COBIT 5 and its use to leverage the business world

Ramsés Gallego
CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT(f), Six Sigma Black Belt
Security Strategist & Evangelist
ramses.gallego@quest.com

Research Director & Strategic Planning, ISACA Barcelona Chapter
International Vice President, ISACA Board of Directors
ramses.gallego@me.com
@ramsesgallego


FCB
JpegWallpapers.com


ISACA
Trust in, and value from, information systems
COBIT®
5
Implementation

implementation |ˌimpləmənˈtāSHən|

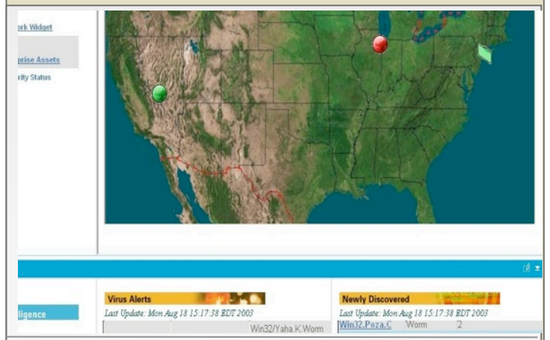
the process of putting a decision or plan into effect;

execution, to put into practical effect;

a means for achieving and end


Information
Tactics
Auditing
Trust
Strategy
Business
Technology
KPIs
Real-time
Dashboards
Efficiency
Metrics
Availability
Partners
Value
Accountability
Resiliency
KGIs
Access
Indicators
Governance
Effectiveness
Arquitecture
Management
Compliance
Integration
Identity
Risk

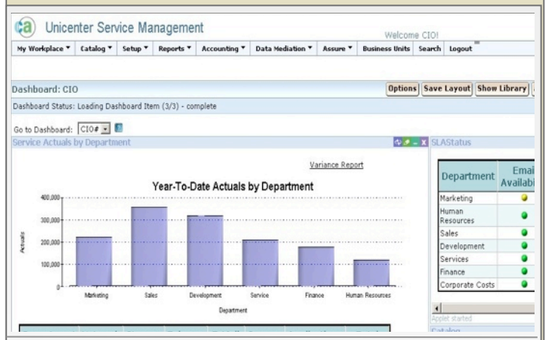
Manage risk



- Compliance
- Protect assets
- Business continuity

Manage operational and business risk

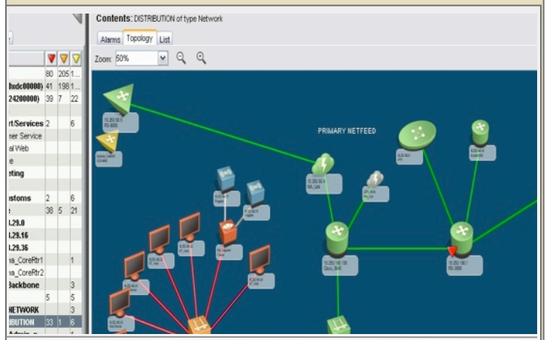
Manage cost



- Resource optimization
- Process automation

Better management of CAPEX and OPEX

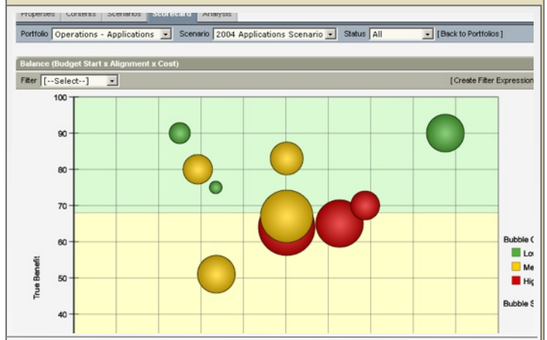
Improve service



- Service Availability
- Service Management

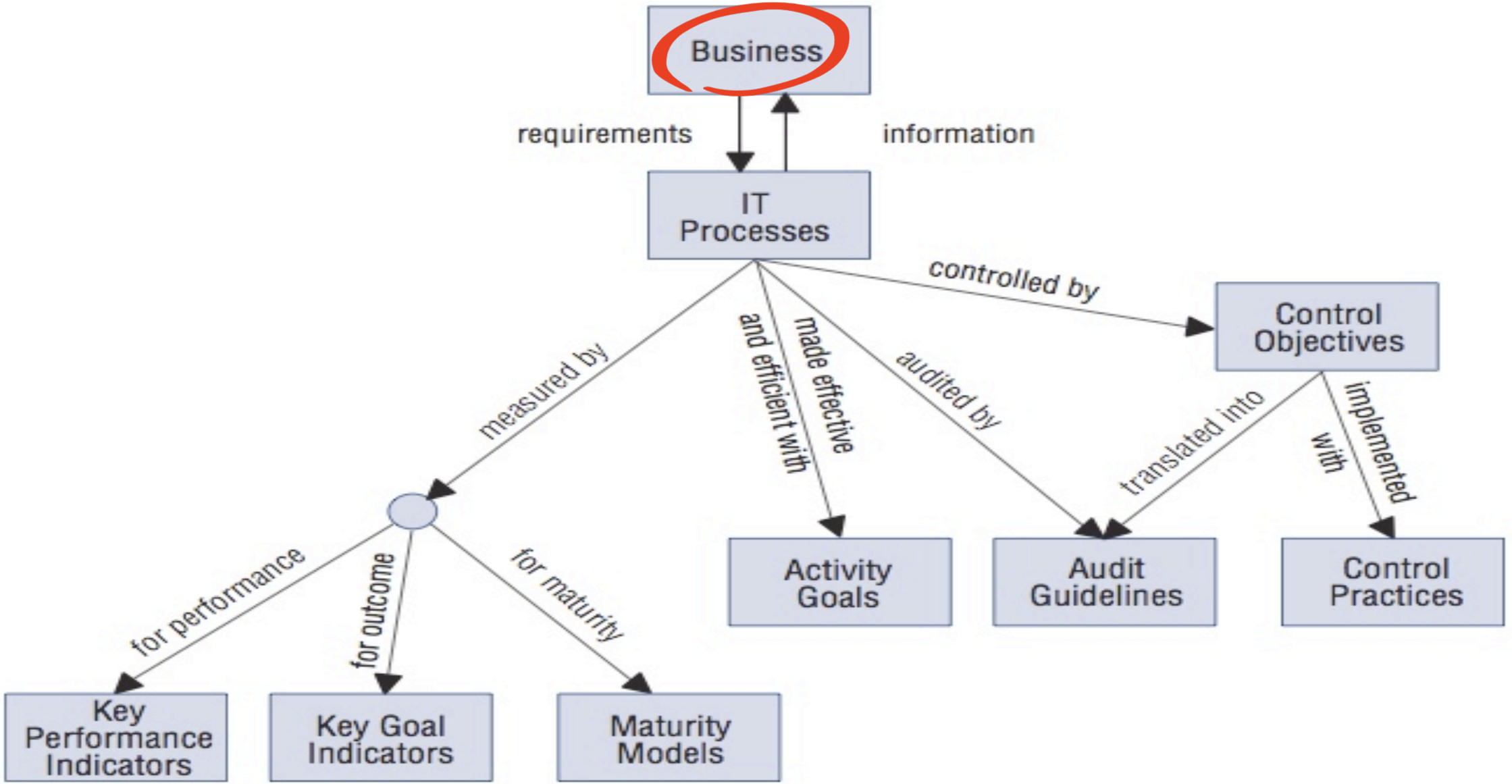
Optimal value providing effective and efficient services

