h·de
CYBER SECURITY

HIDE

عرض الخدمات المهنية

h·de
CYBER SECURITY

الرؤيـة

أن تكون هايد الشريك الرائد في مجال الأمن السيبراني للمنظمات في منطقة الخليج

h·de
CYBER SECURITY

المهمة

الاستفادة من مهاراتنا وخبراتنا وشفافيتنا لتقديم قيمة لعملائنا من خلال إدارة مخاطر الأمن السيبراني للأصول التنظيمية

h·de
CYBER SECURITY

عرض الخدمات المهنية

الدفاع السيبراني

- الاستجابة للحوادث
- الجنائية السيبرانية
- اصطياد التهديدات الامنية
- التدريب والتوعية المتخصصة

الحوكمة والالتزام

- الإستراتيجية \ عمارة التطوير
- إدارة السياسات والإجراءات
- المراجعات
- ISO 27001: 2013
- SAMA CSF
- NCA ECC, CCC, CSCC
- CSA / STAR / FedRAMP
- ISO 22301 (BC)/ISO 27031 (DR)
- COBIT 2019
- NDMO

التقييم

- تقييم الثغرات مقابل المعايير
- تقييم المخاطر
- تقييم أمان السحابة
- تقييم أمان التطبيق
- اختبار الاختراق \ الفريق الاحمر
- تقييم نقاط الضعف

h·de
CYBER SECURITY

تحليل الثغرة

h·de
CYBER SECURITY

ISO 27001
ISO 20000
STAR

NCA ECC
SAMA
COBIT

GAP ANALYSIS

Build Domains Framework
Analyze Gap
Assess Control Maturity

GAP ANALYSIS REPORT

Compliance Status
Recommendation
Ownership
Domain Maturity Level

h·de
CYBER SECURITY

Internal Policies
Processes

NDMO

GAP ANALYSIS

Analyze Gap

NDMO Driven: Data Governance & Management Deliverables

Policies, Plans, procedures, Training
Data Governance, Mgt.
Data Quality
Data Reliability, Security, etc.

المنهجية

التقرير والإبلاغ ← التحليل ← التقييم ← جمع المعلومات ← التخطيط

مراجعة الوثائق

ملاحظات

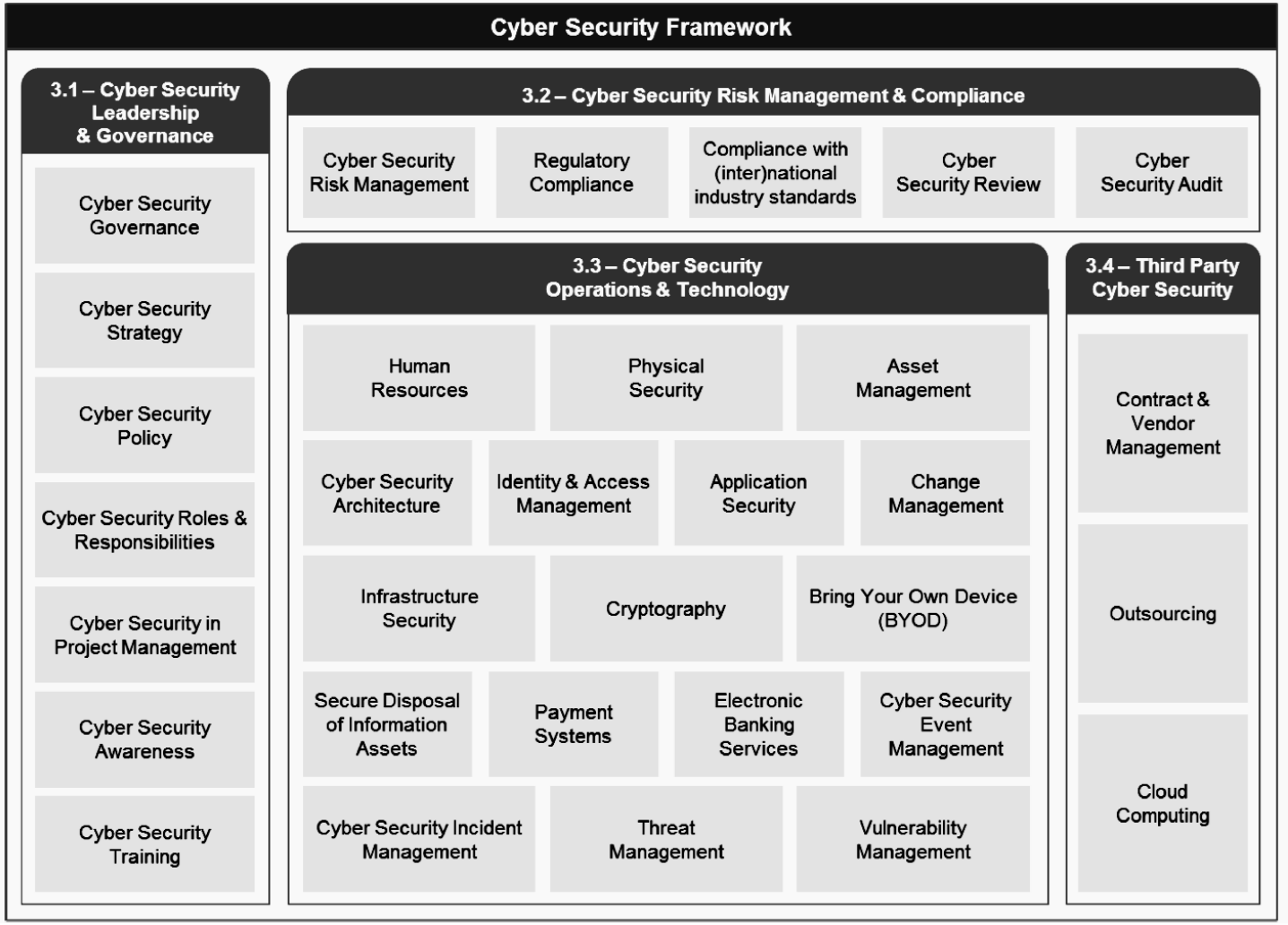
اجتماعات

h·de
CYBER SECURITY

معايير قياسية أخرى

h·de
CYBER SECURITY

إطار عمل الأمن السيبراني لبنك المركزي السعودي (SAMA)



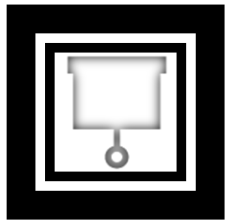
h·de
CYBER SECURITY

h·de
CYBER SECURITY

إطار عمل NIST للامن السيبراني

التصنيف	المعرف الخاص بالتصنيف	الوظيفة	المعرف الخاص بالوظيفة
إدارة الأصول (Asset Management)	AM	التحديد (Identify)	ID
بيئة العمل (Business Environment)	BE		
الحوكمة (Governance)	GV		
تقييم المخاطر (Risk Assessment)	RA		
استراتيجية إدارة المخاطر (Risk Management Strategy)	RM		
إدارة الهوية والمصادقة عليها والتحكم في الوصول (Identity Management, Authentication and Access Control)	AC	الحماية (Protect)	PR
التوعية والتدريب (Awareness and Training)	AT		
أمن البيانات (Data Security)	DS		
عمليات وإجراءات حماية المعلومات (Information Protection Processes and Procedures)	IP		
التقنية الوقائية (Protective Technology)	PT		
الحالات غير الطبيعية والأحداث (Anomalies and Events)	AE	الرصد (Detect)	DE
المراقبة الأمنية المستمرة (Security Continuous Monitoring)	CM		
عمليات الرصد (Detection Processes)	DP		
الاتصالات (Communications)	CO	الاستجابة (Respond)	RS
التحليل (Analysis)	AN		
التقليل (Mitigation)	MI		
التحسينات (Improvements)	IM		
خطة الاستعادة (Recovery Planning)	RP	الاستعادة (Recover)	RC
التحسينات (Improvements)	IM		

إطار تحليل الفجوة (GAF)

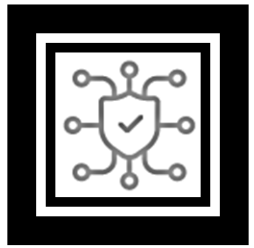


التدريب والتوعية

إدارة المخاطر

عمارة الأمن

الحوكمة والامتثال



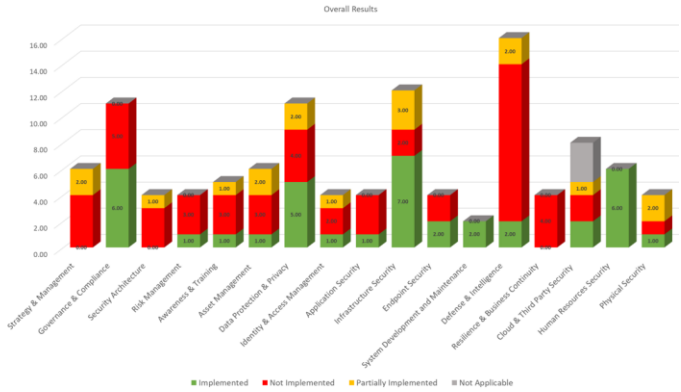
الدفاع

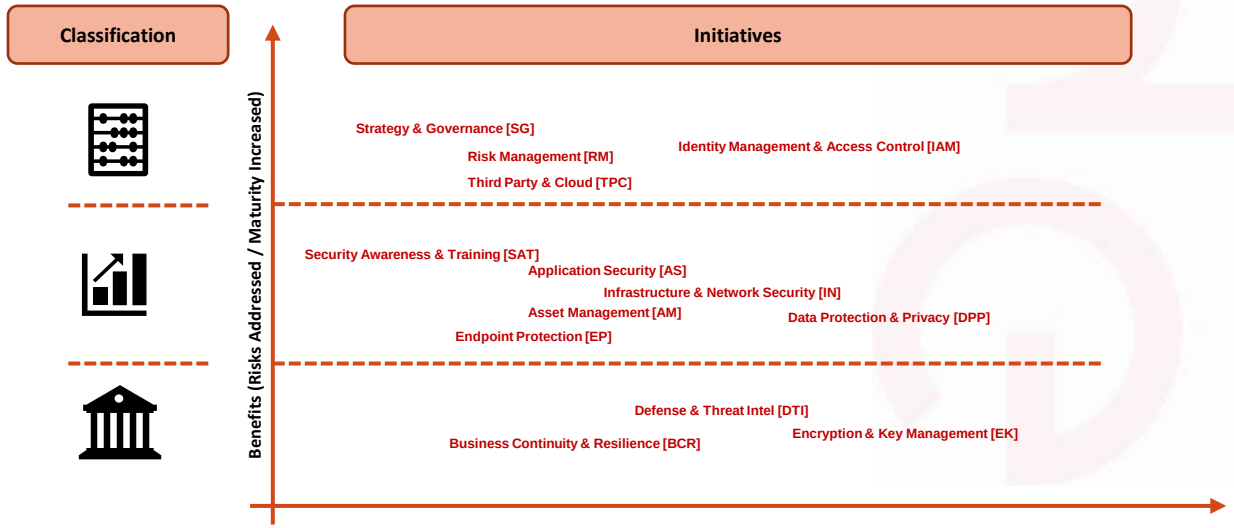
أمان التطبيق

أمن نقطة النهاية

عينة من المخرجات

Overall Results					
Cybersecurity Domains	Implemented	Not Implemented	Partially Implemented	Not Applicable	TOTAL
Strategy & Management	0.00	4.00	2.00	0.00	6.00
Governance & Compliance	6.00	5.00	0.00	0.00	11.00
Security Architecture	0.00	3.00	1.00	0.00	4.00
Risk Management	1.00	3.00	0.00	0.00	4.00
Awareness & Training	1.00	3.00	1.00	0.00	5.00
Asset Management	1.00	3.00	2.00	0.00	6.00
Data Protection & Privacy	5.00	4.00	2.00	0.00	11.00
Identity & Access Management	1.00	2.00	1.00	0.00	4.00
Application Security	1.00	3.00	0.00	0.00	4.00
Infrastructure Security	7.00	2.00	3.00	0.00	12.00
Endpoint Security	2.00	2.00	0.00	0.00	4.00
System Development and Maintenance	2.00	0.00	0.00	0.00	2.00
Defense & Intelligence	2.00	12.00	2.00	0.00	16.00
Resilience & Business Continuity	0.00	4.00	0.00	0.00	4.00
Cloud & Third Party Security	2.00	2.00	1.00	3.00	8.00
Human Resources Security	6.00	0.00	0.00	0.00	6.00
Physical Security	1.00	1.00	2.00	0.00	4.00
TOTAL	38.00	53.00	17.00	3.00	111.00
PERCENTAGE	34.23%	47.75%	15.32%	2.70%	

