Regence

Deloitte & Touche

A Framework Approach to HIPAA Security Readiness

March 13, 2002

Why Use a Framework Approach?

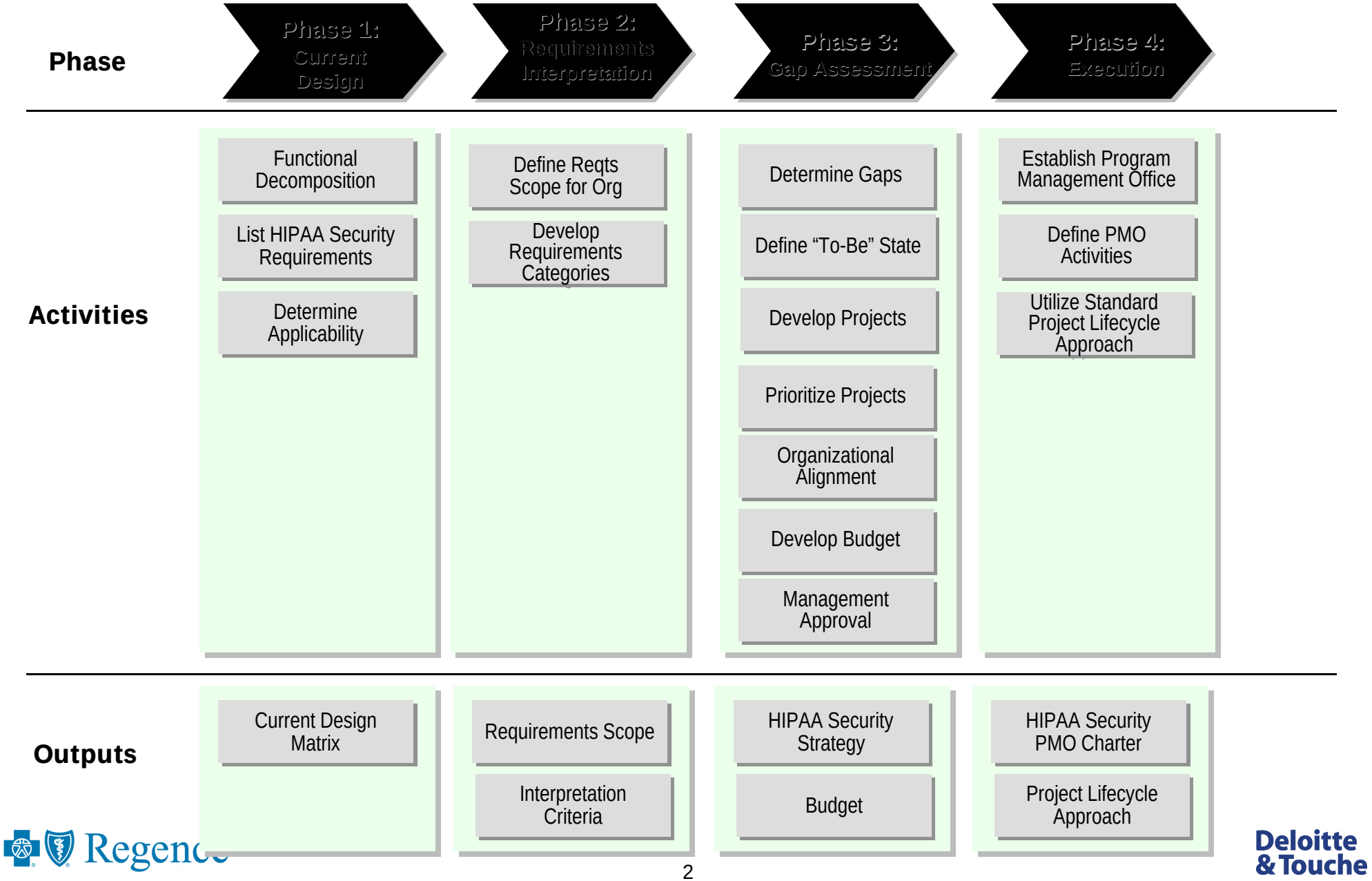
- HIPAA tells you “what to do”, but not “how to do it”, which means some level of interpretation of the requirements will be necessary by your organization. What makes sense for your organization?

- Organizations can have multiple sites, applications and processes. How do you determine what areas to assess for HIPAA security readiness? How do you decide what requirements will apply to what areas?

- Your HIPAA security readiness assessment is complete and you have a list of gaps. How do you take the gaps identified in the HIPAA readiness assessment and develop them into actionable projects to address those gaps?

- Typically, addressing HIPAA security readiness will mean executing a number of projects at the same time, which will be competing for sometimes the same resources. How do you effectively manage the execution of multiple projects?