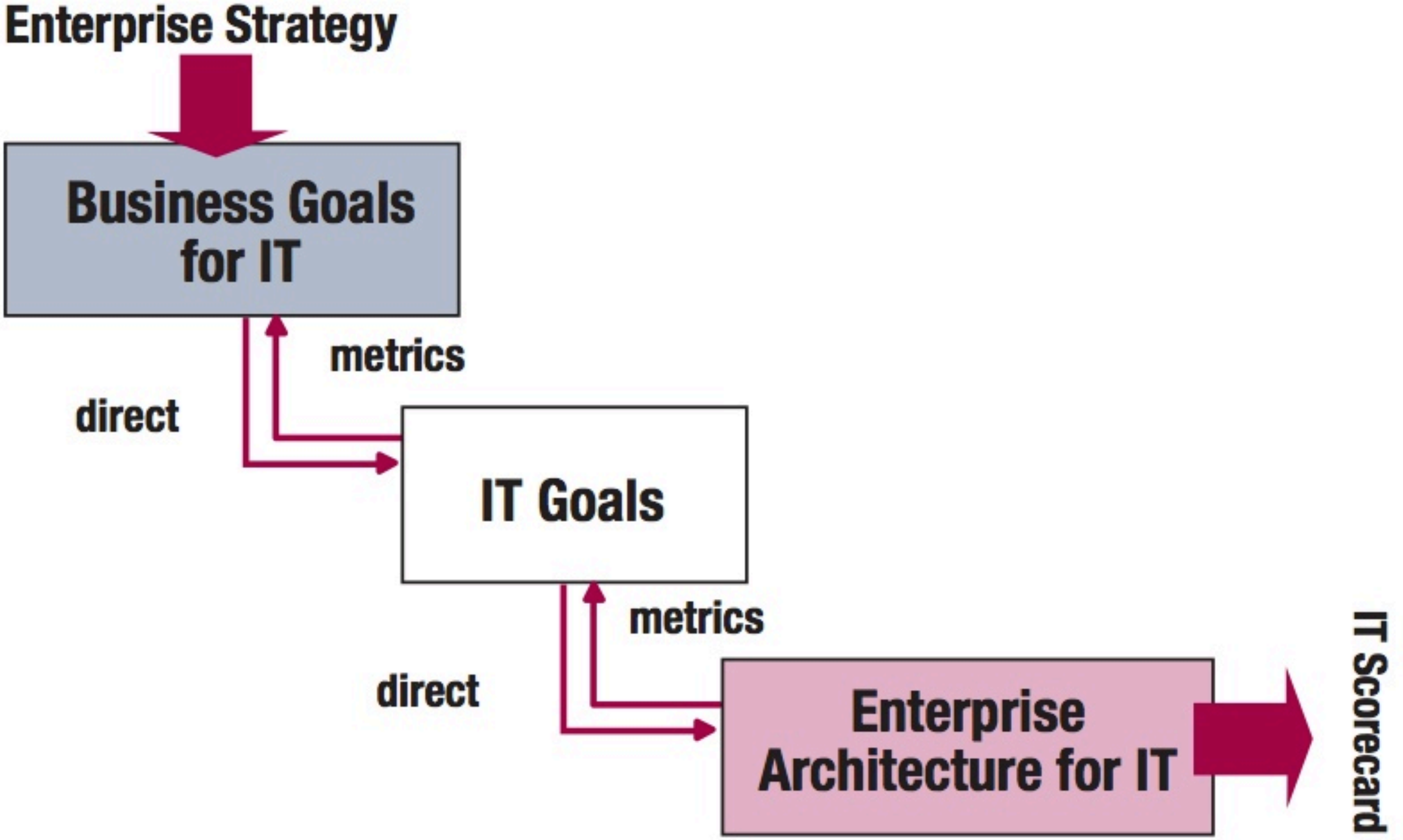
Align IT investments

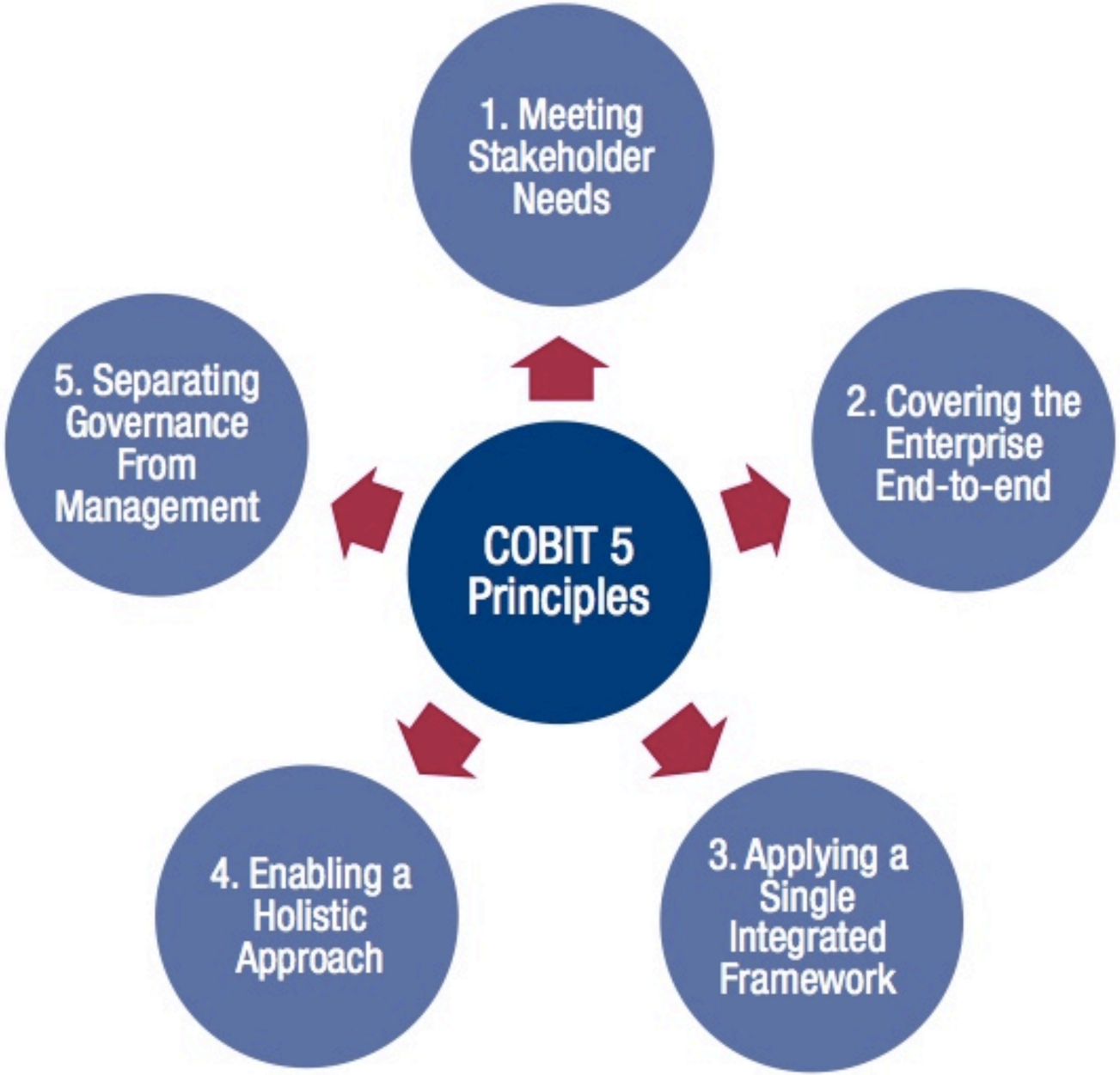


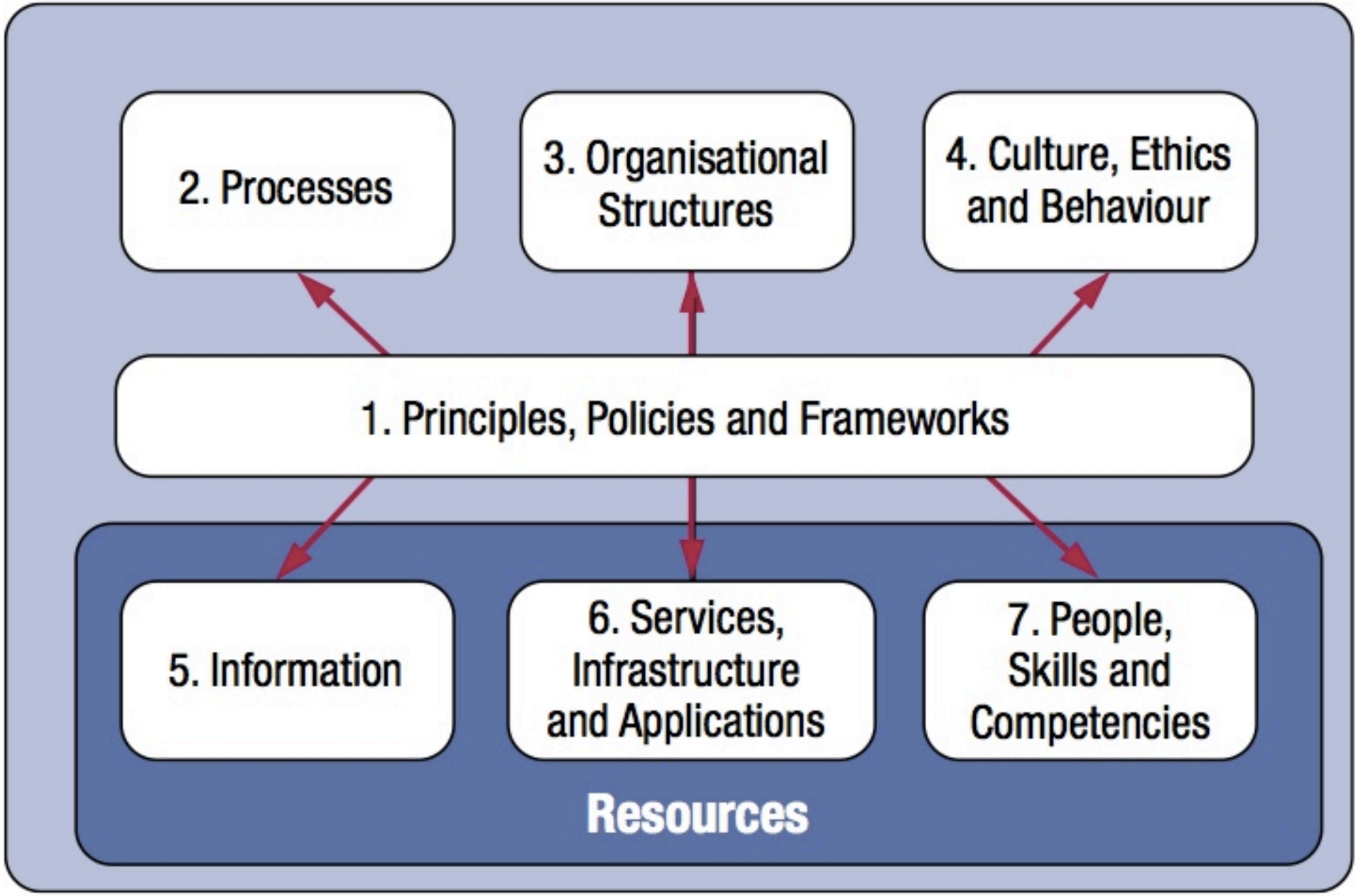
- IT Portfolio Management
- Value Management
- Business Process Management

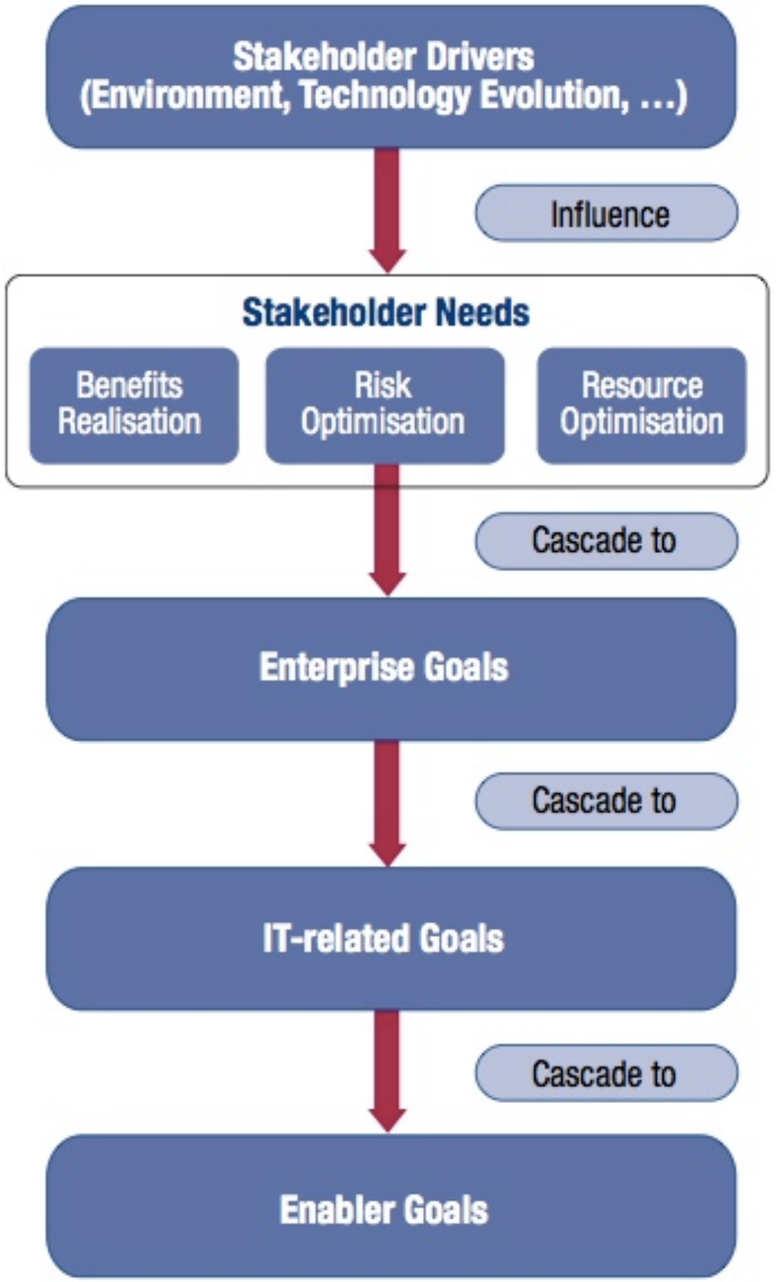
Align IT investments with the corporate goals