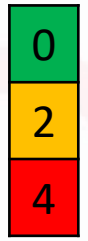




عينة من المخرجات

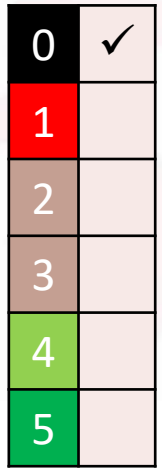
DESCRIPTION
A Cybersecurity strategy must be defined , documented, approved and supported by the head of the organization. The strategy goals must be in line with the rules and regulations. A road map must be in place to implement the strategy.
A Cybersecurity steering committee must be established, and the committee member's roles and responsibilities must be defined, documented and approved. The head of the Cybersecurity must be included as a member of the committee and the committee should report directly to the organization head.

G-SM



Current Maturity Level	0 [Non-Existent]	**Target Maturity Level**	4 [Transformed] | 2 Years

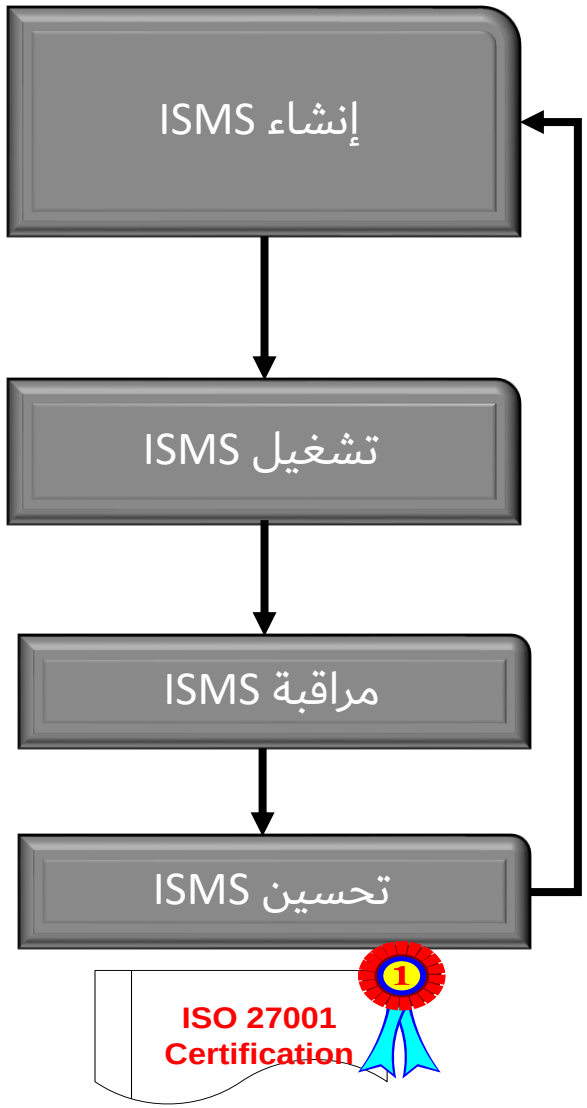
Highs	Enterprise Strategy in Progress. Cybersecurity strategy soon to be developed
Lows	No Overarching Strategy to guide and steer Cybersecurity initiatives Were ISO 27001 certified; however, certification has expired. Implementation Lacking



h·de
CYBER SECURITY

نظام إدارة أمن المعلومات (ISMS)

نهج تنفيذ ISMS



1. تحديد سياسة أمن المعلومات
2. تحديد نطاق ISMS
3. تحديد أصول المعلومات وتقييمها
4. تحديد المخاطر
5. تحديد الضوابط

1. تحديد ونشر السياسات والإجراءات والمعايير
2. تنفيذ الضوابط والتوعية والتدريب

1. التدقيق الداخلي
2. مراجعة إدارة ISMS

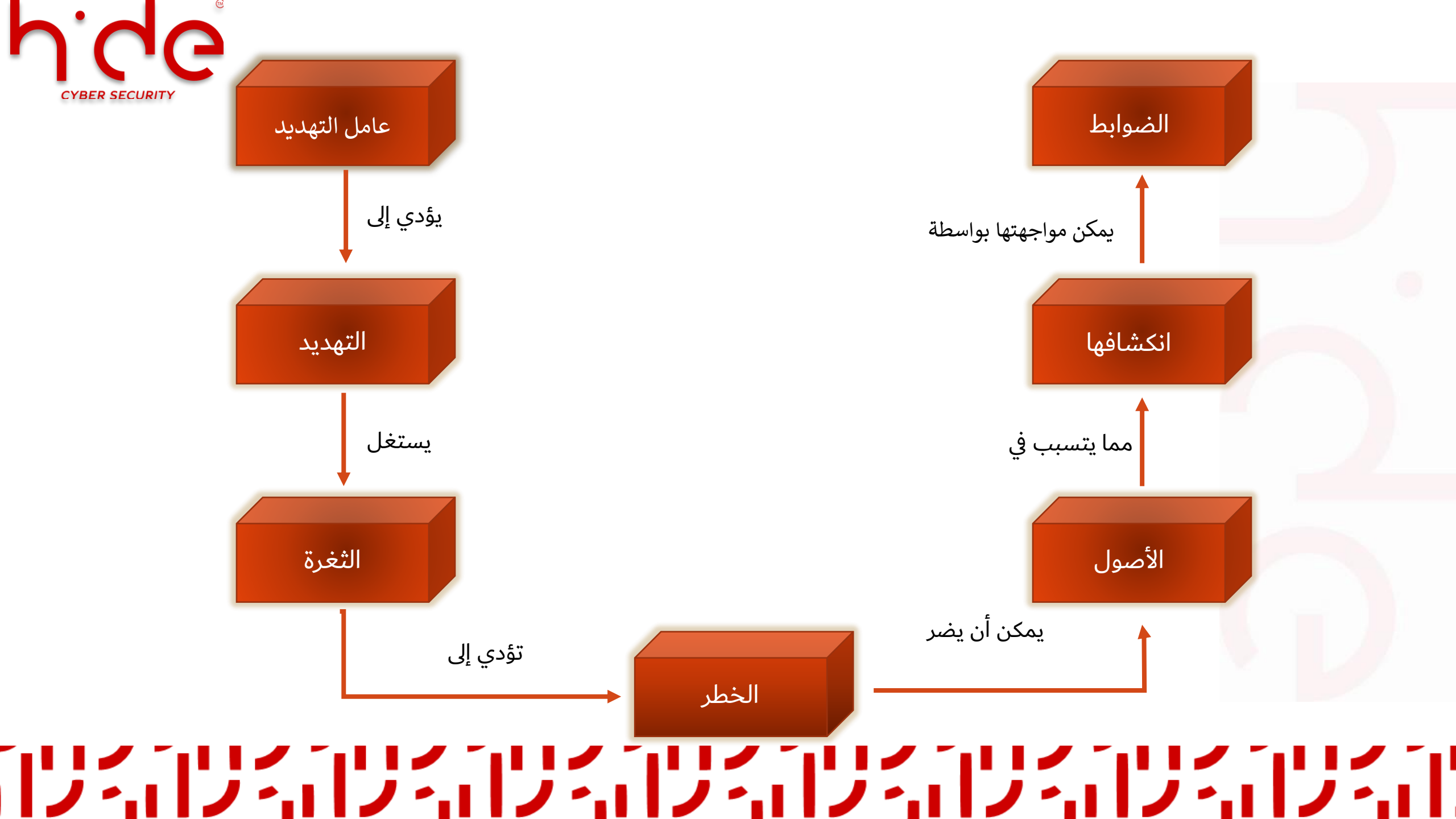
1. اتخاذ الإجراءات التصحيحية / الوقائية ((CAPA