HIPAA Security Readiness Framework - Overview



Phase 1: Current Design

Phase 1:
Current
Design

- Functional Decomposition
- List HIPAA Security Requirements
- Determine Applicability

Regence

Deloitte & Touche

Phase 1: Current Design - *Functional Decomposition*

"Framing Your Organization's Environment"

Sample Functional Areas	Examples
Processes	Membership and Enrollment; Claims Administration; Contract Management; Administration; Financial; Scheduling
Locations	Hospital; Outpatient Clinic; Off-site storage; Headquarters; Remote Sales office; Data Center
IT Environment	Wireless; WAN; LAN; Dial-up; WebServers; Workstations; Facilities; Databases
Applications	Laboratory; Radiology; Pharmacy; Order Entry; Nurse Management; Financial; Enrollment; Billing & A/R; Provider Management; Sales Management
Strategic Initiatives	Integrating the Healthcare Enterprise (IHE); Electronic Medical Records; Web-Enabling Clinical Applications; Electronic Data Interchange (EDI); Customer Relationship Management (CRM)

Phase 1: Current Design - *List HIPAA Security Requirements*

HIPAA Security Requirements

- Administrative Procedures
- Physical Safeguards
- Technical Security Services
- Technical Security Mechanisms
- Electronic Signatures

HIPAA Security Requirements			
Administrative Procedures	***.308(a)(1)***	Certification	
	.308(a)(2)	Chain of Trust Partner Agreement	
	.308(a)(3)	Contingency Plan	Applications and data criticality analysis
			Data backup plan
			Disaster recovery plan
			Emergency mode operation plan
			Testing and revision
	.308(a)(4)	Formal Mechanism for Processing Records	
	.308(a)(5)	Information Access Control	Access authorization
			Access establishment
			Access modification

Phase 1: Current Design – *Determine Applicability*

- **HIPAA Security Requirements mapped against your environment**
- **Using the HIPAA security requirements, determine "First Cut" applicability to narrow assessment focus – X**
- **Phase 2 will define what the X means**

Current Design Matrix

HIPAA Security Requirements				Processes				Locations			Applications			IT Environment		
				Claims / Encounters	Customer Service	Membership	Claims	Data Center	Headquarters	Remote Sales Office	Claims	Sales Management	Enrollment	Internet	WAN	LAN
Administrative Procedures	*.308(a)(1)*	Certification									X	X	X	X	X	X
	.308(a)(2)	Chain of Trust Partner Agreement					X									
	.308(a)(3)	Contingency Plan	Applications and data criticality analysis					X	X	X	X	X	X	X	X	X
			Data backup plan	X	X	X	X				X	X	X			X
			Disaster recovery plan					X	X	X	X					
			Emergency mode operation plan	X	X	X	X	X	X	X						
			Testing and revision	X	X	X	X	X	X	X	X	X	X			X
	.308(a)(4)	Formal Mechanism for Processing Records		X	X	X	X				X	X	X			
	.308(a)(5)	Information Access Control	Access authorization								X	X	X	X	X	X
			Access establishment								X	X	X	X	X	X
			Access modification								X	X	X	X	X	X

Phase 2: Requirements Interpretation

Phase 2:
Requirements
Interpretation

- Define Reqts Scope for Org
- Develop Requirements Categories

Phase 2: Requirements Interpretation

"Focus on the Current Design Matrix Cell"
What does the X mean?

HIPAA Security Requirements				Processes				Locations			Applications			IT Environment		
				Claims / Encounters	Customer Service	Membership	Claims	Data Center	Headquarters	Remote Sales Office	Claims	Sales Management	Enrollment	Internet	WAN	LAN
Administrative Procedures	*.308(a)(1)*	Certification									X	X	X	X	X	X
	.308(a)(2)	Chain of Trust Partner Agreement					X									
	.308(a)(3)	Contingency Plan	Applications and data criticality analysis					X	X	X	X	X	X	X	X	X
			Data backup plan	X	X	X	X				X	X	X			X
			Disaster recovery plan					X	X	X	X					
			Emergency mode operation plan	X	X	X	X	X	X	X						
			Testing and revision	X	X	X	X	X	X	X	X	X	X			X
	.308(a)(4)	Formal Mechanism for Processing Records		X	X	X	X				X	X	X			
	.308(a)(5)	Information Access Control	Access authorization								X	X	X	X	X	X
			Access establishment								X	X	X	X	X	X
			Access modification								X	X	X	X	X	X

Phase 2: Requirements Interpretation – *Develop Reqt's Categories*

" Start with Generally Accepted Security Practices"