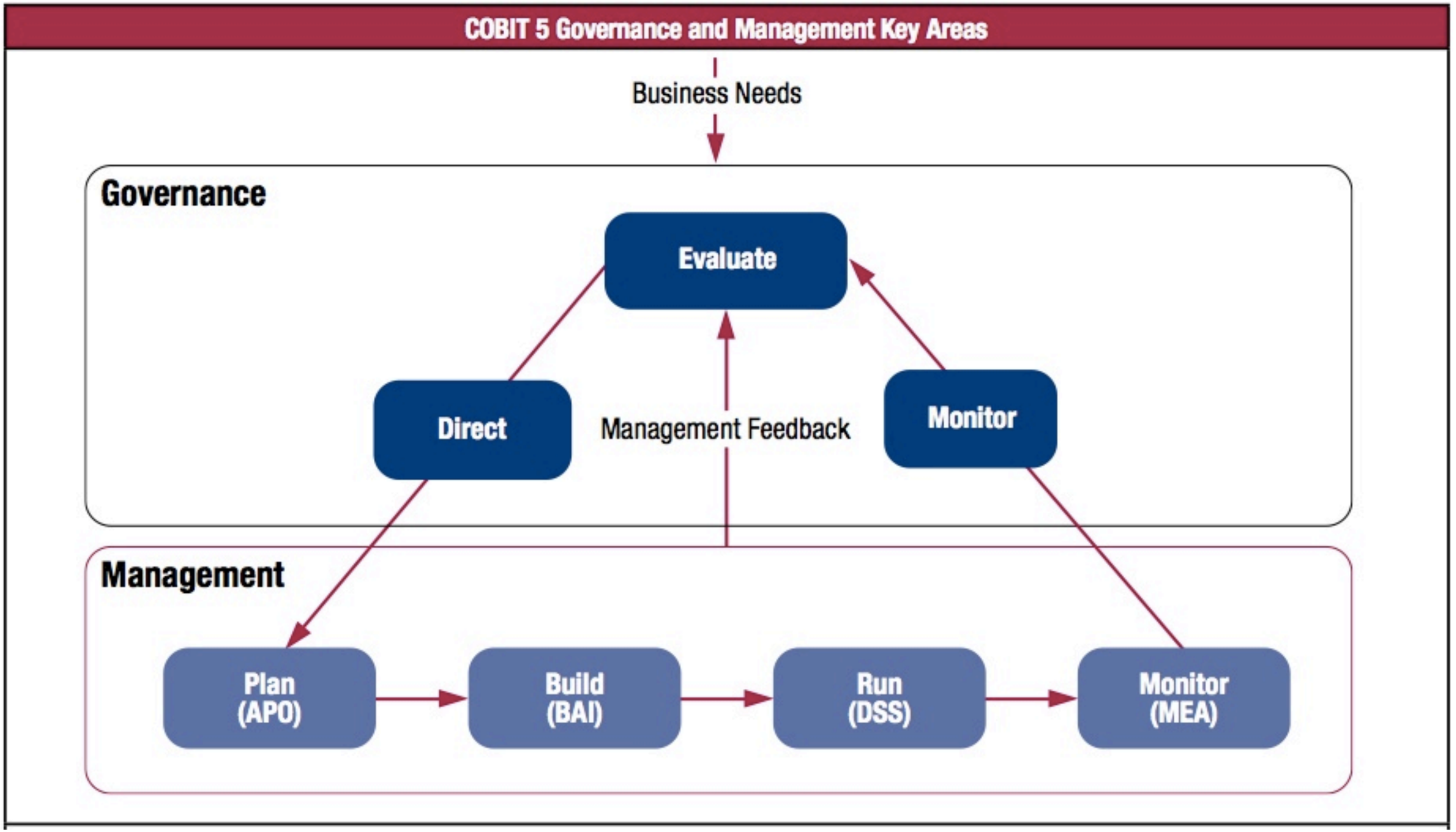

Business
requirements
information
IT Processes
controlled by
Control Objectives
measured by
made effective and efficient with
audited by
translated into
implemented with
for performance
for outcome
for maturity
Activity Goals
Audit Guidelines
Control Practices
Key Performance Indicators
Key Goal Indicators
Maturity Models


Enterprise Strategy
Business Goals for IT
metrics
direct
IT Goals
metrics
direct
Enterprise Architecture for IT
IT Scorecard