1. المراجعة الخارجية للاعتماد

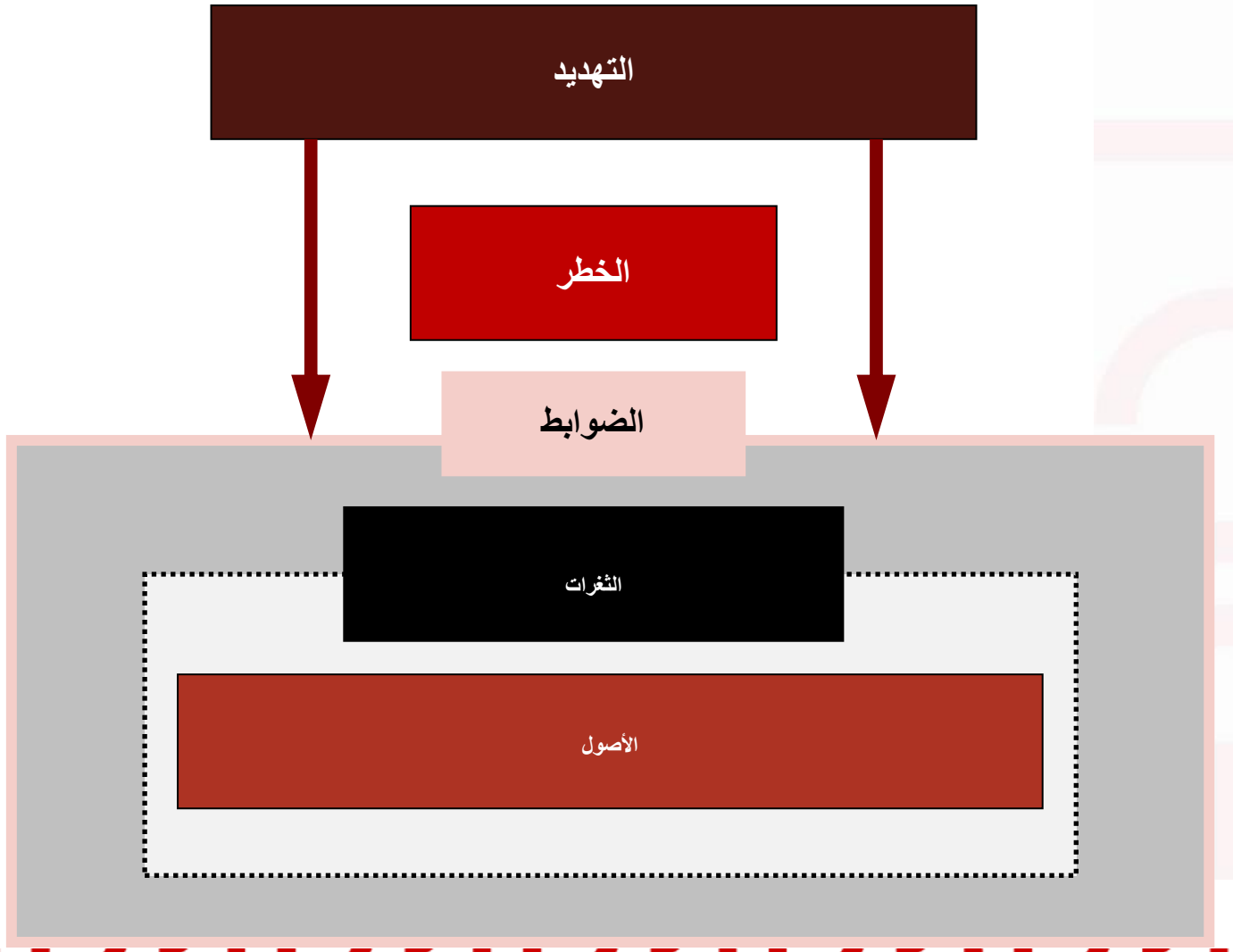
إدارة المخاطر

المخاطرة

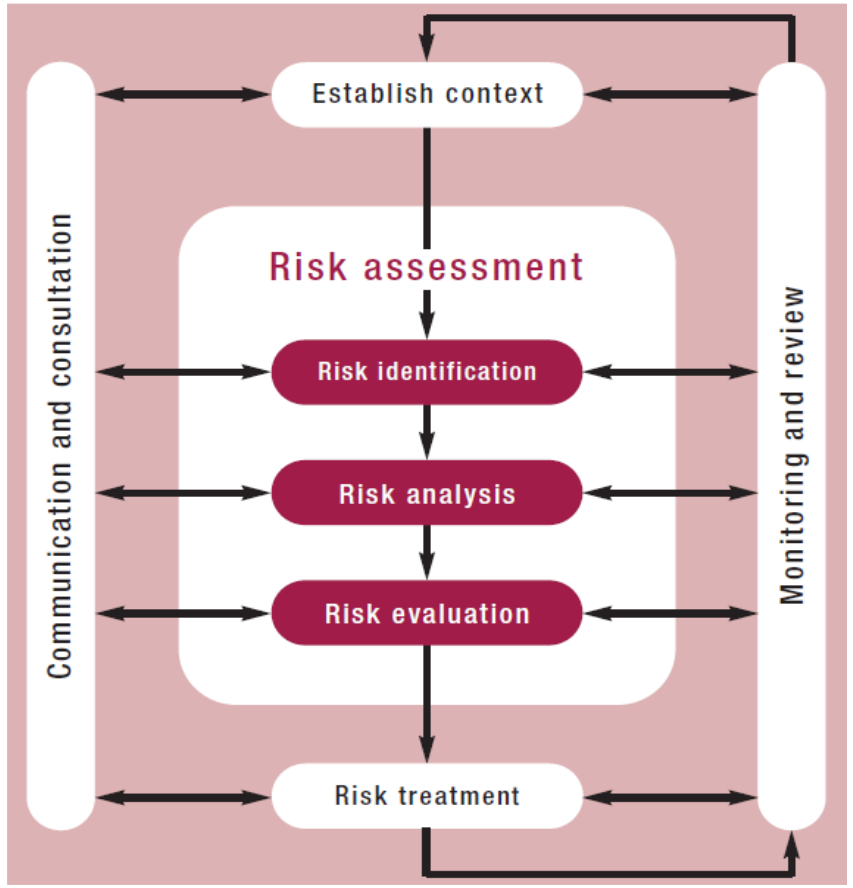
موقف يتضمن التعرض للخطر


عامل التهديد
يؤدي إلى
التهديد
يستغل
الثغرة
تؤدي إلى
الخطر
يمكن أن يضر
الأصول
مما يتسبب في
انكشافها
يمكن مواجهتها بواسطة
الضوابط

المخاطر



ISO 31000
ISO/IEC
27005:2011



h·de
CYBER SECURITY

الخطر المتبقي

مساوية للمخاطر الحالية إضافية مع تطبيق استجابات مخاطر، يتم تحديد الاستجابات الإضافية للمخاطر بناءً على تحليل المخاطر الحالية

الخطر الحالي

المخاطر الفعلية اليوم ، أي المخاطر الكامنة مع تطبيق الاستجابات الحالية للمخاطر

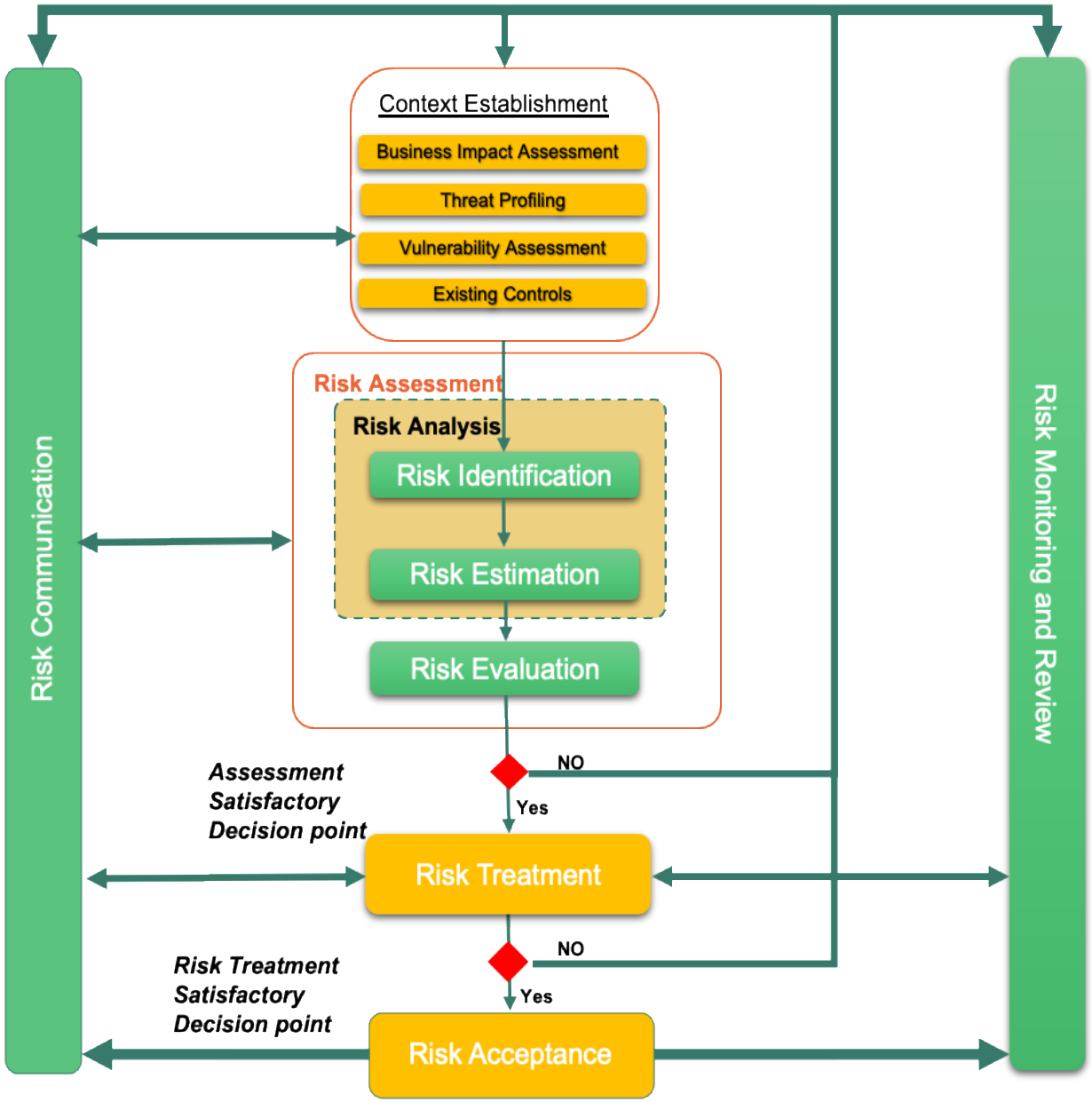
الخطر الكامن

دون الأخذ بعين الاعتبار أي استجابة للمخاطر

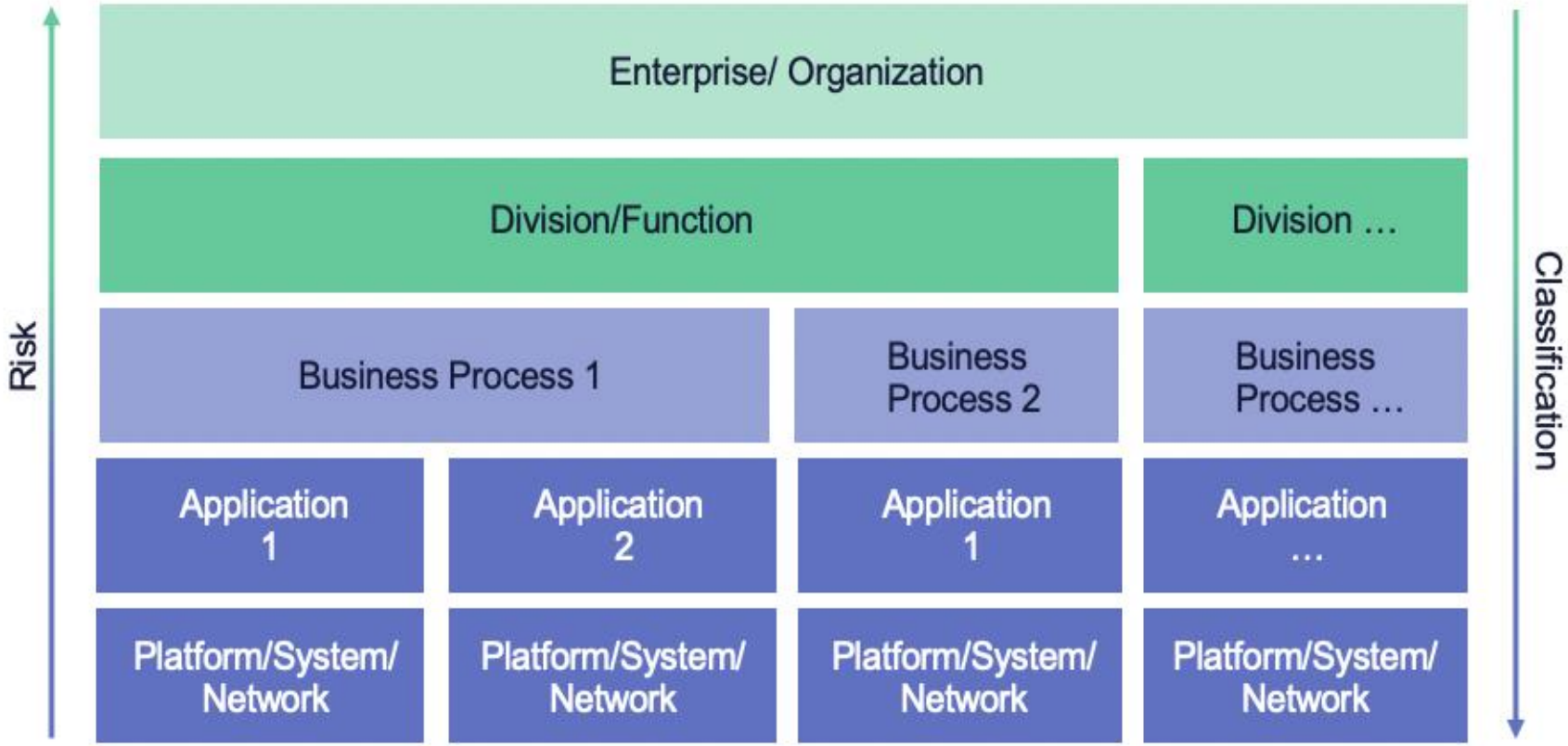
منهجية إدارة المخاطر


إدارة إطار عمل المخاطر
سياسة إدارة المخاطر
تقبل المخاطر.
منهجية تقييم المخاطر
جراءات تقييم المخاطر
مرجعية فهارس
التهديدات ذات الصلة.
الثغرات ذات الصلة.
الضوابط القابلة للتطبيق.
الموارد
مقدم الطلب.
المقيم.
موارد خارجية.
التواصل
المراقبة