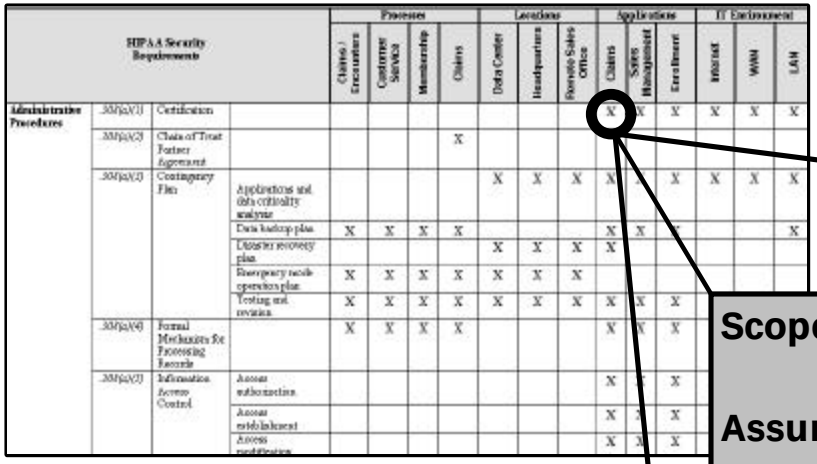
"Generally Accepted Practices"

- NIST
- ISO17799
- HCFA
- SANS
- I4

HIPAA Security Requirements				Processes				Locations			Applications			IT Environment		
				Claims / Encounters	Customer Service	Membership	Claims	Data Center	Headquarters	Remote Sales Office	Claims	Sales Management	Enrollment	Internet	WAN	LAN
Administrative Procedures	*.308(a)(1)*	Certification									X	X	X	X	X	X
	.308(a)(2)	Chain of Trust Partner Agreement					X									
	.308(a)(3)	Contingency Plan	Applications and data criticality analysis					X	X	X	X	X	X	X	X	X
			Data backup plan	X	X	X	X				X	X	X			X
			Disaster recovery plan					X	X	X	X					
			Emergency mode operation plan	X	X	X	X	X	X	X						
			Testing and revision	X	X	X	X	X	X	X	X	X	X			X
	.308(a)(4)	Formal Mechanism for Processing Records		X	X	X	X				X	X	X			
	.308(a)(5)	Information Access Control	Access authorization								X	X	X	X	X	X
			Access establishment								X	X	X	X	X	X
			Access modification								X	X	X	X	X	X

Phase 2: Requirements Interpretation – *Define Requirements Scope*

" Claims System Certification Example"



HIPAA Security Requirements				Processes				Locations			Applications			IT Environment		
				Claims / Encounters	Customer Service	Membership	Claims	Data Center	Headquarters	Roanoke Sales Office	Claims	Sales Management	Enrollment	Internet	WAN	LAN
Administrative Procedures	308(a)(1)	Certification									X	X	X	X	X	X
	308(a)(2)	Chain of Trust Partner Agreement					X									
	308(a)(3)	Contingency Plan	Applications and data criticality analysis					X	X	X	X		X	X	X	X
			Data backup plan	X	X	X	X				X	X	X			X
			Disaster recovery plan					X	X	X	X					
			Emergency mode operation plan	X	X	X	X	X	X	X						
			Testing and revision	X	X	X	X	X	X	X	X	X	X			
	308(a)(4)	Formal Mechanism for Processing Records		X	X	X	X				X	X	X			
	308(a)(5)	Information Access Control	Access authorization								X		X			
			Access establishment								X	X	X			
			Access modification								X	X	X			

- **Define the scope and criteria using generally accepted practices**
- **Assumptions will document your decisions and will help guide you over time as you come back to the matrix in the future**

Scope: Certification requirement will apply to claims systems

Assumptions: Will not apply to systems that will be replaced in less than 2 years

Categories:

Policy/Standards:

Procedures:

Tools/Infrastructure:

Operational:

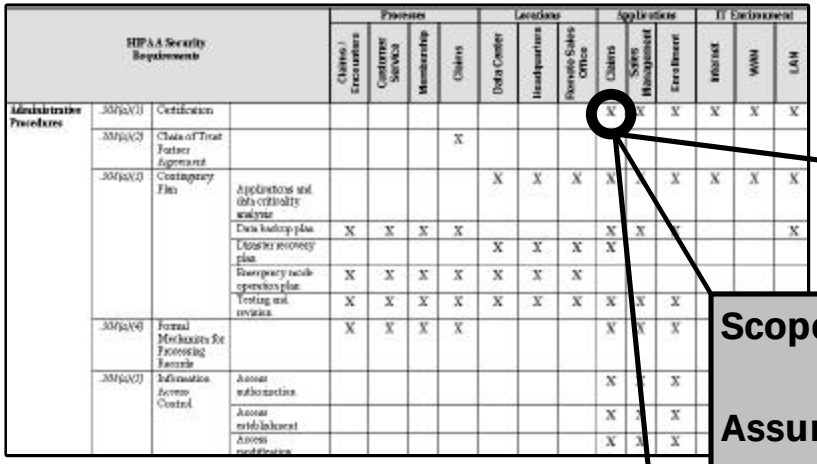
Phase 2: Requirements Interpretation – *Develop Reqt's Categories*