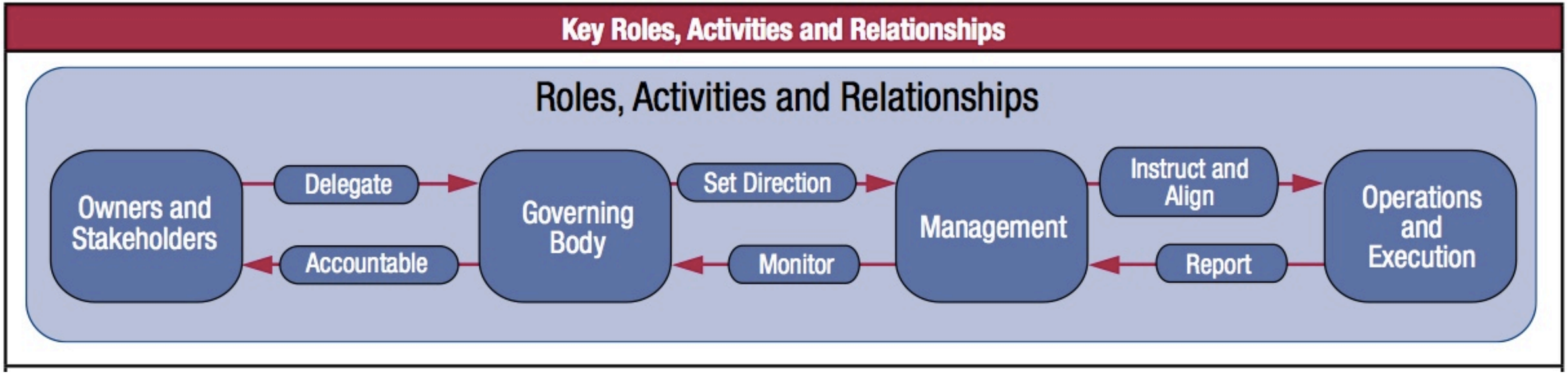


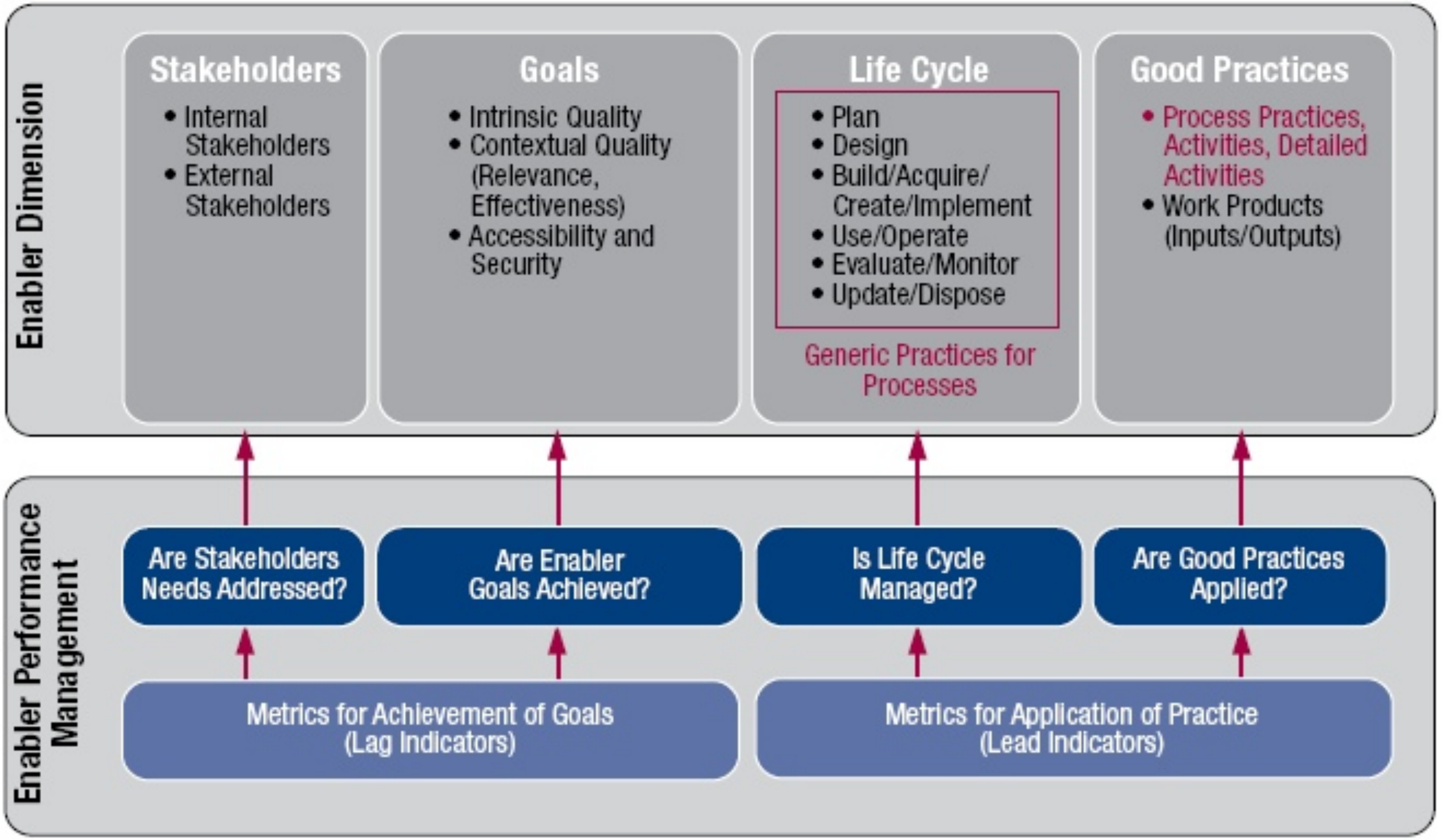


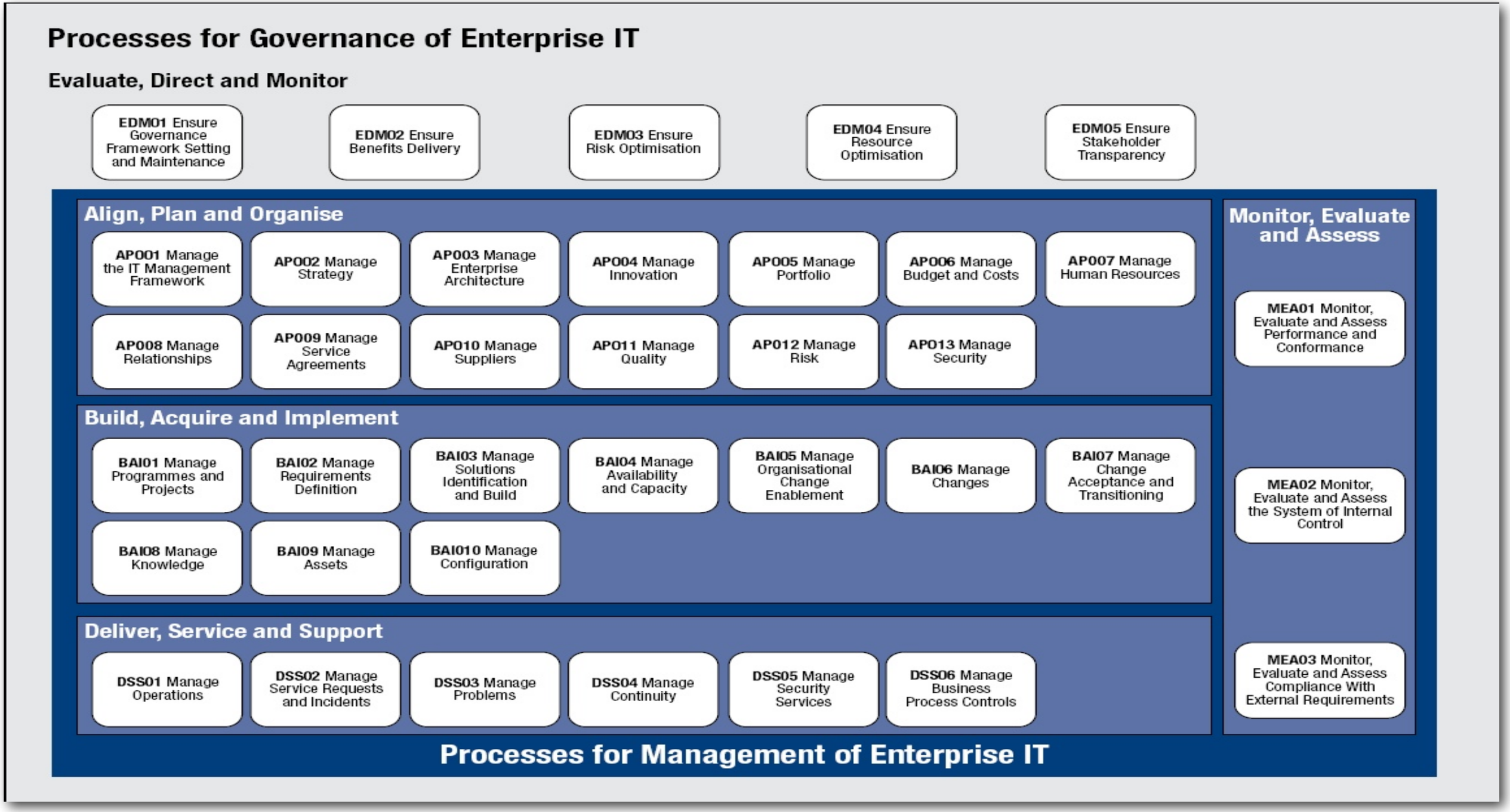




Key Roles, Activities and Relationships






Processes for Governance of Enterprise IT
Evaluate, Direct and Monitor
EDM01 Ensure Governance Framework Setting and Maintenance
EDM02 Ensure Benefits Delivery
EDM03 Ensure Risk Optimisation
EDM04 Ensure Resource Optimisation
EDM05 Ensure Stakeholder Transparency
Align, Plan and Organise
AP001 Manage the IT Management Framework
AP002 Manage Strategy
AP003 Manage Enterprise Architecture
AP004 Manage Innovation
AP005 Manage Portfolio
AP006 Manage Budget and Costs
AP007 Manage Human Resources
AP008 Manage Relationships
AP009 Manage Service Agreements
AP010 Manage Suppliers
AP011 Manage Quality
AP012 Manage Risk
AP013 Manage Security
Build, Acquire and Implement
BAI01 Manage Programmes and Projects
BAI02 Manage Requirements Definition
BAI03 Manage Solutions Identification and Build
BAI04 Manage Availability and Capacity
BAI05 Manage Organisational Change Enablement
BAI06 Manage Changes
BAI07 Manage Change Acceptance and Transitioning
BAI08 Manage Knowledge
BAI09 Manage Assets
BAI010 Manage Configuration
Deliver, Service and Support
DSS01 Manage Operations
DSS02 Manage Service Requests and Incidents
DSS03 Manage Problems
DSS04 Manage Continuity
DSS05 Manage Security Services
DSS06 Manage Business Process Controls
Monitor, Evaluate and Assess
MEA01 Monitor, Evaluate and Assess Performance and Conformance
MEA02 Monitor, Evaluate and Assess the System of Internal Control
MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
Processes for Management of Enterprise IT

RACI Chart

Functions

Activities

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Create and maintain a technology infrastructure plan.		I	I	A		C	R	C	C		C
Create and maintain technology standards.				A		C	R	C	I	I	I
Publish technology standards.		I	I	A		I	R	I	I	I	I
Monitor technology evolution.		I	I	A		C	R	C		C	C
Define (future) (strategic) use of new technology.		C	C	A		C	R	C		C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Align, Plan and Organise

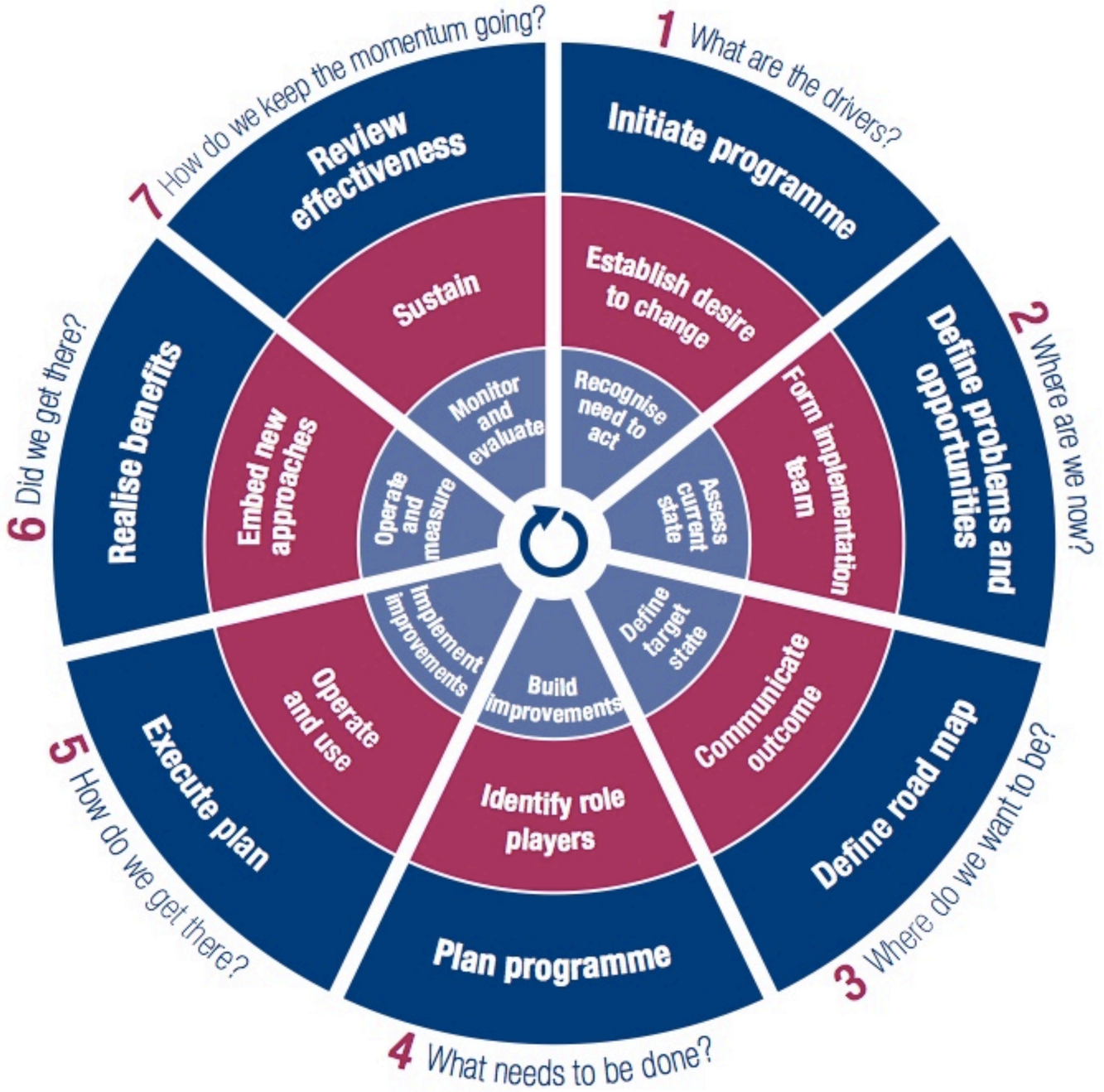
APO12 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO12.01 Collect data.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
APO12.02 Analyse risk.		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C
APO12.03 Maintain a risk profile.		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C
APO12.04 Articulate risk.		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C
APO12.05 Define a risk management action portfolio.		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C
APO12.06 Respond to risk.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R

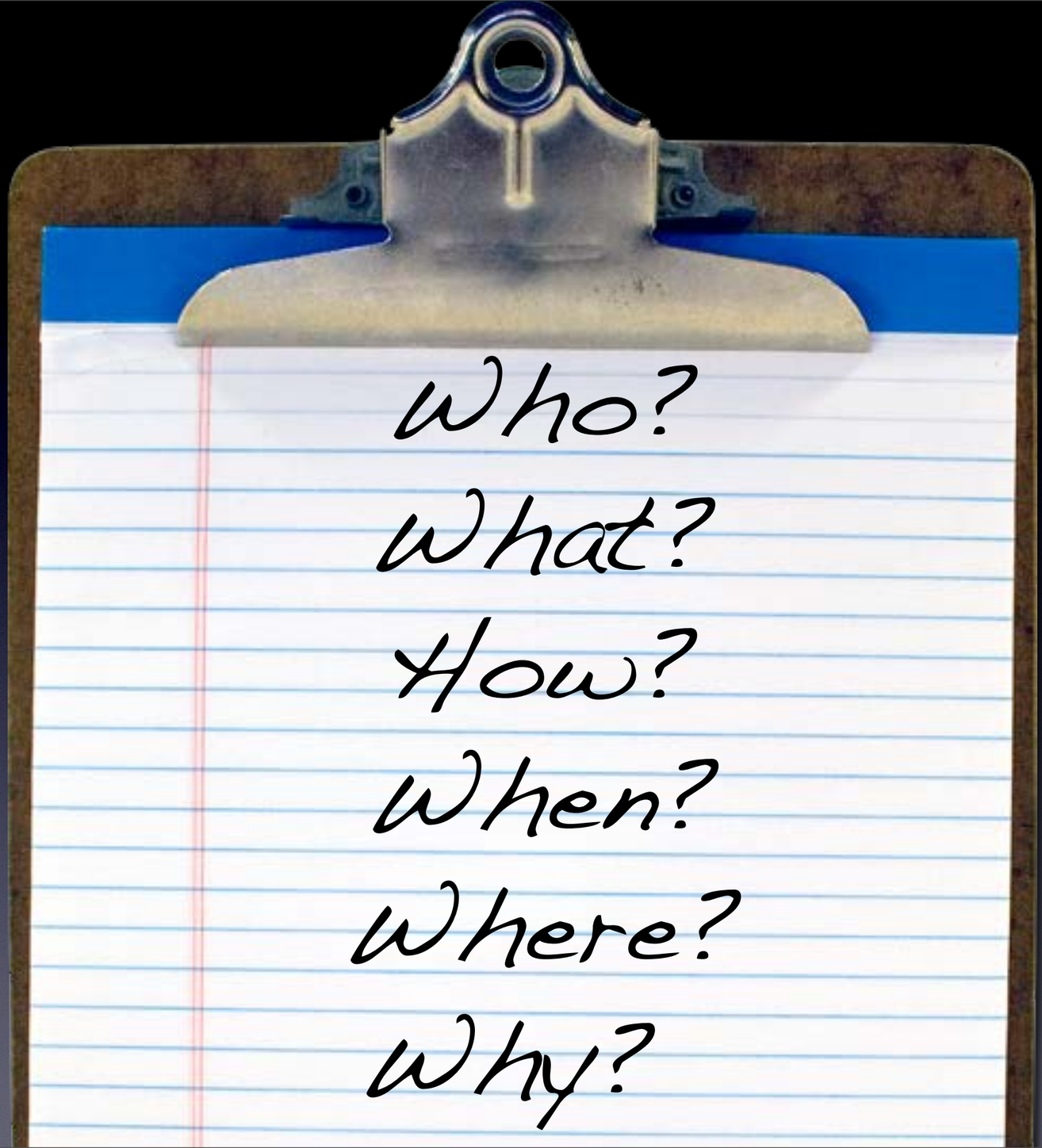
Figure 22—Mapping COBIT 5 Enterprise Goals to IT-related Goals