عملية تقييم المخاطر


Context Establishment
Business Impact Assessment
Threat Profiling
Vulnerability Assessment
Existing Controls
Risk Assessment
Risk Analysis
Risk Identification
Risk Estimation
Risk Evaluation
Risk Communication
Risk Monitoring and Review
Assessment Satisfactory Decision point
NO
Yes
Risk Treatment
Risk Treatment Satisfactory Decision point
NO
Yes
Risk Acceptance

سياق المخاطر والتصنيف



نموذج العمليات الحسابية

Threat Valuation

Threat Score			Likelihood					
			Unlikely	1	Could happen	2	Very likely	3
Impact	Low	1	1		2		3	
	Medium	2	2		4		6	
	High	3	3		6		9	
	Very High	4	4		8		12	

Threat Score	Threat Value	
1	Low	1
2		
3		
4	Medium	2
5		
6		
7	High	3
8		
9		
10	Very High	4
11		
12		

Vulnerability Value

Ease of Exploitation	Vulnerability Value	
Very Difficult	Low	1
Difficult	Medium	2
Easy	High	3
Very Easy	Very High	4

Risk Calculation BASELINE = 8

risk score = asset value x threat value x vulnerability value

	Threat Value	Low				Medium				High				Very High			
	Vulnerability Value	L	M	H	VH	L	M	H	VH	L	M	H	VH	L	M	H	VH
Asset Value	Low	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
	Medium	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
	High	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
	Very High	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

risk value = risk score / control strength

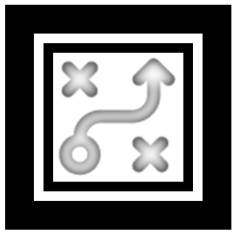
1	2	3	4	6	8	9	12	16	18	24	27	32	36	48	64

Acceptable Risks

Non Acceptable Risks

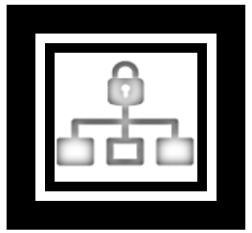
Prioritization of Non Acceptable Risks	
Low	1 to 11
Medium	12 to 23
High	24 to 31
Very High	32 to 64

إطار عمل UCF



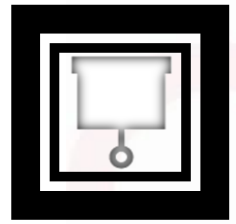
الإستراتيجية والإدارة

الحوكمة و الامتثال



عمارة أمنية

إدارة المخاطر



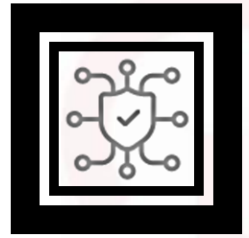
التدريب والتوعية

أمان نقطة النهاية

حماية البيانات والخصوصية

إدارة الهوية والوصول

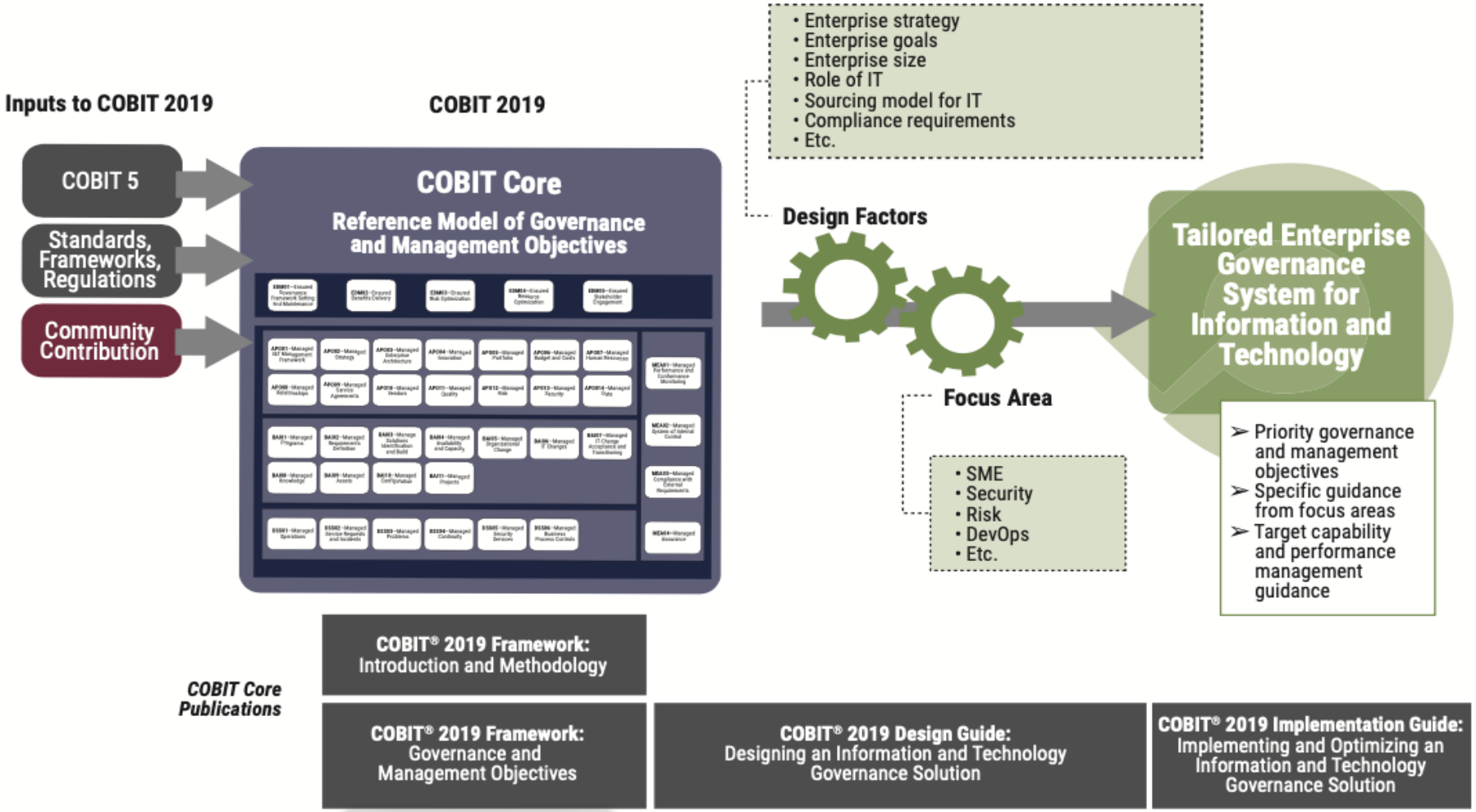
أمن التطبيقات



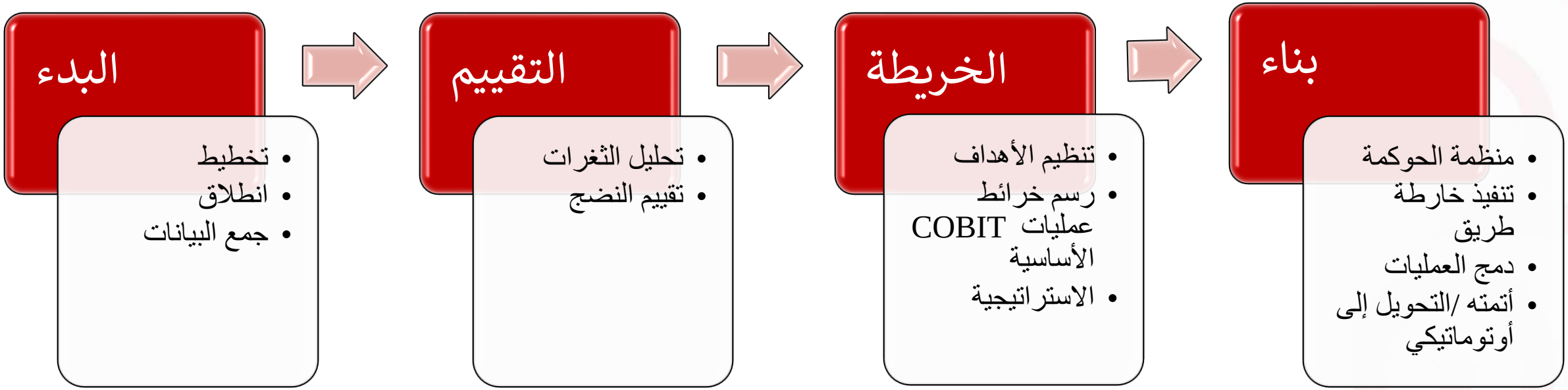
الدفاع و الذكاء

حوكمة تكنولوجيا المعلومات في المؤسسة

COBIT 2019


Inputs to COBIT 2019
COBIT 2019
COBIT 5
Standards, Frameworks, Regulations
Community Contribution
COBIT Core
Reference Model of Governance and Management Objectives
• Enterprise strategy
• Enterprise goals
• Enterprise size
• Role of IT
• Sourcing model for IT
• Compliance requirements
• Etc.
Design Factors
Focus Area
• SME
• Security
• Risk
• DevOps
• Etc.
Tailored Enterprise Governance System for Information and Technology
➢ Priority governance and management objectives
➢ Specific guidance from focus areas
➢ Target capability and performance management guidance
COBIT Core Publications
COBIT® 2019 Framework: Introduction and Methodology
COBIT® 2019 Framework: Governance and Management Objectives
COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution
COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution

المنهجية


البدء
• تخطيط
• انطلاق
• جمع البيانات
التقييم
• تحليل الثغرات
• تقييم النضج
الخريطة
• تنظيم الأهداف
• رسم خرائط عمليات COBIT الأساسية
• الاستراتيجية
بناء
• منظمة الحوكمة
• تنفيذ خارطة طريق
• دمج العمليات
• أتمته /التحويل إلى أوتوماتيكي

h·de CYBER SECURITY

تقييم، توجيه و مراقبة

امتثال

75-100 %
50-74 %
25-49%
1- 24%
% 0

EDM01 Ensure Governance framework setting & maintenance | **EDM02 Ensure Benefits Delivery** | EDM03 Ensure Risk Optimization | EDM04 Ensure Resource Optimization | EDM05 Ensure Stakeholder transparency

محاذاة، تخطيط و تنظيم

APO01 Manage the IT Management Framework	APO02 Manage Strategy	APO03 Manage Enterprise Architecture	APO04 Manage Innovation	APO05 Manage Portfolio	APO06 Manage Budget and Costs
APO07 Manage Human Resources	**APO08 Manage Relationships**	APO09 Manage Service Agreements	APO10 Manage Suppliers	APO11 Manage Quality	APO12 Manage Risk
APO13 Manage Security					

بناء، اكتساب و تنفيذ

BAI01 Manage Programs & Projects	BAI02 Manage Requirement Definition	BAI03 Manage Solutions Identification & build	BAI04 Manage Availability & Capacity	BAI05 Manage Organizational Change enablement	BAI06 Manage Changes
BAI07 Manage Change acceptance & transitioning	BAI08 Manage knowledge	BAI09 Manage Assets	BAI10 Manage Configuration		

تقديم الخدمة و الدعم

DSS01 Manage Operations	DSS02 Manage service requests & incidents	DSS03 Manage problems	DSS04 Manage Continuity	DSS05 Manage Security services	DSS06 Manage business process controls

المراقبة و التقييم

MEA01 Monitor, Evaluate & Assess Conformance and Performance

MEA02 Monitor, evaluate & assess the system of internal control

MEA03 Monitor, evaluate & assess compliance with external requirements

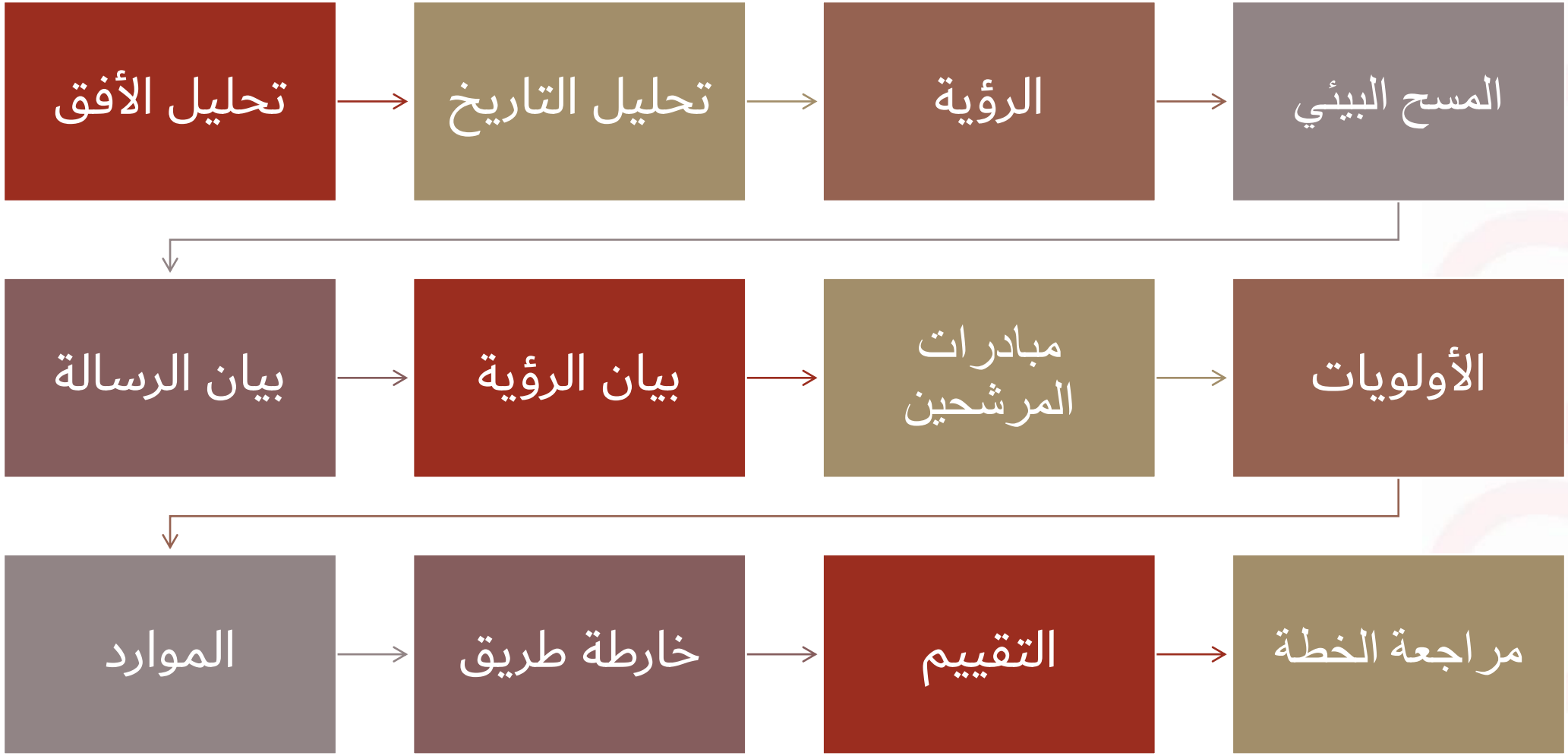
h·de
CYBER SECURITY

تطوير استراتيجية الأمن السيبراني

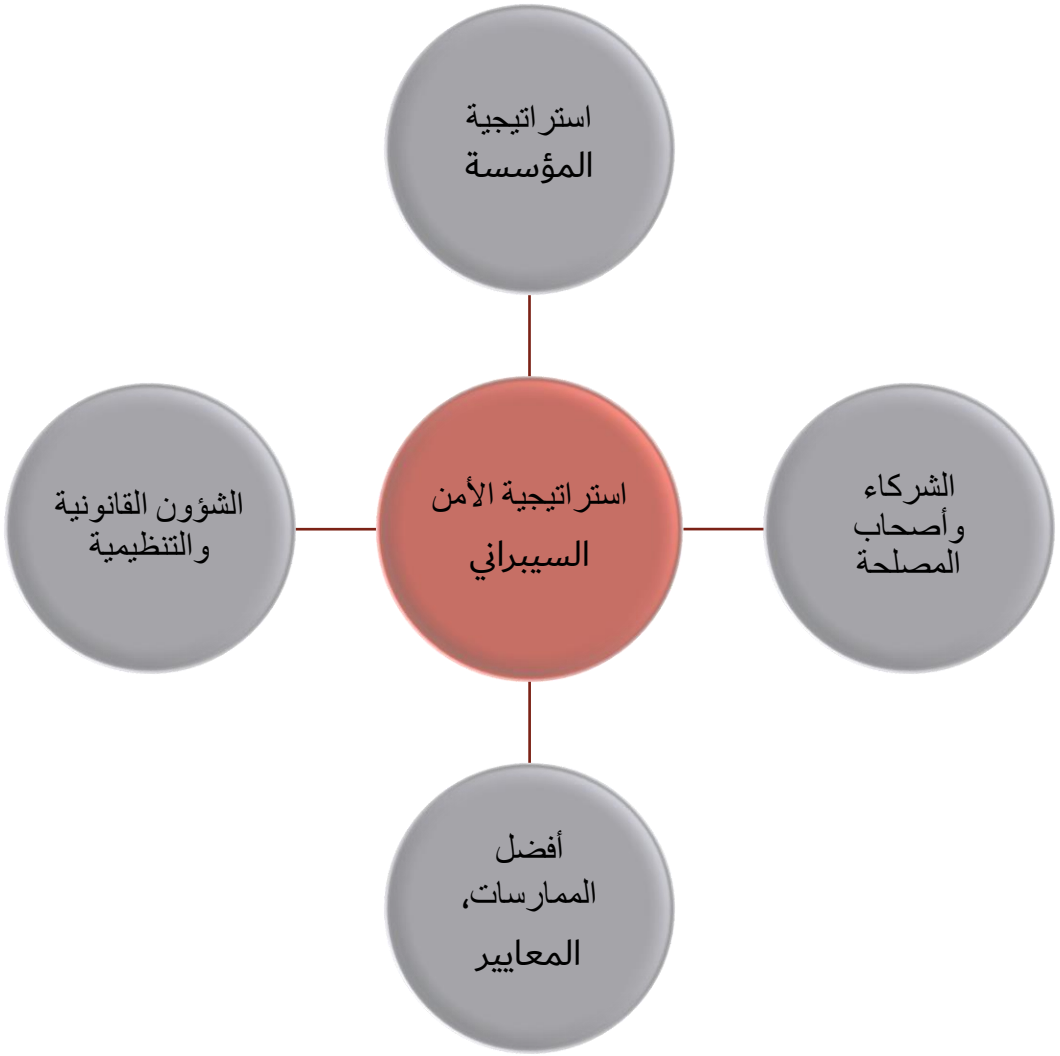
الاستراتيجية: خطة أو طريقة أو سلسلة من المناورات أو الحيل لتحقيق هدف أو نتيجة معينة

