing client relationships
- Global expertise – Over 50 offices worldwide
- Passionate about creating collaborative atmosphere

We're easy to work with

- We do the right thing for our client
- Clients love our collaborative, collegial style
- We simplify the complex
- Private, employee owned company that stresses team ownership and accountability to our clients
- Ensure knowledge transfers to clients and they own the solution

We're a catalyst for client success

- If clients are successful, we are successful
- We are highly responsive to client needs and help them achieve more with fewer resources
- We help clients deliver on promises they make to their management
- We help client teams broaden their skills and grow professionally

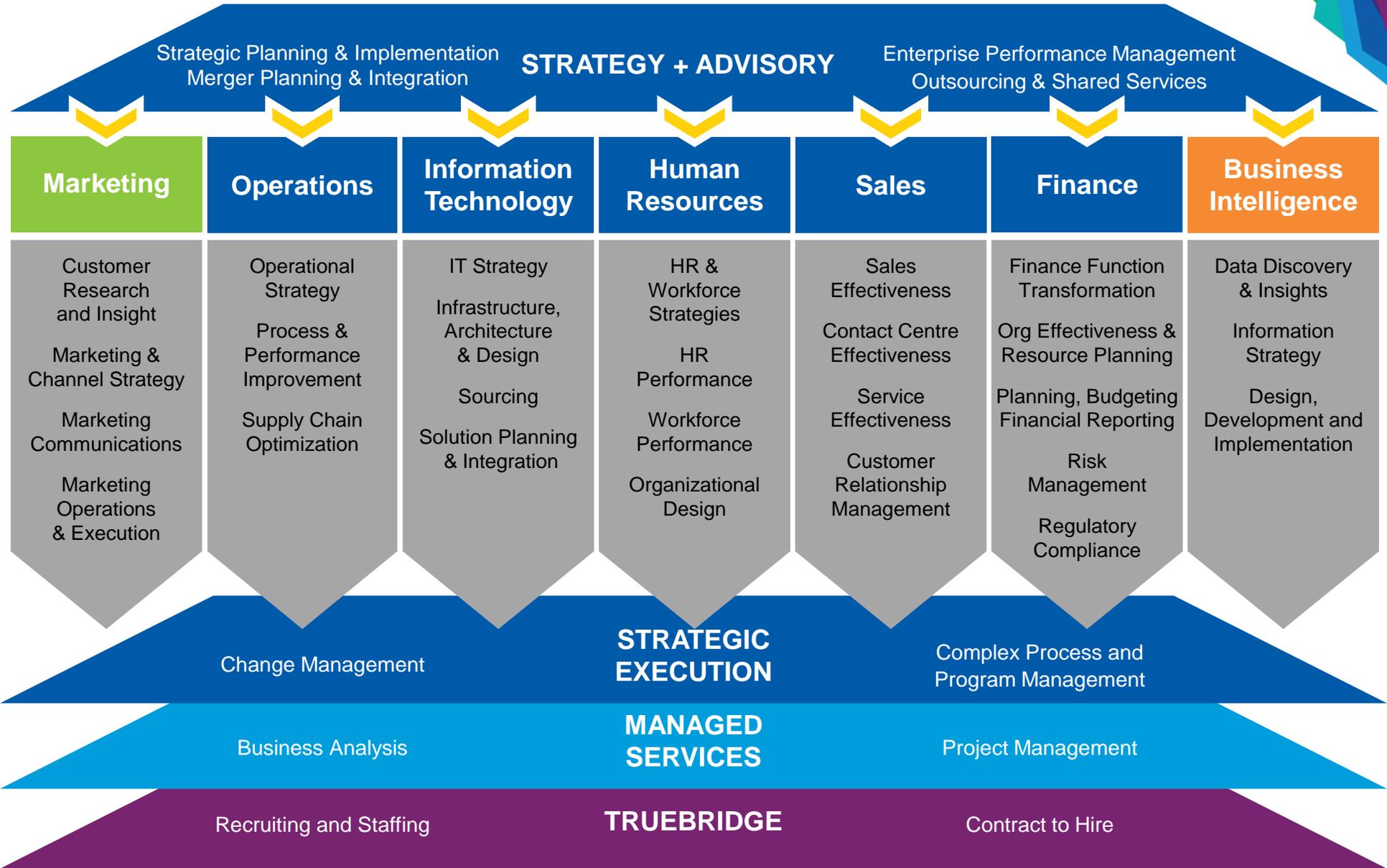
North Highland's Specialist Expertise

North Highland provides a growing portfolio of specialized expertise through individually branded divisions – organized into delivery models that align seamlessly to address the diverse business needs of our clients.



Each division shares the common culture and values of North Highland and works together in an integrated “one team” approach to make it easy for our clients to engage services across different lines of business

North Highland Offerings By Functional Area



Who Is North Highland?

We're a different kind of consulting firm

We have one simple premise – to do what's right for our clients and our people. After all, **relationships** matter.

That belief has guided us to become a global consulting firm that builds its success on the **value** we provide for our clients. We bring **BIG** ideas and **challenge** the expected way of doing things.

We want to change the way the world thinks about Consulting

– *not an easy task. But it's okay, we're ambitious.*

Some key facts about us

- **2,500+** professionals across the globe; over 1,100 in the U.S.
- Over **50** offices in the U.S., Europe and Asia-Pacific
- Our global headquarters are in **Atlanta** in the U.S
- We are a **employee-owned**, private company
- We are also one of the top **four** firms in the world on *Consulting Magazine's* list of Best Firms to Work For: 2007, 2008, 2009, 2010, 2011, 2012, & 2013

Who Is North Highland?

We are a global consulting firm that has changed the model of how a consultancy serves its clients. **We guarantee our work**, hire top notch talent and work with some of the largest organizations in the world – to **achieve exceptional results**.

Headquarters

Atlanta, GA

Professionals

- 2,500 worldwide
- Average 15+ years consulting experience

Private company

100% employee owned

Best Firm to Work For

Ranked 3rd in Consulting Magazine's 2013 list of "Best Firms to Work For" – our seventh consecutive year in the top 4



50 offices in the U.S., Europe and Asia-Pacific