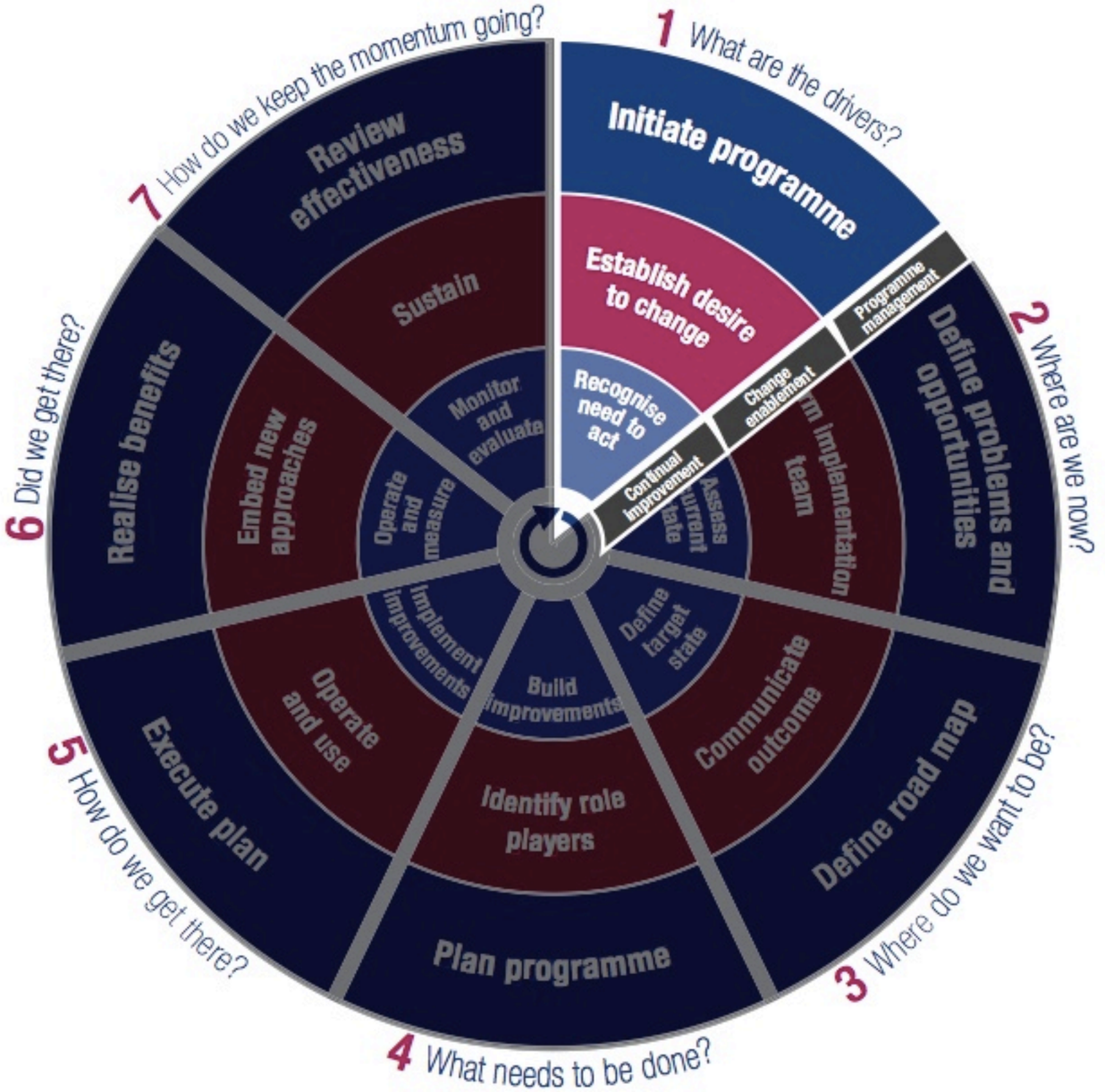
		IT-related Goal	Enterprise Goal																	
			Stakeholder value of business investments	Portfolio of competitive products and services	Managed business risk (safeguarding of assets)	Compliance with external laws and regulations	Financial transparency	Customer-oriented service culture	Business service continuity and availability	Agile responses to a changing business environment	Information-based strategic decision making	Optimisation of service delivery costs	Optimisation of business process functionality	Optimisation of business process costs	Managed business change programmes	Operational and staff productivity	Compliance with internal policies	Skilled and motivated people	Product and business innovation culture
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
			Financial					Customer					Internal					Learning and Growth	
Financial	01	Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	IT compliance and support for business compliance with external laws and regulations			S	P											P		
	03	Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
	04	Managed IT-related business risk			P	S			P	S		P			S		S	S	
	05	Realised benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
	06	Transparency of IT costs, benefits and risk	S		S		P				S	P		P					
Customer	07	Delivery of IT services in line with business requirements	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Adequate use of applications, information and technology solutions	S	S	S			S	S		S	S	P	S		P		S	S
	09	IT agility	S	P	S			S		P			P		S	S		S	P

EDM03 Process Practices, Inputs/Outputs and Activities				
Governance Practice	**Inputs**		**Outputs**	
EDM03.01 Evaluate risk management. Continually examine and make judgement on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risk to enterprise value related to the use of IT is identified and managed.	**From**	**Description**	**Description**	**To**
	AP012.01	Emerging risk issues and factors	Risk appetite guidance	AP012.03
			Approved risk tolerance levels	AP012.03
	Outside COBIT	Enterprise risk management principles	Evaluation of risk management activities	AP012.01
Activities				
1. Determine the level of IT-related risk that the enterprise is willing to take to meet its objectives (risk appetite).				
2. Evaluate and approve proposed IT risk tolerance thresholds against the enterprise's acceptable risk and opportunity levels.				
3. Determine the extent of alignment of the IT risk strategy to enterprise risk strategy.				
4. Proactively evaluate IT risk factors in advance of pending strategic enterprise decisions and ensure that risk-aware enterprise decisions are made.				
5. Determine that IT use is subject to appropriate risk assessment and evaluation, as described in relevant international and national standards.				
6. Evaluate risk management activities to ensure alignment with the enterprise's capacity for IT-related loss and leadership's tolerance of it.				
Governance Practice	**Inputs**		**Outputs**	
EDM03.02 Direct risk management. Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite.	**From**	**Description**	**Description**	**To**
	AP012.03	Aggregated risk profile, including status of risk management actions	Risk management policies	AP012.01
			Key objectives to be monitored for risk management	AP012.01
	Outside COBIT	Enterprise risk management (ERM) profiles and mitigation plans	Approved process for measuring risk management	AP012.01
Activities				
1. Promote an IT risk-aware culture and empower the enterprise to proactively identify IT risk, opportunity and potential business impacts.				

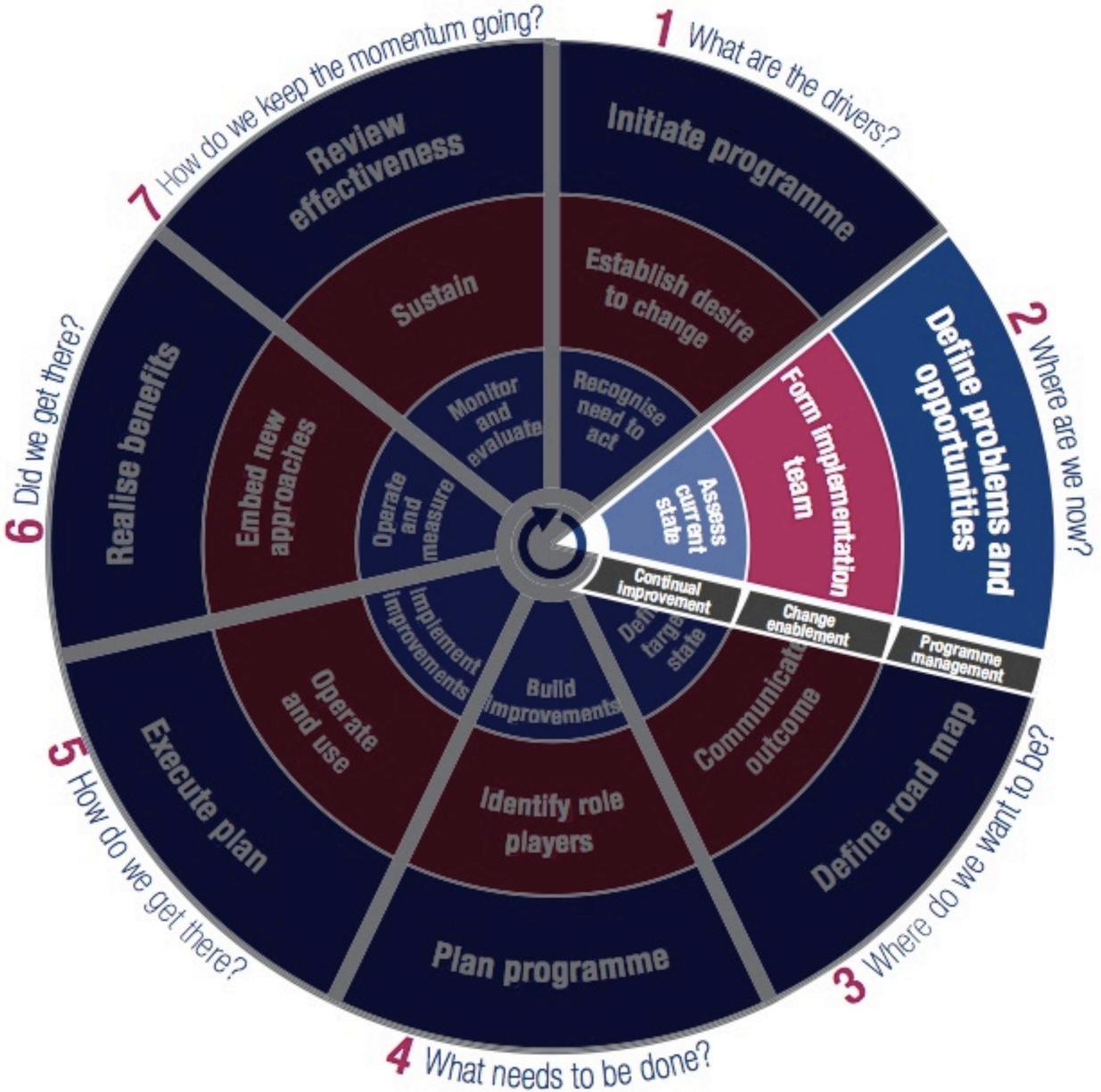


- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)