h·de
CYBER SECURITY

خطوات التخطيط الاستراتيجي



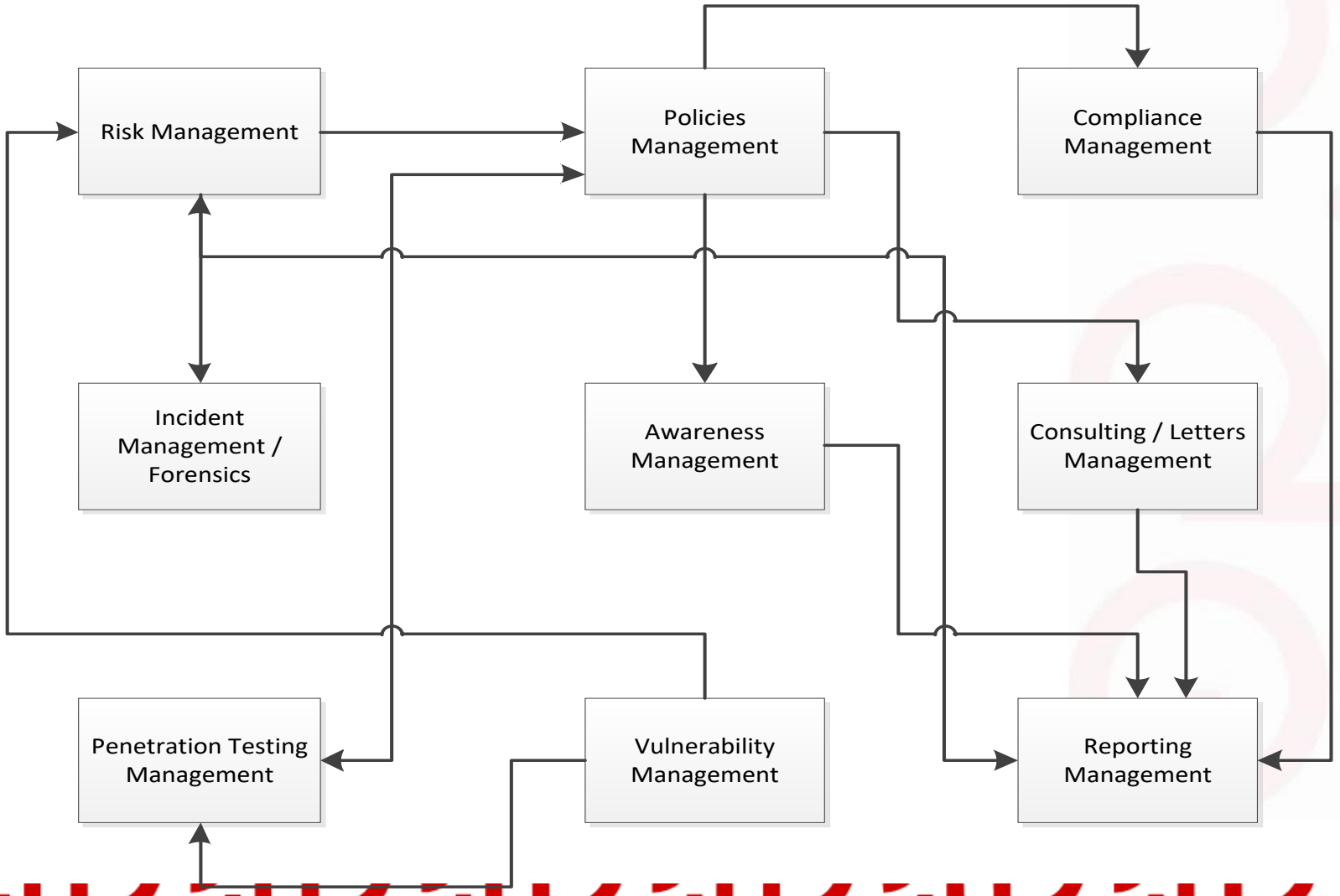
h·de
CYBER SECURITY



المدخلات الأساسية لتطوير إستراتيجية الأمن السيبراني

h·de
CYBER SECURITY

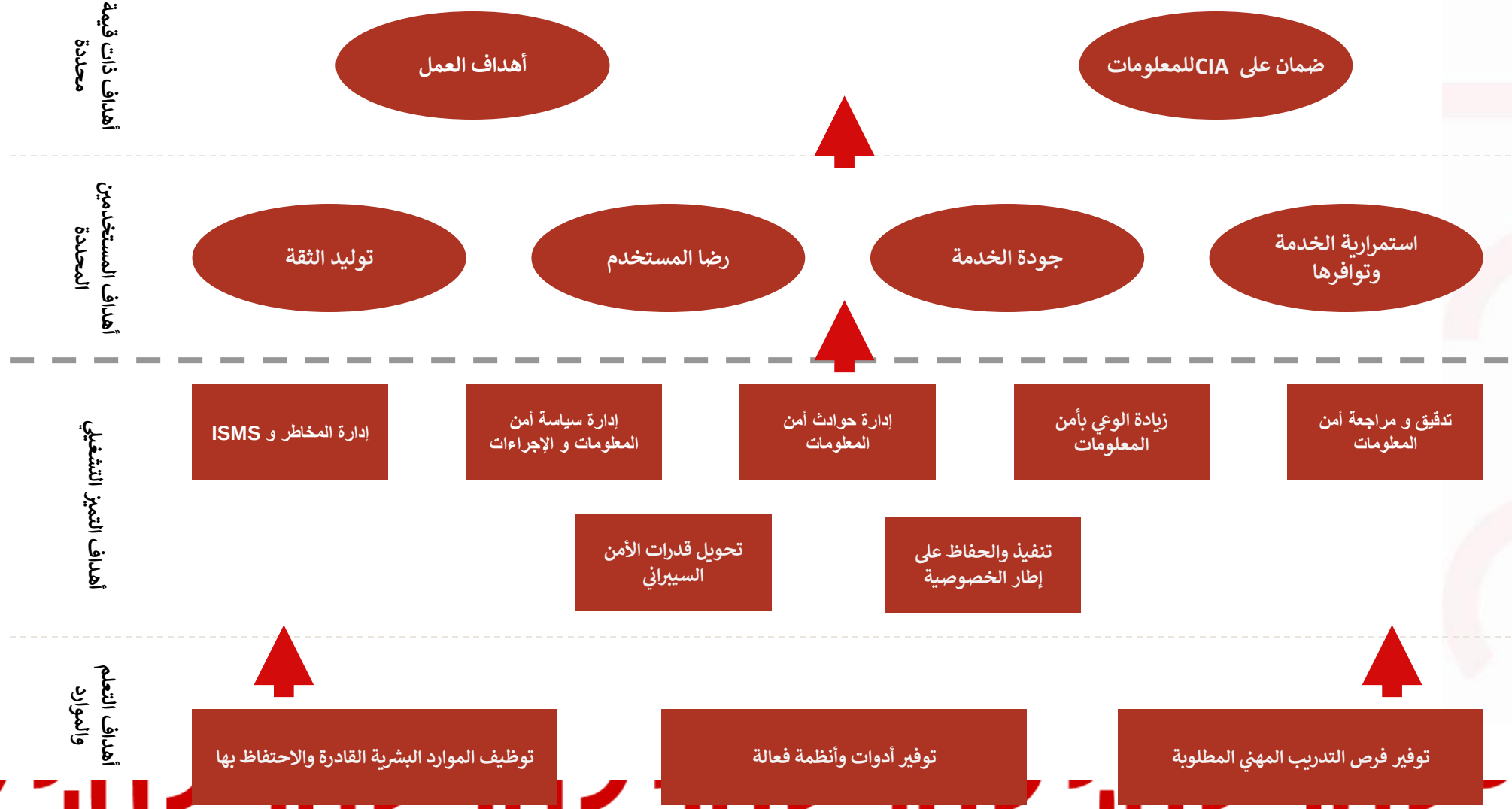
نموذج لعمليات الأعمال



تنظيم أهداف العينة لأهداف أمن المعلومات

	الهدف الاستراتيجي	الغاية الاستراتيجية	غاية الأمن السيبراني(SG)
1	إدارة المخاطر وتعزيز الأمن القومي	تعظيم الأمن	إدارة مخاطر أمن المعلومات (SG-1-1)
			إدارة سياسات وإجراءات أمن المعلومات (SG-1-2)
2	الحفاظ على التميز في الخدمة	تحسين الخدمات المقدمة للعملاء والمساهمة في الإستراتيجية	تنفيذ والحفاظ على إطار عمل الخصوصية (SG-2-1)
			زيادة الوعي بأمن المعلومات (SG-2-2)
3	تمكين الخدمات الذكية للحكومة والشركات والأفراد	توفير قدرات فعالة لدعم القرار	تحويل قدرات الأمن السيبراني (SG-3-1)
4	تعزيز المعايير والحوكمة	تحسين نضج إدارة خدمات تكنولوجيا المعلومات	إدارة حوادث أمن المعلومات (SG-4-1)
			تدقيق ومراجعة أمن المعلومات (SG-4-2)

نموذج الأهداف و الغايات (BSC)



استراتيجية الأمن السيبراني
مستند: عينة من المخرجات

الأمن السيبراني
التسلسل الهرمي للمؤسسة

الأمن السيبراني
الرؤية والرسالة

الأمن السيبراني
المبادرات وخارطة الطريق

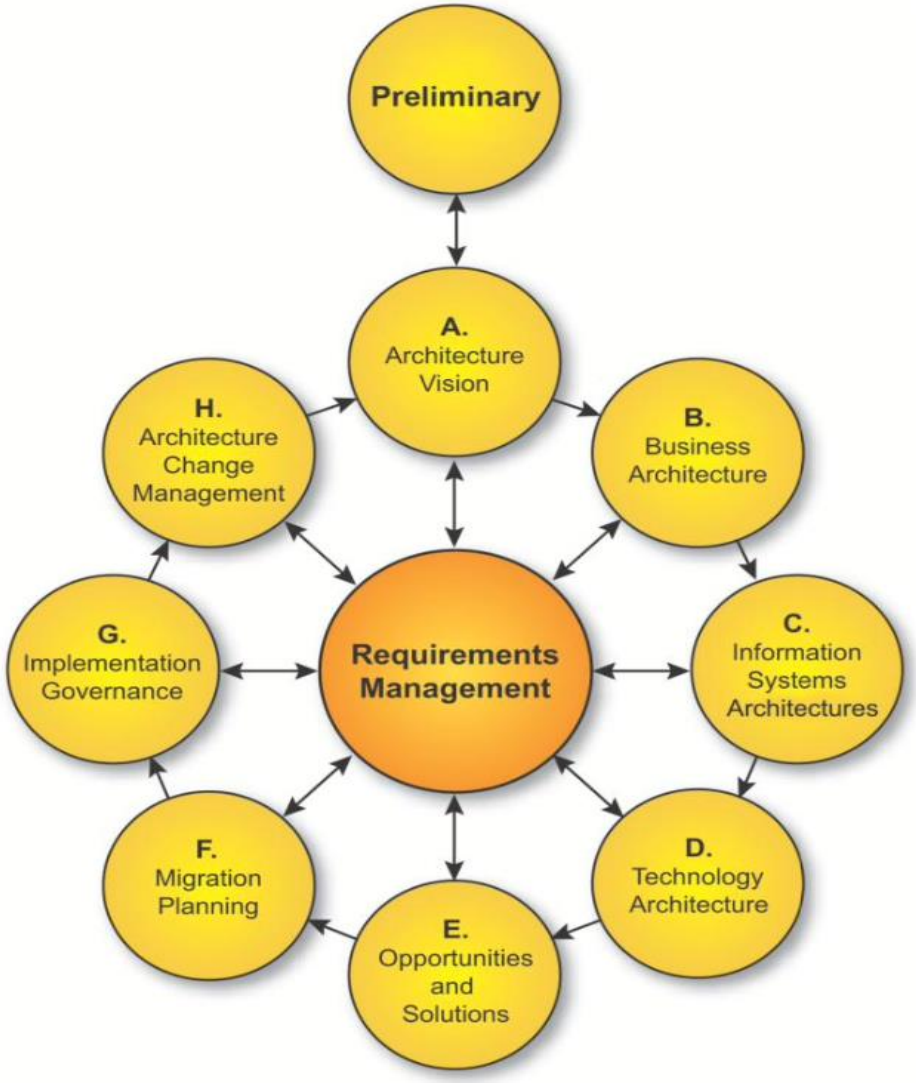
الأمن السيبراني
المهارات و الناس

الأمن السيبراني
المقاييس ، KPI، BSC

الأمن السيبراني
نموذج التشغيل

معمارية الأمن السيبراني

h·de
CYBER SECURITY



استناداً إلى TOGAF....