"Logical Means of Grouping the Criteria to Measure Progress"

Category	Description
Policies and Standards	Policies include senior management's directives to create a computer security function, establish goals for the function, and assign responsibilities for the function. Standards include specific security rules for particular information systems and practices
Procedures	Procedures include the activities and tasks that dictate how the policies or supporting standards will be implemented in the organization's environment
Tools / Infrastructure	Tools or infrastructure include the elements that are necessary to support implementation of the requirements within the organization such as process, organizational structure, network and system related controls, and logging and monitoring devices
Operational	Operational includes all the activities and supporting processes associated with maintaining the solution or system and ensuring it is running as intended. Typically, an owner is assigned to manage the execution of the activities and supporting processes. Examples of activities and supporting processes include maintenance, configuration management, technical documentation, backups, software support and user support

Phase 2: Requirements Interpretation – *Develop Reqt's Categories*

" Claims System Certification Example Continued"



HIPAA Security Requirements				Processes				Locations			Applications			IT Environment		
				Claims / Encounters	Customer Service	Membership	Claims	Data Center	Headquarters	Remote Sales Office	Claims	Sales Management	Enrollment	Internet	WAN	LAN
Administrative Procedures	308(a)(1)	Certification									X	X	X	X	X	X
	308(a)(2)	Chain of Trust Partner Agreement					X									
	308(a)(3)	Contingency Plan	Applications and data criticality analysis					X	X	X	X		X	X	X	X
			Data backup plan	X	X	X	X				X	X	X			X
			Disaster recovery plan					X	X	X	X					
			Emergency mode operation plan	X	X	X	X	X	X	X						
			Testing and revision	X	X	X	X	X	X	X	X	X	X			
	308(a)(4)	Formal Mechanism for Processing Records		X	X	X	X				X	X	X			
	308(a)(5)	Information Access Control	Access authorization								X		X			
			Access establishment								X	X	X			
			Access modification								X	X	X			

- **Documents your organization's interpretation of the HIPAA security requirements**
- **Measurement for progress towards HIPAA security Readiness**
- **Documents your organization's baseline, since the criteria will also change over time – "Living" Document**

Scope: Certification requirement will apply to claims systems

Assumptions: Will not apply to systems that will be replaced in less than 2 years

Categories:

Policy/Standards:
1) Written policy that identifies certification requirements
2) Policy identifies individuals responsible for implementing that policy and what their duties are
3) Policy identifies consequences of non compliance
4) Security Standards for the configuration of networks, security services and mechanism, systems, applications, databases, and middleware

Procedures:
1) Identifying certification need review
2) Pre-certification review
3) Certification readiness
4)Periodic Re-certification review

Tools/Infrastructure:
1) Pre-certification readiness tool
2) Certification criteria tool (standards)
3) Certification compliance issue resolution tool

Operational:
1) Operational when the following criteria are established: Owner, Budget, Charter & Certification Plan

Regence

Deloitte & Touche

Phase 3: Gap Assessment

Phase 3:
Gap Assessment

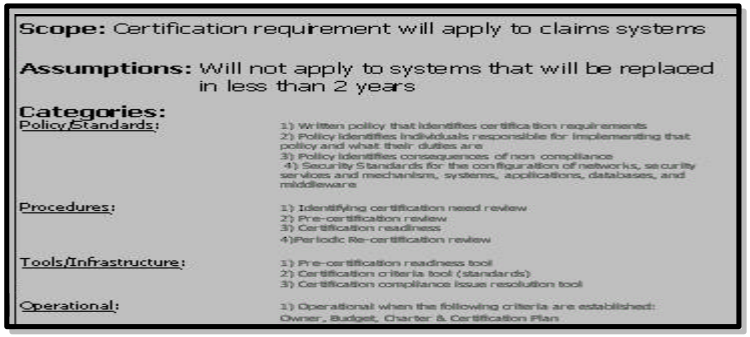
- Determine Gaps
- Define “To-Be” State
- Develop Projects
- Prioritize Projects
- Organizational Alignment
- Develop Budget
- Management Approval

Phase 3: Gap Assessment – *Determine Gaps*

“ Avoid the Road to Abilene by Getting Organizational Alignment ”

Current State

+



Scope: Certification requirement will apply to claims systems

Assumptions: Will not apply to systems that will be replaced in less than 2 years

Categories:

Policy/Standards:
1) Written policy that identifies certification requirements
2) Policy identifies individuals responsible for implementing that policy and what their duties are
3) Policy identifies consequences of non compliance
4) Security Standards for the configuration of networks, security services and mechanism, systems, applications, databases, and middleware

Procedures:
1) Identifying certification need review
2) Pre-certification review
3) Certification readiness
4)Periodic Re-certification review

Tools/Infrastructure:
1) Pre-certification readiness tool
2) Certification criteria tool (standards)
3) Certification compliance issue resolution tool

Operational:
1) Operational when the following criteria are established: Owner, Budget, Charter & Certification Plan

- **Use the HIPAA Security Criteria(*Phase 2*) to assess organization’s current state**

HIPAA Gap Analysis

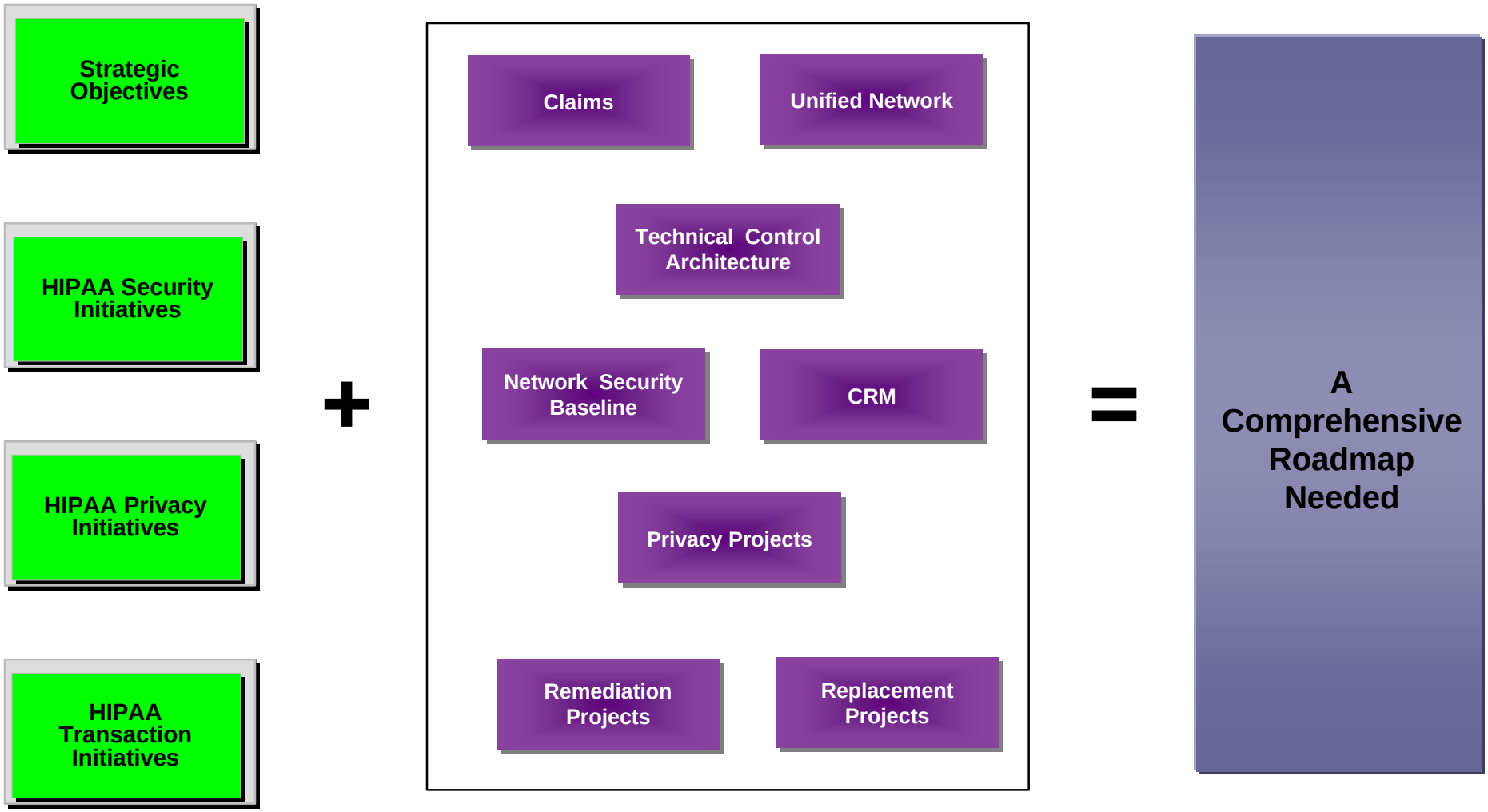
- **Determine gaps from the current state requirements**