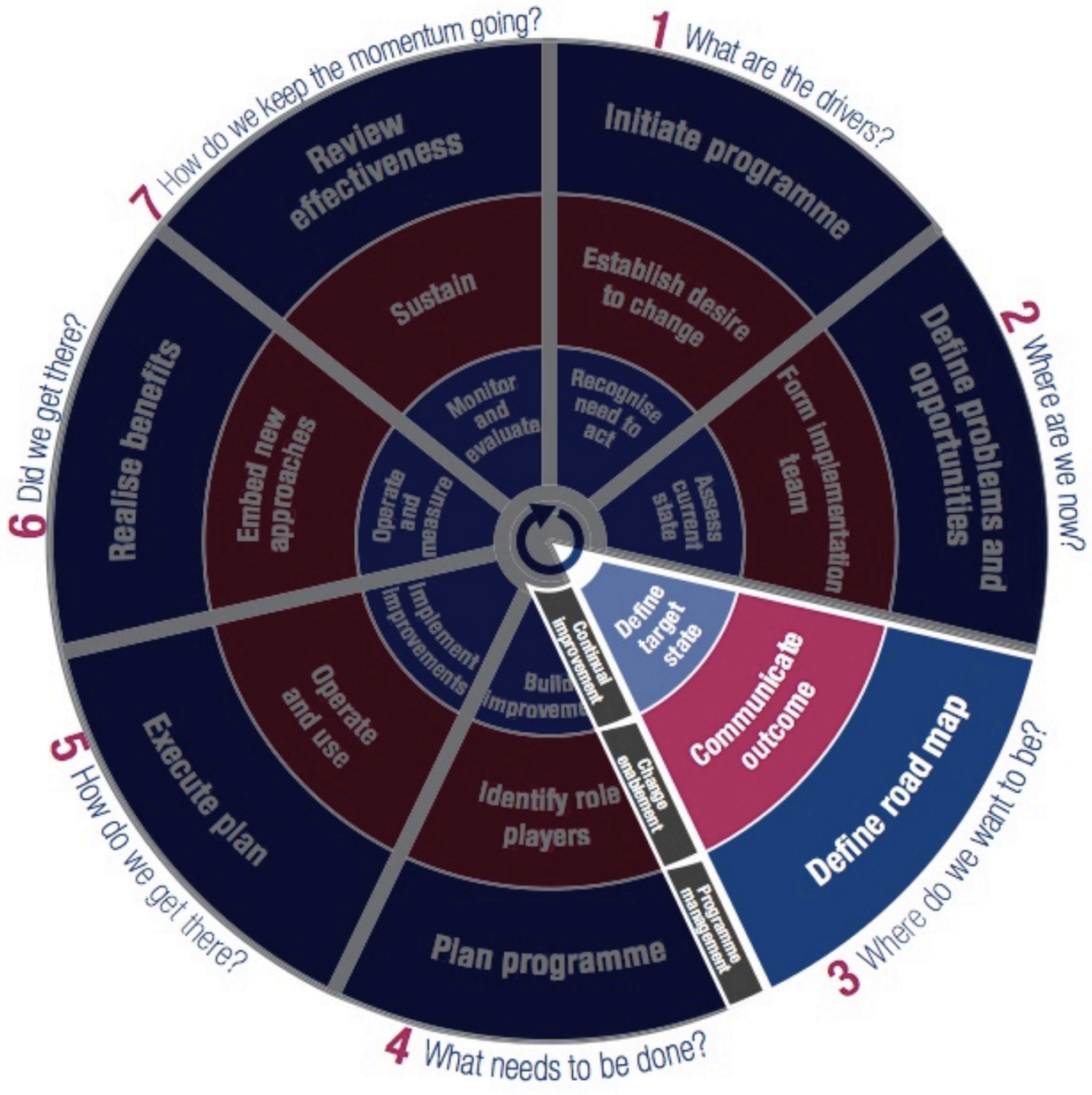

Who?
What?
How?
When?
Where?
Why?



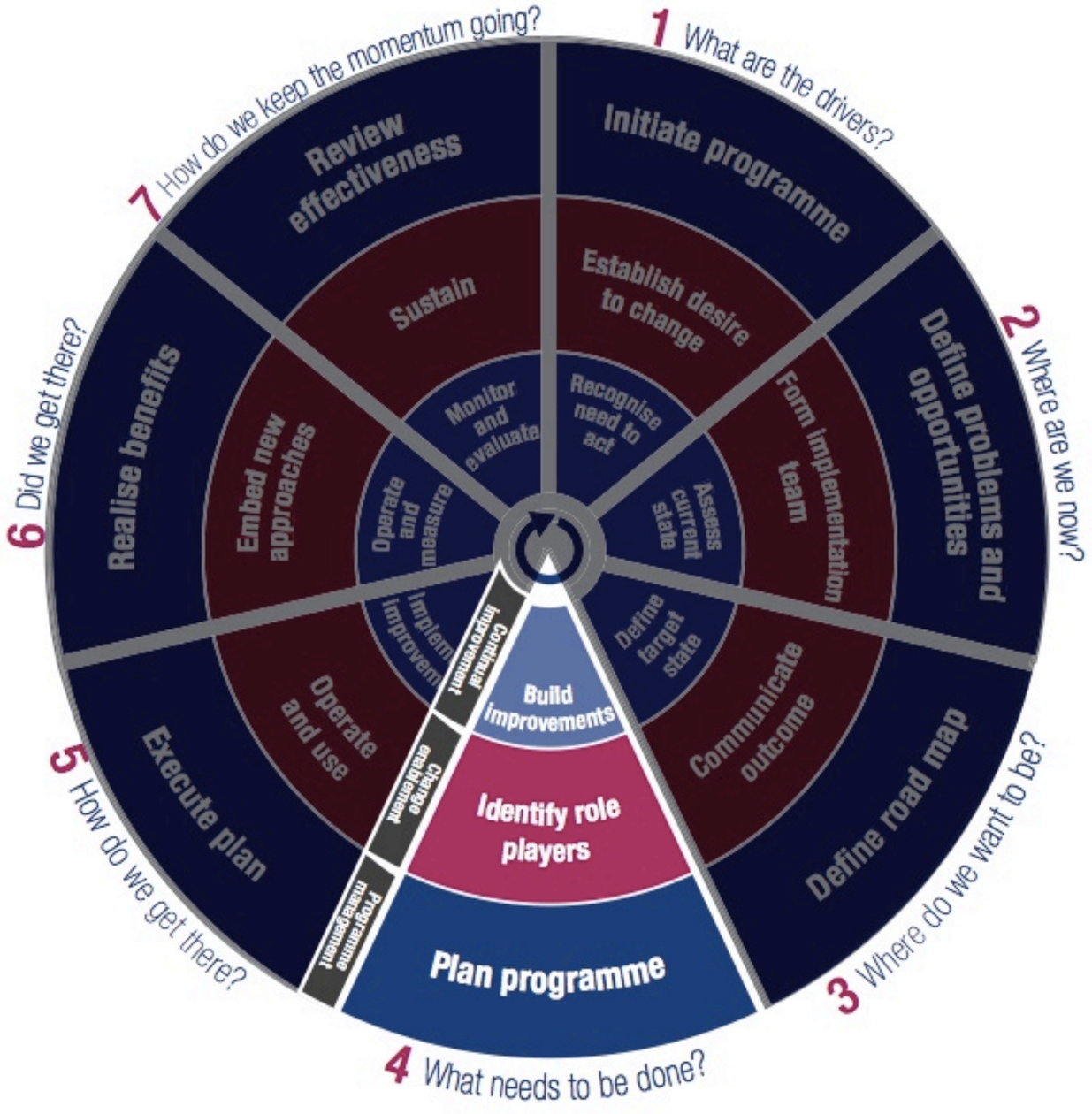
- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)



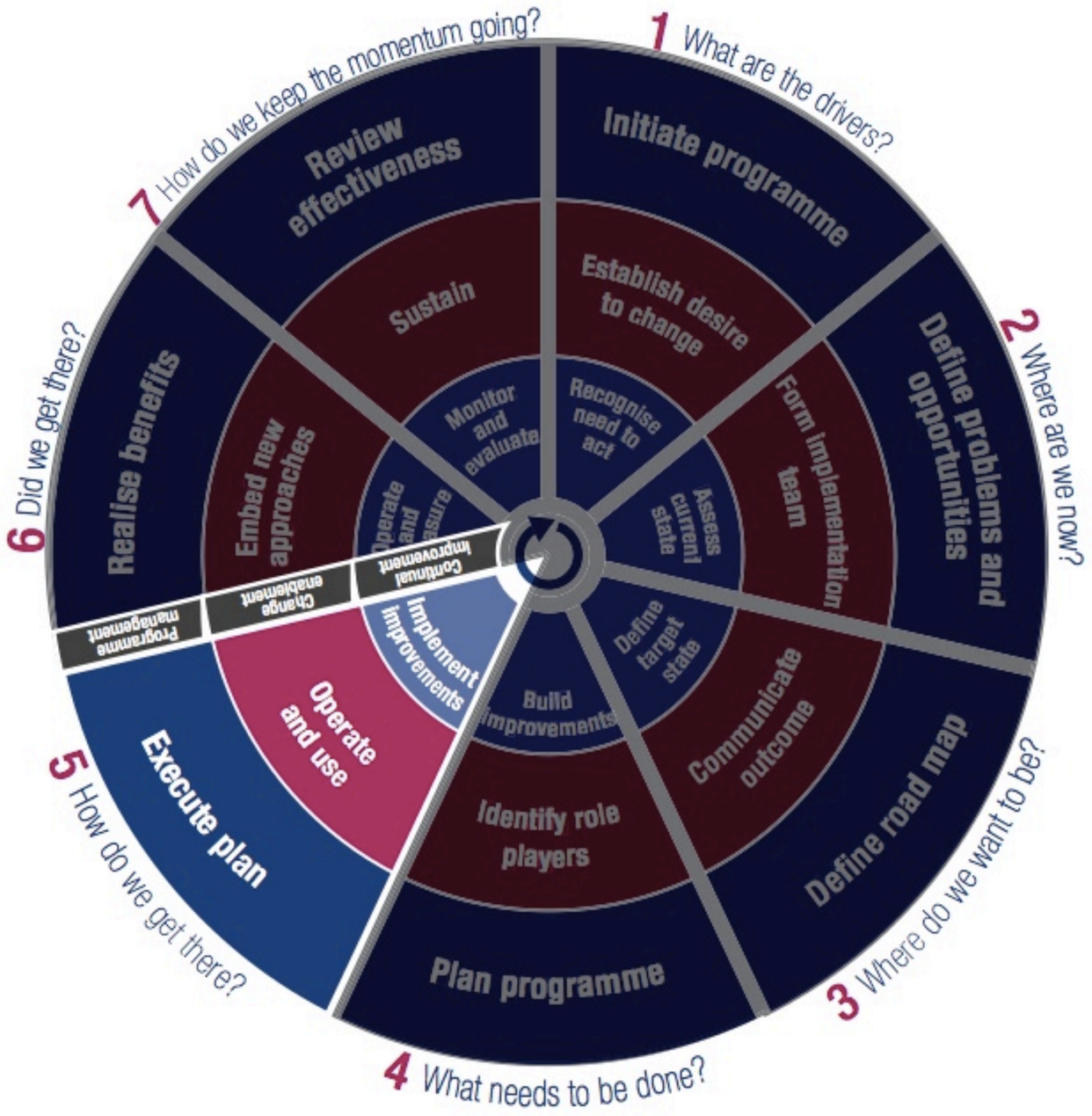
- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)