Regence

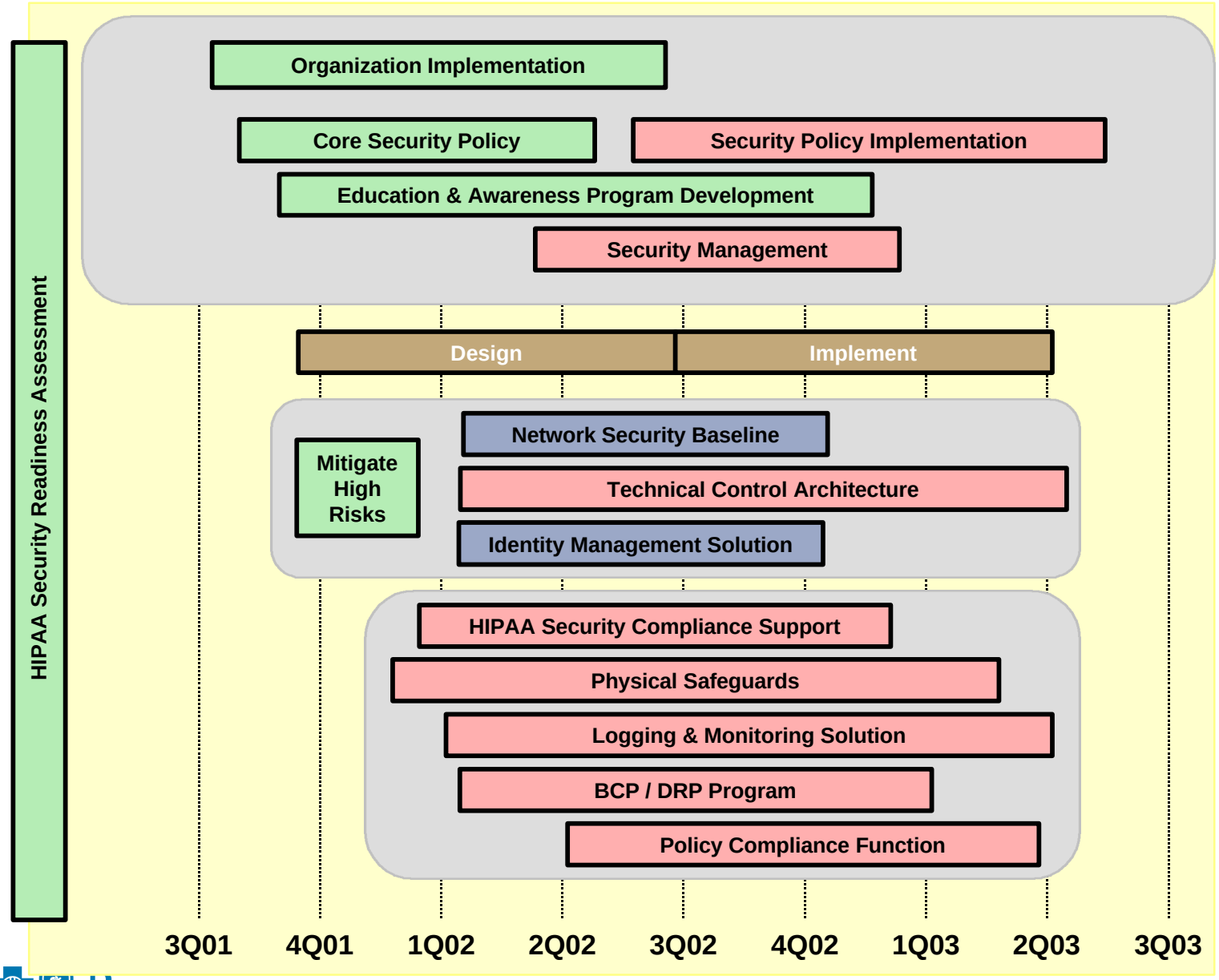
Deloitte & Touche

Phase 3: Gap Assessment – *Define "To-Be" State*

" HIPAA + To-Be State = Projects "



Phase 3: Gap Assessment – *Define Projects and Prioritized*



- **Develop projects based on gaps with the selected criteria**
- **Develop a budget for each of the projects and the overall effort**

LEGEND:

- Complete
- On-Going
- Not Started
- In Process

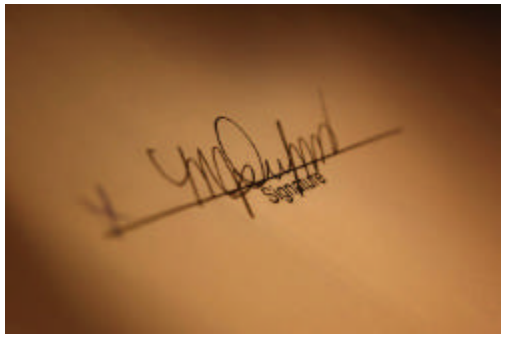
Regence

Deloitte & Touche

Phase 3: Gap Assessment – *Alignment, Budget and Approval*

Gain organizational alignment around projects and schedule

Develop budget estimates for each project in terms of people, hardware and software



Obtain management approval and execute projects

Phase 4: Execution

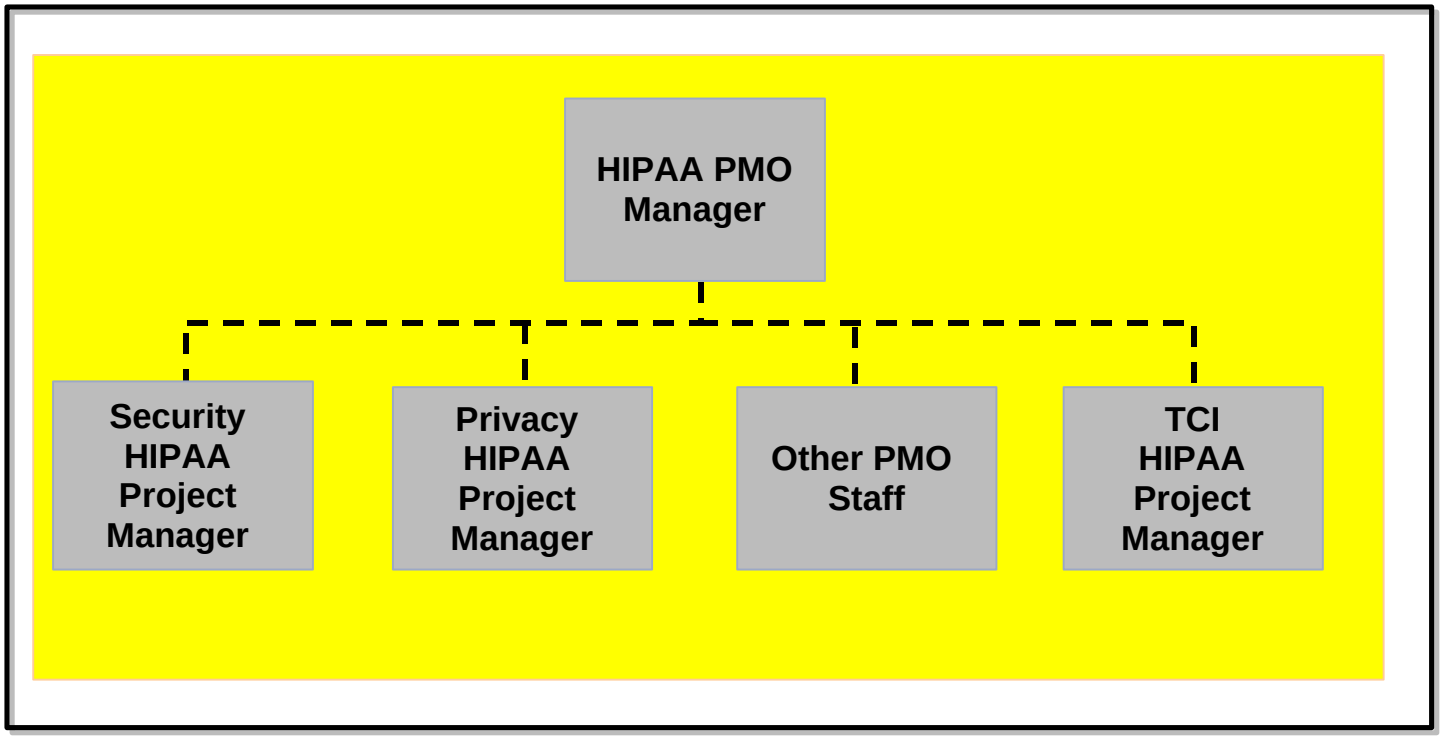
Phase 4:
Execution

- Establish Program Management Office
- Define PMO Activities
- Utilize Standard Project Lifecycle Approach

Phase 4: Execution - *Establish PMO*

" HIPAA Security Readiness is ***NOT*** an IT Project "

- Establish priorities
- Manage both organization and internal HIPAA dependencies
- Resolve project issues