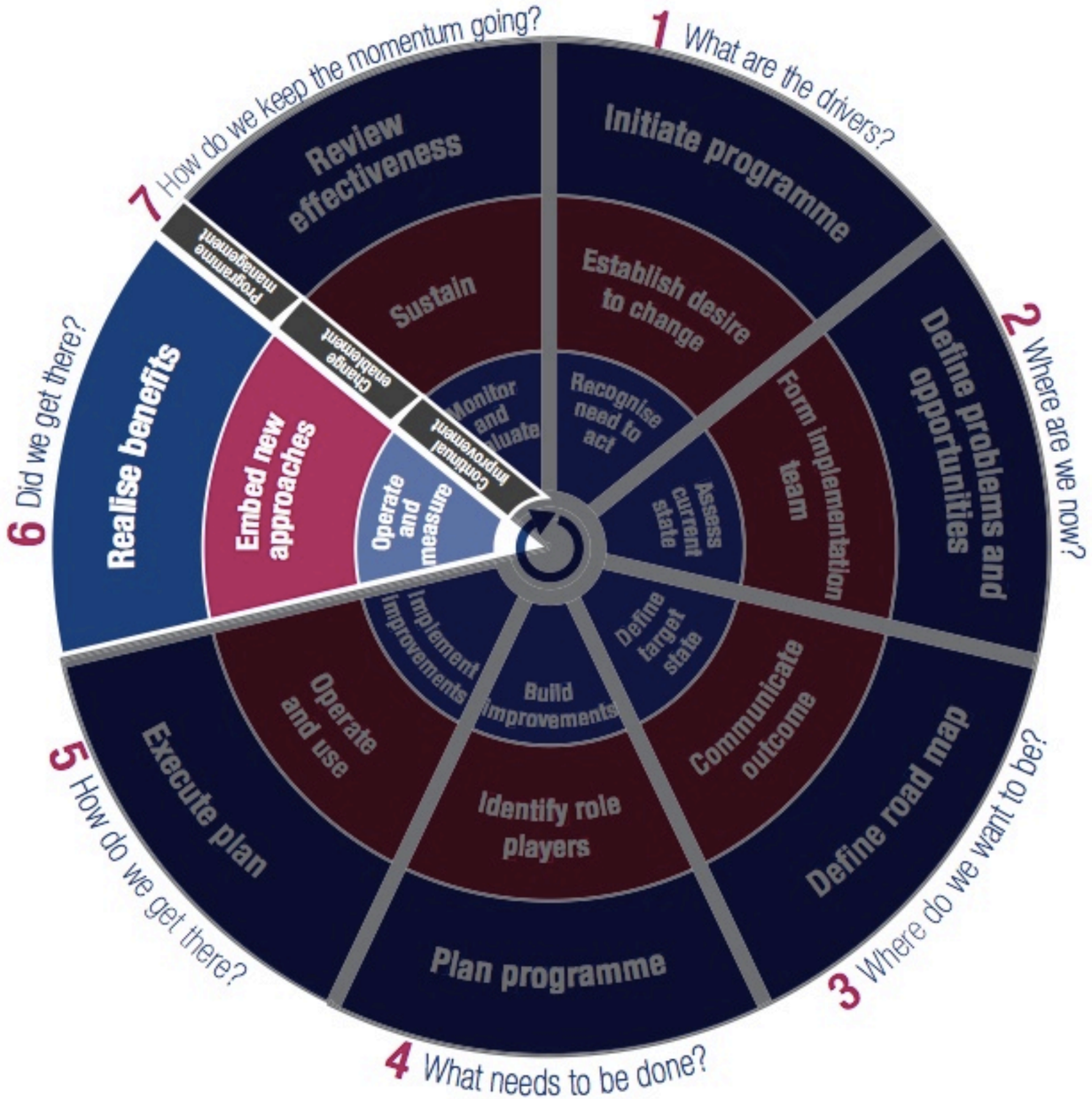
- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)



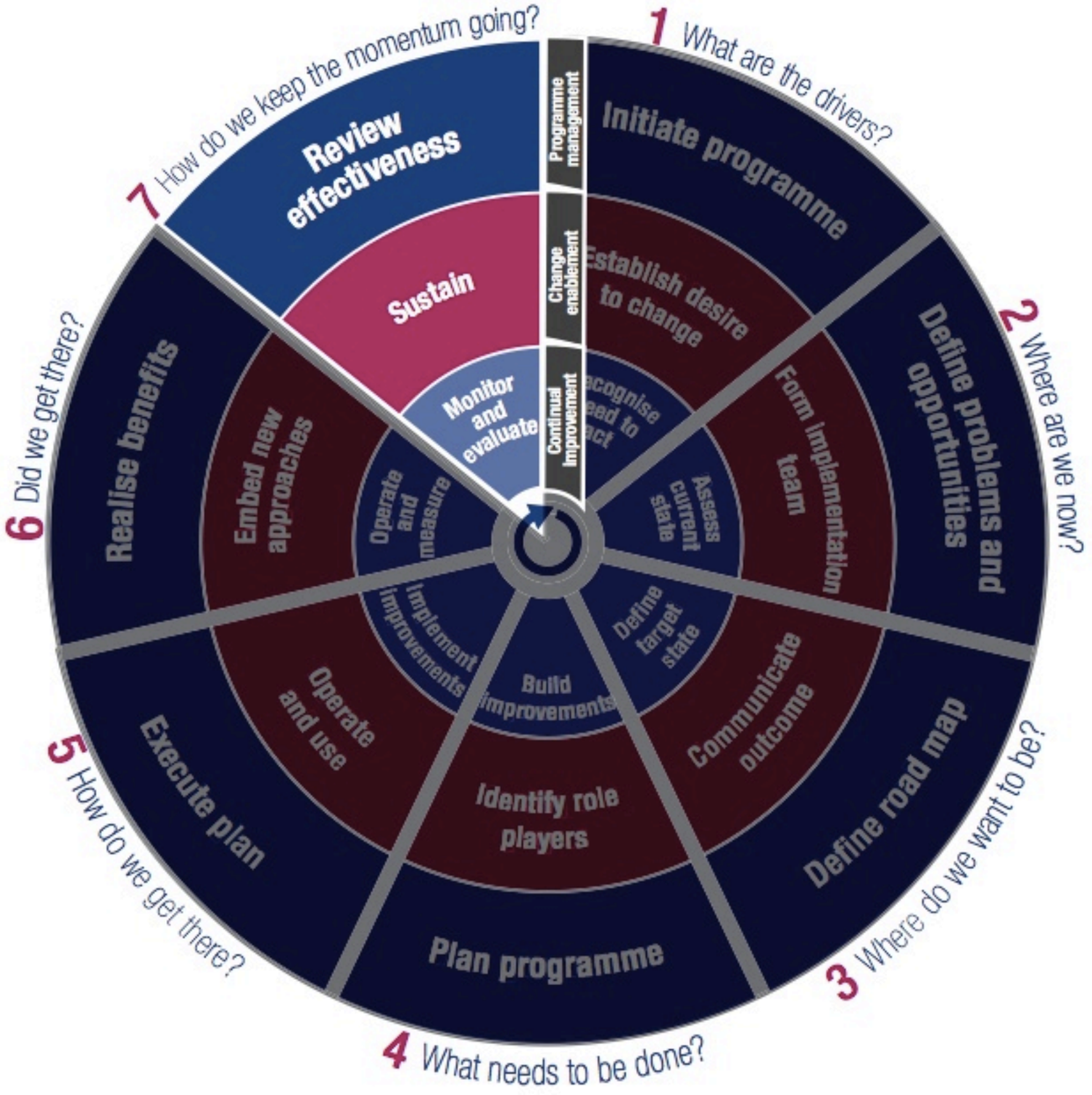
- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)



- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)



- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)



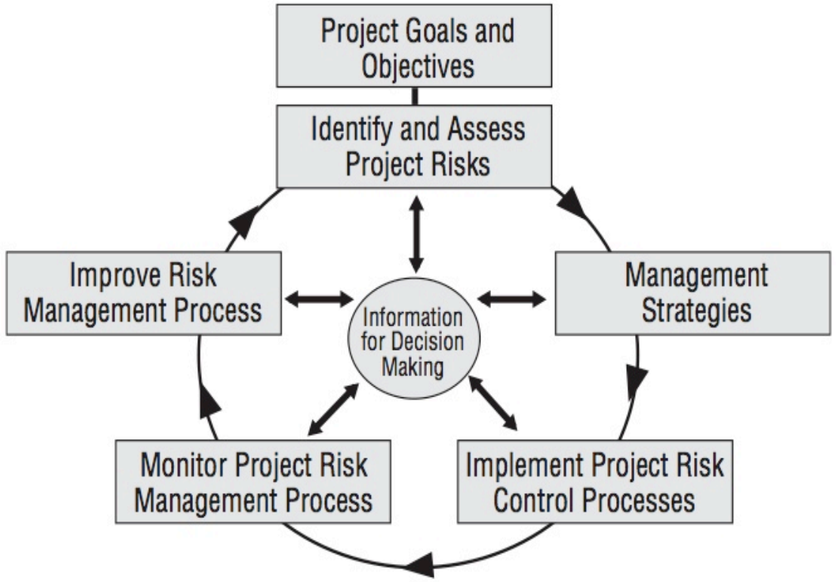
- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)

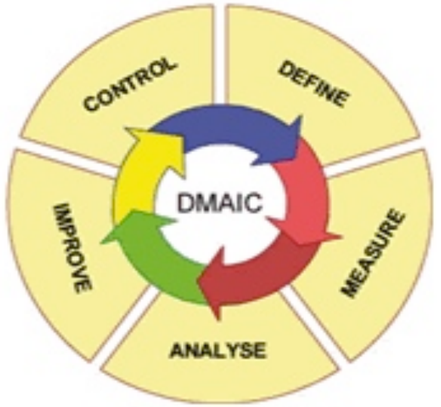

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124

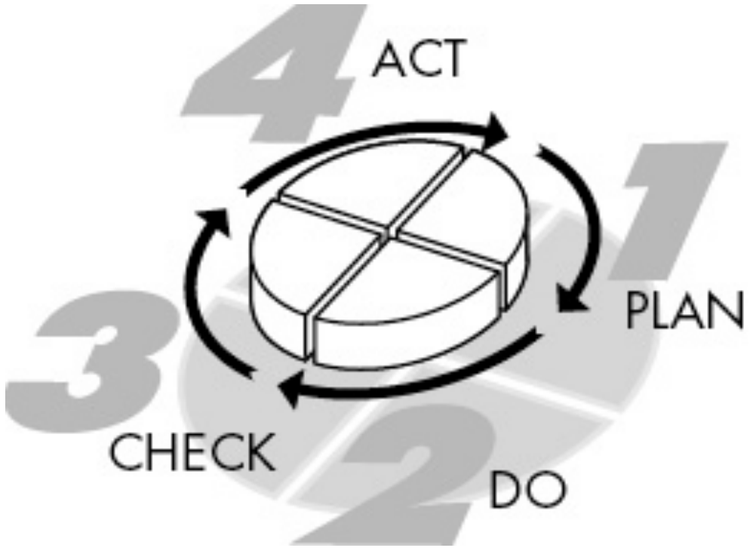
Leave behind your fears


CHANGE
AHEAD

N
NW
NE
W
E
SW
S
SUPERIOR
Duluth
BOSTON
NEW YORK
Winnipeg
Grand Forks
Fargo
Bismarck
Miles City
Mobridge
Great Falls
Helena
Billings
Spokane
Missoula
Butte
Livingston
YELLOWSTONE NATIONAL PARK
Rapid City
Casper
Weiser
Boise
Baker
Pocatello
Twin Falls
Ogden
Salt Lake City
Klamath Falls
Elko
Redding
Reno
Carson City
Sacramento
Stockton
Oakland
Mt. Whitney
Boulder City
Fresno
Pasadena
San Bernardino
Glendale
LOS ANGELES
Long Beach
San Diego
Yuma
UNIT