Phase 4: Execution – *Define PMO Activities*

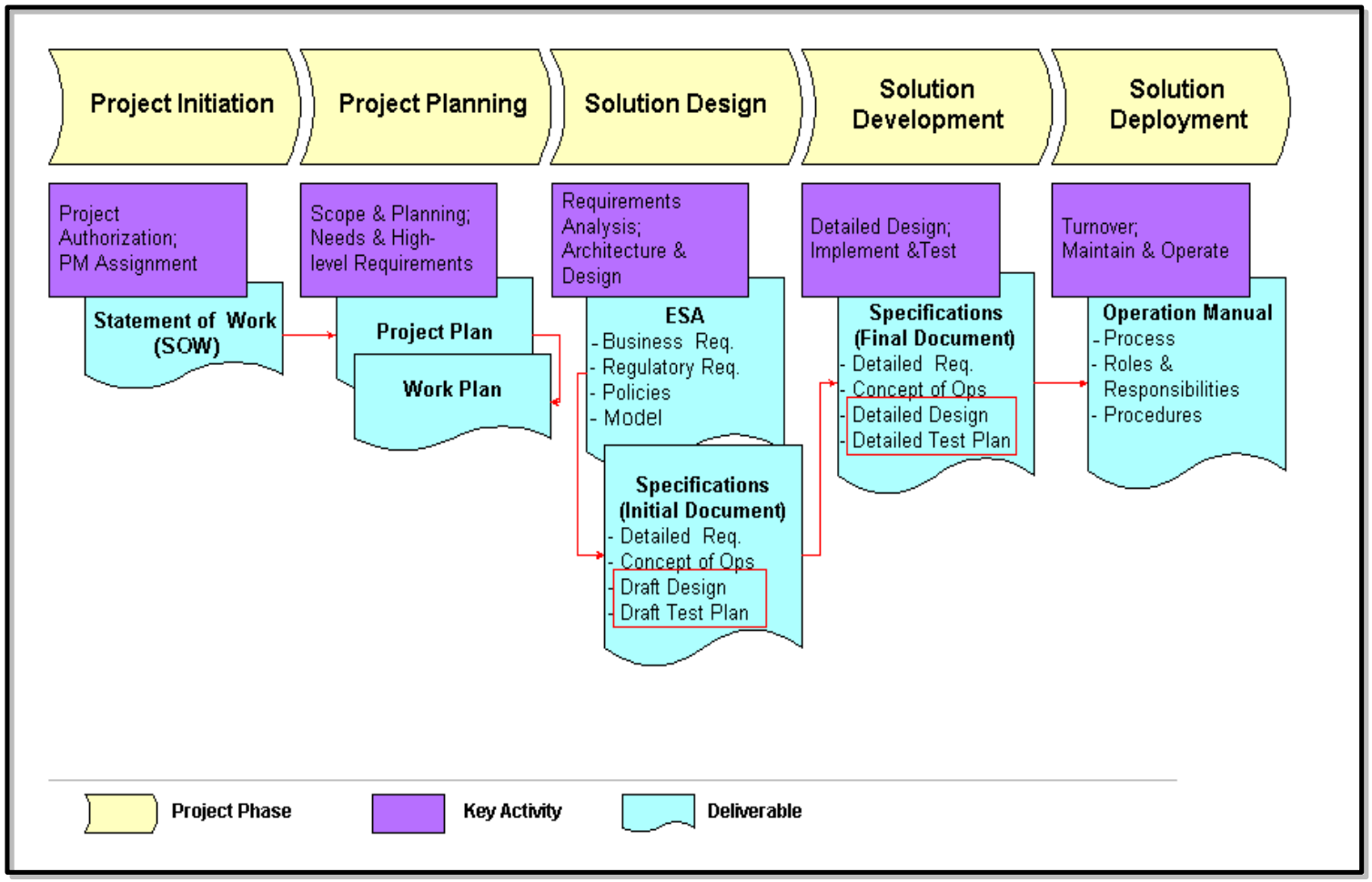
"Keeping Activities and Projects on Track"

Activities	Description
Provide Oversight for Multiple Projects	Prioritize projects, manage project interdependencies and corresponding critical path items
Manage the Allocation of Resources	"De-conflict" resource constraints and shortages resulting from multiple project demands
Manage Budget	Manage the budget for the HIPAA related projects
Resolve Issues	Facilitate resolution of issues both within projects and between cross-organizational departments
Report Status	Provide status reports on a periodic basis to oversight committees and management to report on the progress, issues and challenges of the overall program

Phase 4: Execution - *Utilize Standard Project Lifecycle*

"Consistent, High-Quality Standards Among Different Projects"

- **Streamline design and implementation activities**
- **Support standard set of project documentation**



Summary – “Three Notable Truths”

#1 Develop your security strategy and stay committed to it over time – HIPAA security readiness is a marathon not a sprint

#2 Security = 99% process and 1% technology – if you cannot operationalize security, all you have is an “expensive” science project that will most likely provide partial effectiveness

#3 Develop and maintain active executive-level participation and governance - Security is a “cross-organizational” issue and lack of organizational buy-in can kill a project