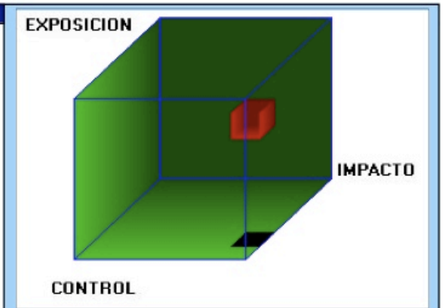


FICHA DE REVISION DE CONTROLES

Area	Area:	9.Control de Accesos.	**Control**	Número:	C-77
	SubArea:	9.2. Gestión de Acceso de Usuarios.		Sistema:	SRV-ID2 Tipo: LINUX-SUSE
	Control:	9.2.3. Gestión de las Contraseñas de Usuario.		Obtención:	AcControl Fecha: 01-feb-02

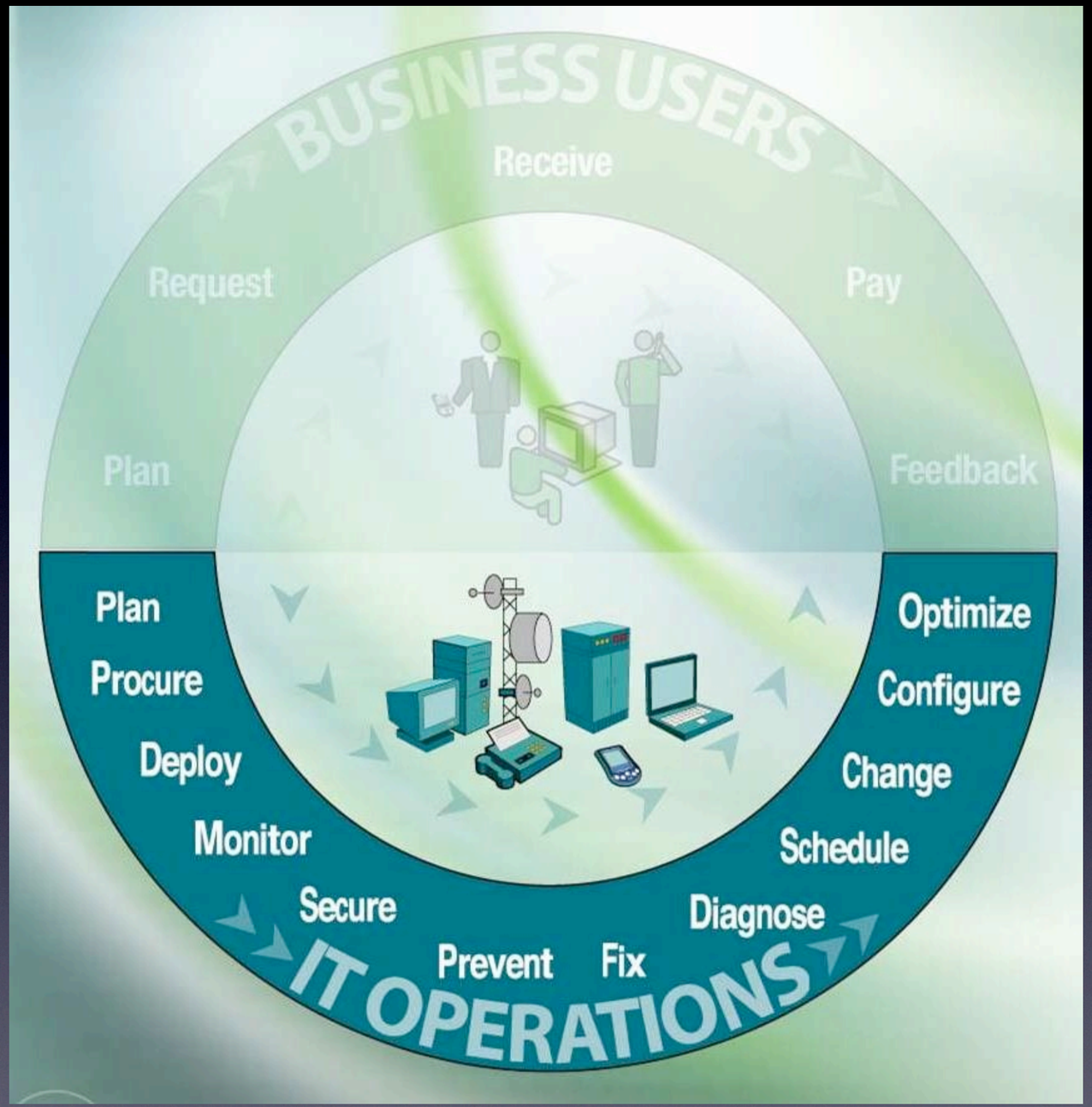
Resultado		
Control	4-Def	A los usuarios del sistema se les exige una contraseña para acceder al mismo pero ésta no caduca ni existen requisitos para su composición.
Explotación	4-Ext.Par.	El sistema es accesible a través de: 1.-Red Corporativa 2.-Red de Clientes 3.-Firewall ADSL
Impacto	5-Muy Alto	La deficiencia de este control supone un riesgo para: 1.-Int(5)/Conf(3)/Dis(4) de Producción 2.-Int(5)/Conf(5)/Dis(5) de Investigación y Desarrollo

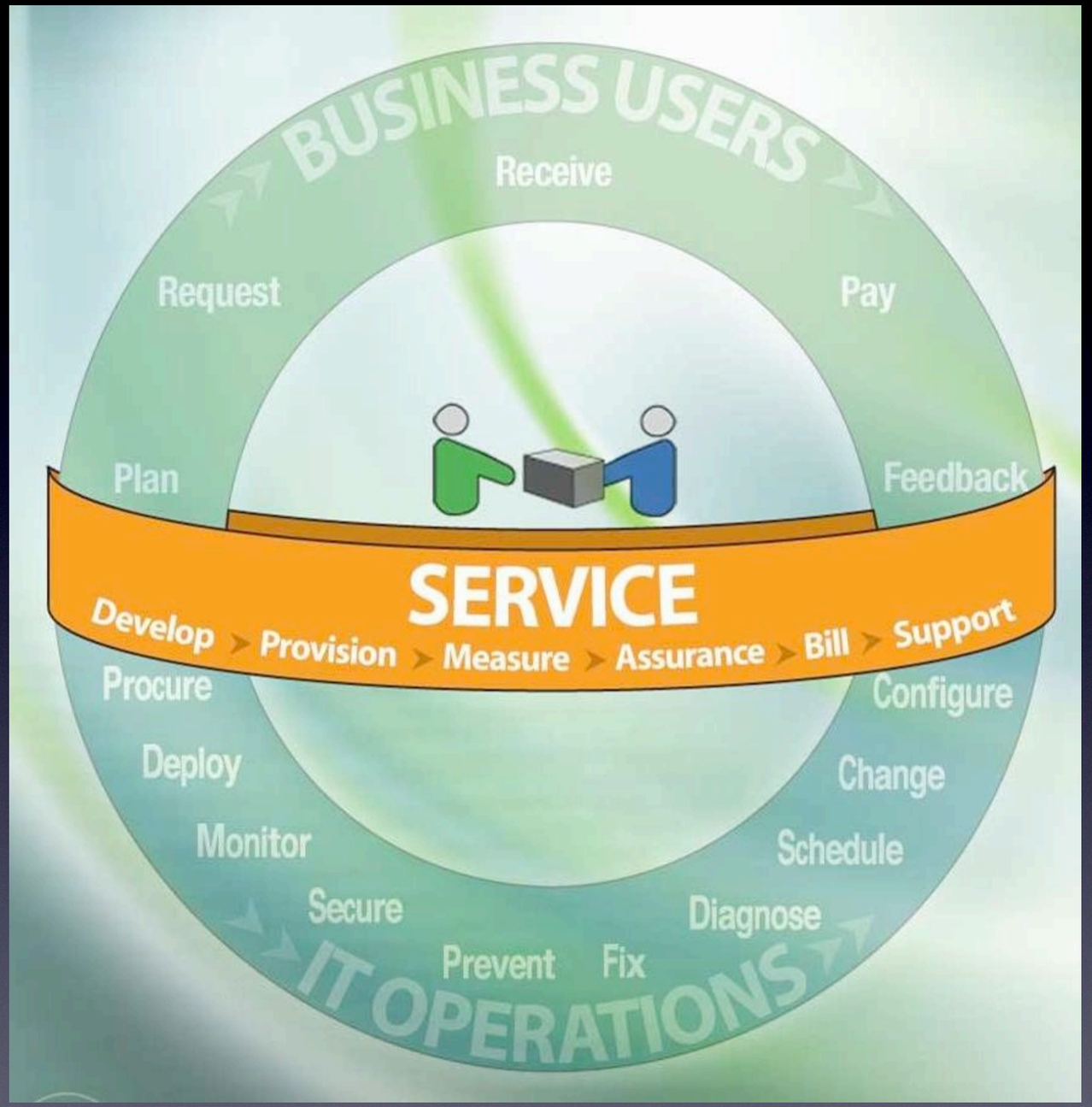
Gráfico



Analisis	**Comentario**
	La permisividad en la gestión de las contraseñas de usuario suele derivar en el uso por estos de contraseñas evidentes o triviales que si ademas no se cambian durante largos periodos de tiempo hacen fácil a posibles atacantes acceder a los sistemas sin necesidad de utilizar procedimientos especialmente complejos.
	Recomendación / Solución
	Recomendamos implantar una política de contraselas adecuada y dado el alto número de sistemas de la Sociedad estudiar la posibilidad de instalar sistemas como SSO que faciliten la gestión de contraseñas a los usuarios y a los administradores de sistemas reduciendo así el impacto de esta tarea en la Sociedad
	Respuesta


BUSINESS USERS
Receive
Request
Pay
Plan
Feedback


BUSINESS USERS
Receive
Request
Pay
Plan
Feedback
Plan
Procure
Deploy
Monitor
Secure
Prevent
Fix
Diagnose
Schedule
Change
Configure
Optimize
IT OPERATIONS


BUSINESS USERS
Receive
Request
Pay
Plan
Feedback
SERVICE
Develop
Provision
Measure
Assurance
Bill
Support
Procure
Configure
Deploy
Change
Monitor
Schedule
Secure
Diagnose
Prevent
Fix
IT OPERATIONS


Success
Failure

Antoni Gaudí, 1852 -1926

‘...originality consists in returning to the origin’

THANK YOU

COBIT 5 and its use to leverage the business world

Ramsés Gallego
CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT(f), Six Sigma Black Belt
Security Strategist & Evangelist
ramses.gallego@quest.com

Research Director & Strategic Planning, ISACA Barcelona Chapter
International Vice President, ISACA Board of Directors
ramses.gallego@me.com
@ramsesgallego