h·de
CYBER SECURITY

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

و مصفوفة
SABSA

CCM v4 السحابية

h·de
CYBER SECURITY

AIS	Application & Interface Security
AAC	Audit Assurance & Compliance
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control & Configuration Management
DSI	Data Security & Information Lifecycle Mgmt
DCS	Datacenter Security
EKM	Encryption & Key Management
GRM	Governance & Risk Management
HRS	Human Resources Security
IAM	Identity & Access Management
IVS	Infrastructure & Virtualization
IPY	Interoperability & Portability
MOS	Mobile Security
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management

h·de CYBER SECURITY

شركاؤنا

صندوق التنمية الوطني
NATIONAL DEVELOPMENT FUND

المركز الوطني لأمن المسافرين
National Travellers Security Center

KING KHALID UNIVERSITY

مصرف الإنماء
alinma bank

BARQ SYSTEMS

DataLexing™

إمكان
EMKAN

مستشفى قوى الأمن
SECURITY FORCES HOSPITAL
Dammam | الدمام

GCAM

الهيئة العامة للإعلام المرئي والمسموع
GENERAL COMMISSION FOR AUDIOVISUAL MEDIA

شـــــكرًا لكـــم

للـتواصل

support@hidecybersecurity.com
www.hidecybersecurity.com

HIDE

PROFESSIONAL SERVICES OFFERINGS

h·de
CYBER SECURITY

VISION

To be the Leading Cyber Security Partner for Organizations in the Gulf Region

h·de
CYBER SECURITY

MISSION

Cybersecurity Reloaded: Utilize our Skills, Experience, Honesty, and Transparency to provide Value to our Customers through Managing Cybersecurity Risks to Organizational Assets

h·de
CYBER SECURITY

Professional Services Offering

Assess

- Gap Assessments against standards
- Risk Assessments
- Cloud Security Assessments
- Application Security Assessments
- Penetration Testing / Red Teaming
- Vulnerability Assessments

Govern & Comply

- Strategy / Arch. Development
- Policies & Procedures Mgt.
- Audits
- ISO 27001: 2013
- SAMA CSF
- NCA ECC, CCC, CSCC
- CSA / STAR / FedRAMP
- ISO 22301 (BC)/ISO 27031 (DR)
- COBIT 2019
- NDMO

Cyber Defense

- Incident Response
- Cyber Forensics
- Threat Hunting
- Specialized Trainings & Human Awareness

Gap Analysis

h·de
CYBER SECURITY

ISO 27001
ISO 20000
STAR

NCA ECC
SAMA
COBIT

GAP ANALYSIS

Build Domains Framework
Analyze Gap
Assess Control Maturity

GAP ANALYSIS REPORT

Compliance Status
Recommendation
Ownership
Domain Maturity Level

h·de
CYBER SECURITY

Internal Policies
Processes

NDMO

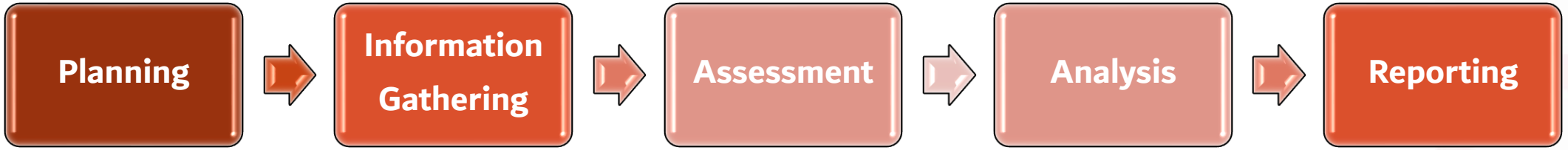
GAP ANALYSIS

Analyze Gap

NDMO Driven: Data Governance & Management Deliverables

Policies, Plans, procedures, Training
Data Governance, Mgt.
Data Quality
Data Reliability, Security, etc.

Methodology



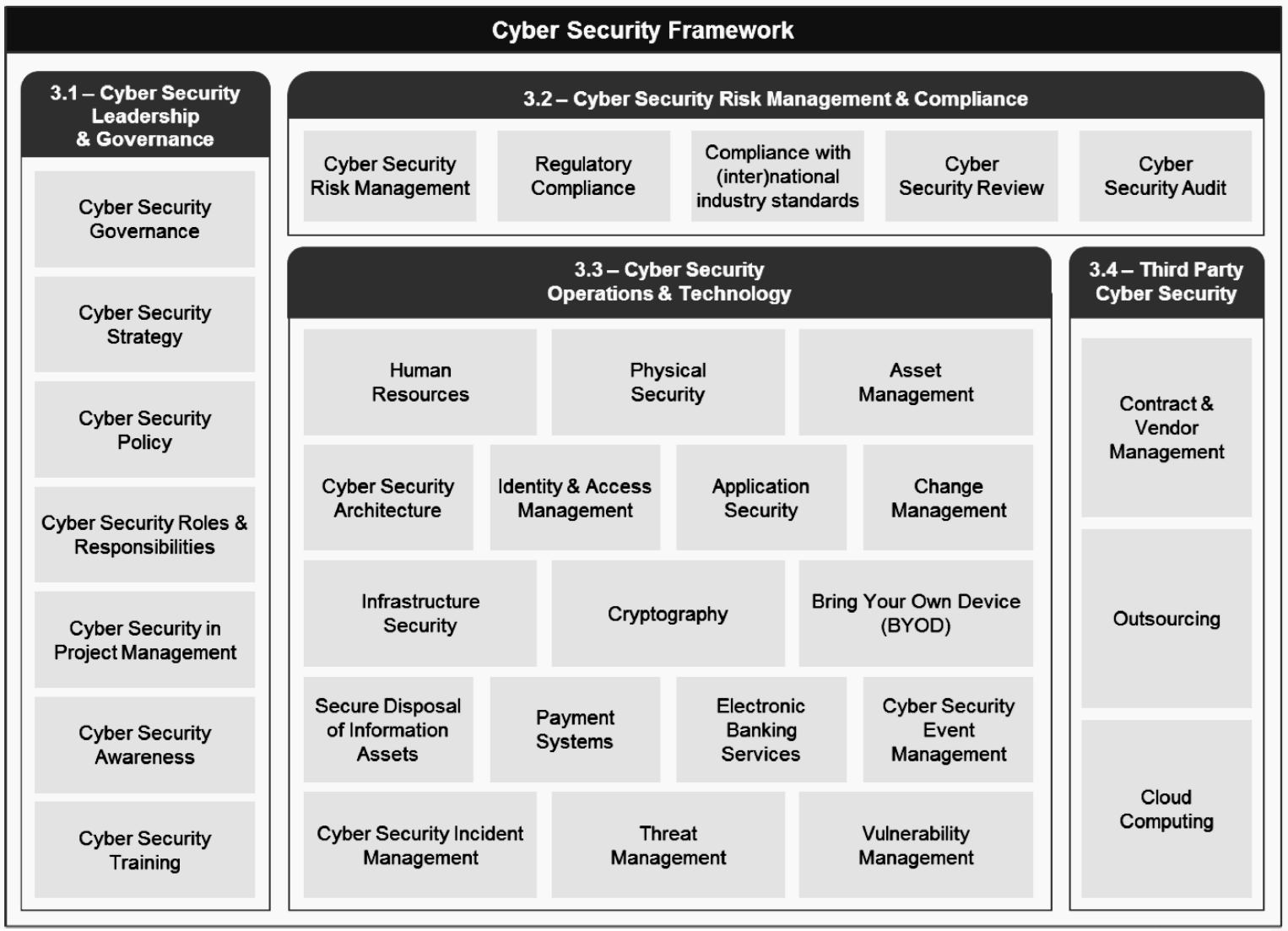
MEETINGS

OBSERVATIONS

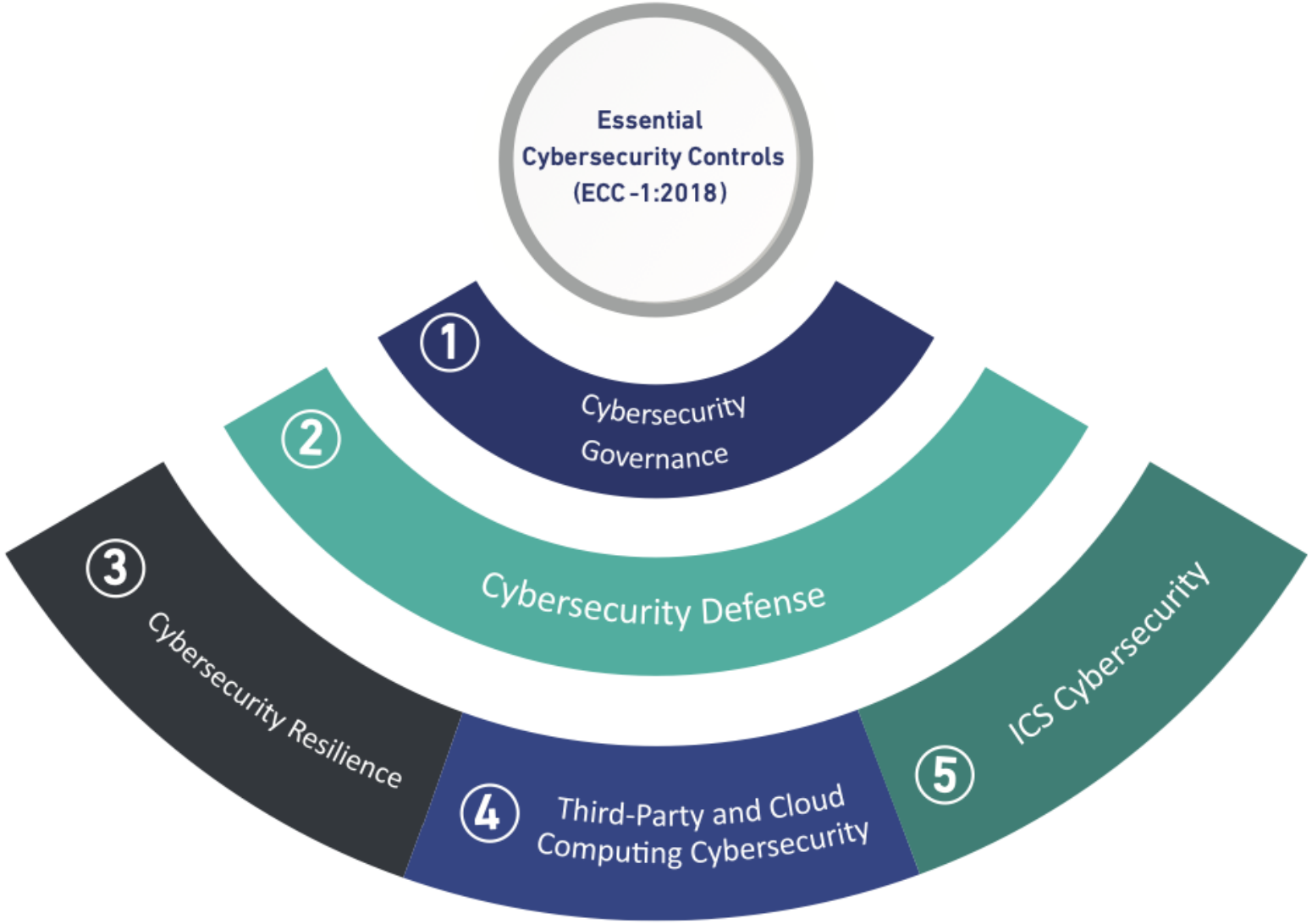
DOCUMENTATION REVIEW

OTHER BENCHMARKED STANDARDS

SAMA CSF


Cyber Security Framework
3.1 – Cyber Security Leadership & Governance
Cyber Security Governance
Cyber Security Strategy
Cyber Security Policy
Cyber Security Roles & Responsibilities
Cyber Security in Project Management
Cyber Security Awareness
Cyber Security Training
3.2 – Cyber Security Risk Management & Compliance
Cyber Security Risk Management
Regulatory Compliance
Compliance with (inter)national industry standards
Cyber Security Review
Cyber Security Audit
3.3 – Cyber Security Operations & Technology
Human Resources
Physical Security
Asset Management
Cyber Security Architecture
Identity & Access Management
Application Security
Change Management
Infrastructure Security
Cryptography
Bring Your Own Device (BYOD)
Secure Disposal of Information Assets
Payment Systems
Electronic Banking Services
Cyber Security Event Management
Cyber Security Incident Management
Threat Management
Vulnerability Management
3.4 – Third Party Cyber Security
Contract & Vendor Management
Outsourcing
Cloud Computing

h·de
CYBER SECURITY



h·de
CYBER SECURITY

The NIST Cybersecurity Framework

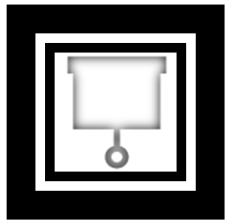
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements

The GAF (Gap Analysis Framework)

Governance & Compliance

Security Architecture

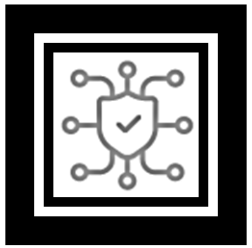
Risk Management



Training & Awareness

Endpoint Security

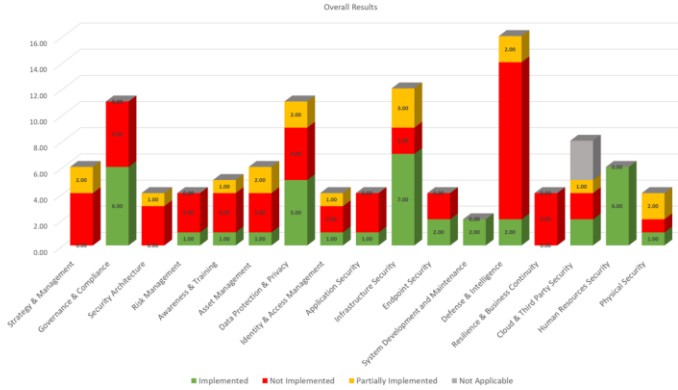
Application Security

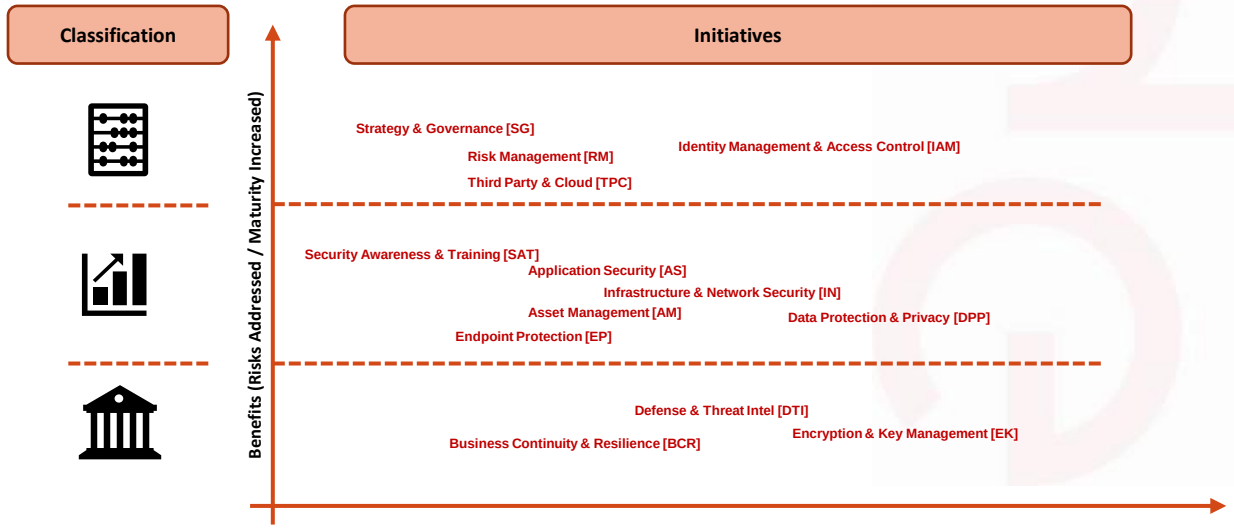


Defense & Intel

Sample Outputs

Overall Results					
Cybersecurity Domains	Implemented	Not Implemented	Partially Implemented	Not Applicable	TOTAL
Strategy & Management	0.00	4.00	2.00	0.00	6.00
Governance & Compliance	6.00	5.00	0.00	0.00	11.00
Security Architecture	0.00	3.00	1.00	0.00	4.00
Risk Management	1.00	3.00	0.00	0.00	4.00
Awareness & Training	1.00	3.00	1.00	0.00	5.00
Asset Management	1.00	3.00	2.00	0.00	6.00
Data Protection & Privacy	5.00	4.00	2.00	0.00	11.00
Identity & Access Management	1.00	2.00	1.00	0.00	4.00
Application Security	1.00	3.00	0.00	0.00	4.00
Infrastructure Security	7.00	2.00	3.00	0.00	12.00
Endpoint Security	2.00	2.00	0.00	0.00	4.00
System Development and Maintenance	2.00	0.00	0.00	0.00	2.00
Defense & Intelligence	2.00	12.00	2.00	0.00	16.00
Resilience & Business Continuity	0.00	4.00	0.00	0.00	4.00
Cloud & Third Party Security	2.00	2.00	1.00	3.00	8.00
Human Resources Security	6.00	0.00	0.00	0.00	6.00
Physical Security	1.00	1.00	2.00	0.00	4.00
TOTAL	38.00	53.00	17.00	3.00	111.00
PERCENTAGE	34.23%	47.75%	15.32%	2.70%	

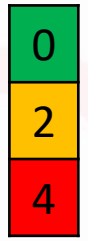




Sample Outputs

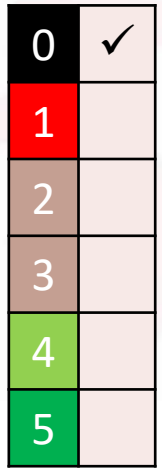
DESCRIPTION
A Cybersecurity strategy must be defined , documented, approved and supported by the head of the organization. The strategy goals must be in line with the rules and regulations. A road map must be in place to implement the strategy.
A Cybersecurity steering committee must be established, and the committee member's roles and responsibilities must be defined, documented and approved. The head of the Cybersecurity must be included as a member of the committee and the committee should report directly to the organization head.

G-SM



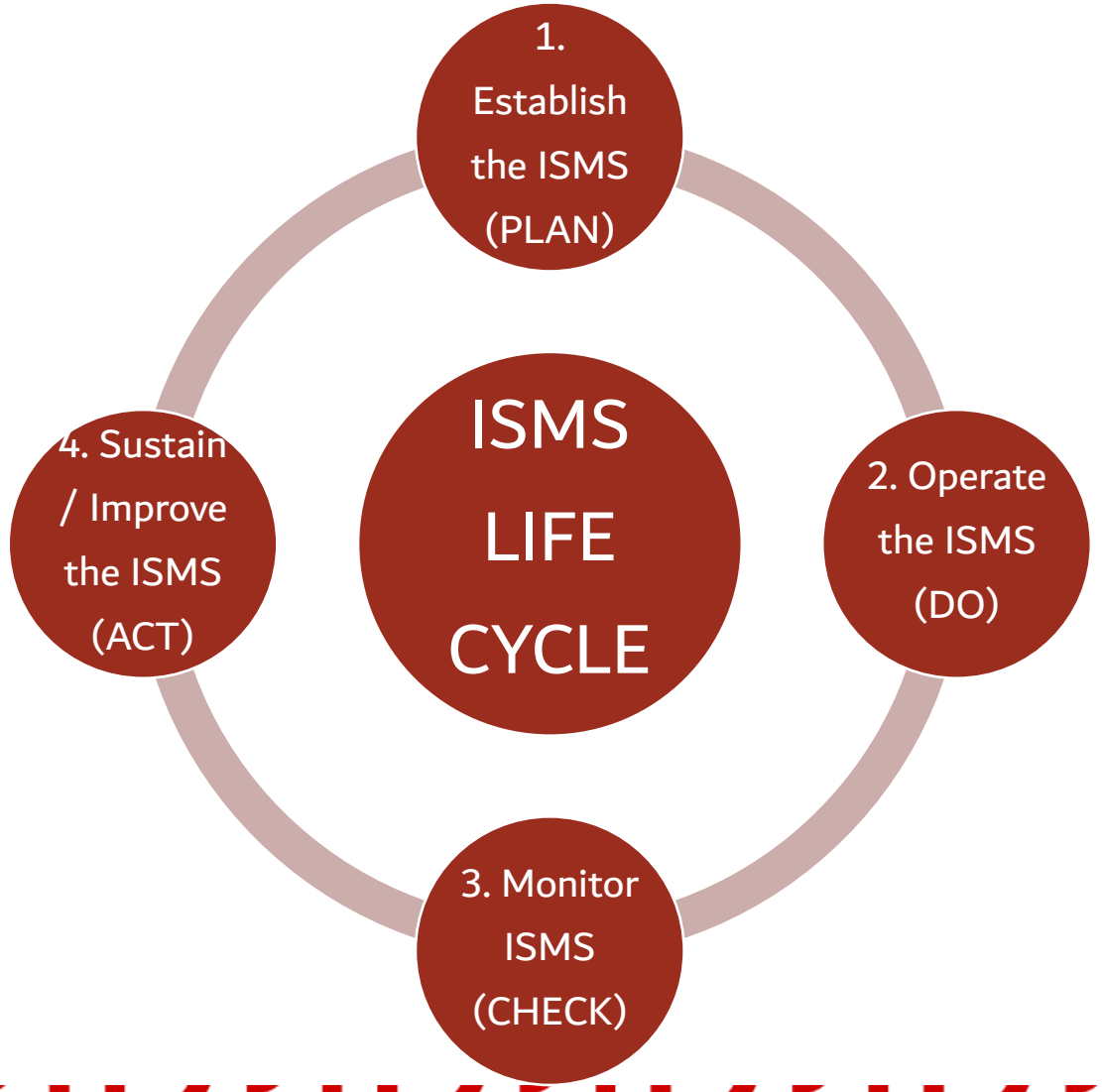
Current Maturity Level	0 [Non-Existent]	**Target Maturity Level**	4 [Transformed] | 2 Years

Highs	Enterprise Strategy in Progress. Cybersecurity strategy soon to be developed
Lows	No Overarching Strategy to guide and steer Cybersecurity initiatives Were ISO 27001 certified; however, certification has expired. Implementation Lacking



h·de
CYBER SECURITY

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)



ISMS Implementation Approach

h·de
CYBER SECURITY

Establish the ISMS

Operate the ISMS

Monitor the ISMS

Improve the ISMS

1. Define Information Security Policy
2. Define Scope of ISMS
3. Information Assets Identification & Evaluation
4. Determine Risk
5. Identify Controls

1. Define & Publish Policies, Procedures, Standards
2. Controls Implementation, Awareness, Training

1. Internal Audit
2. Management Review of ISMS

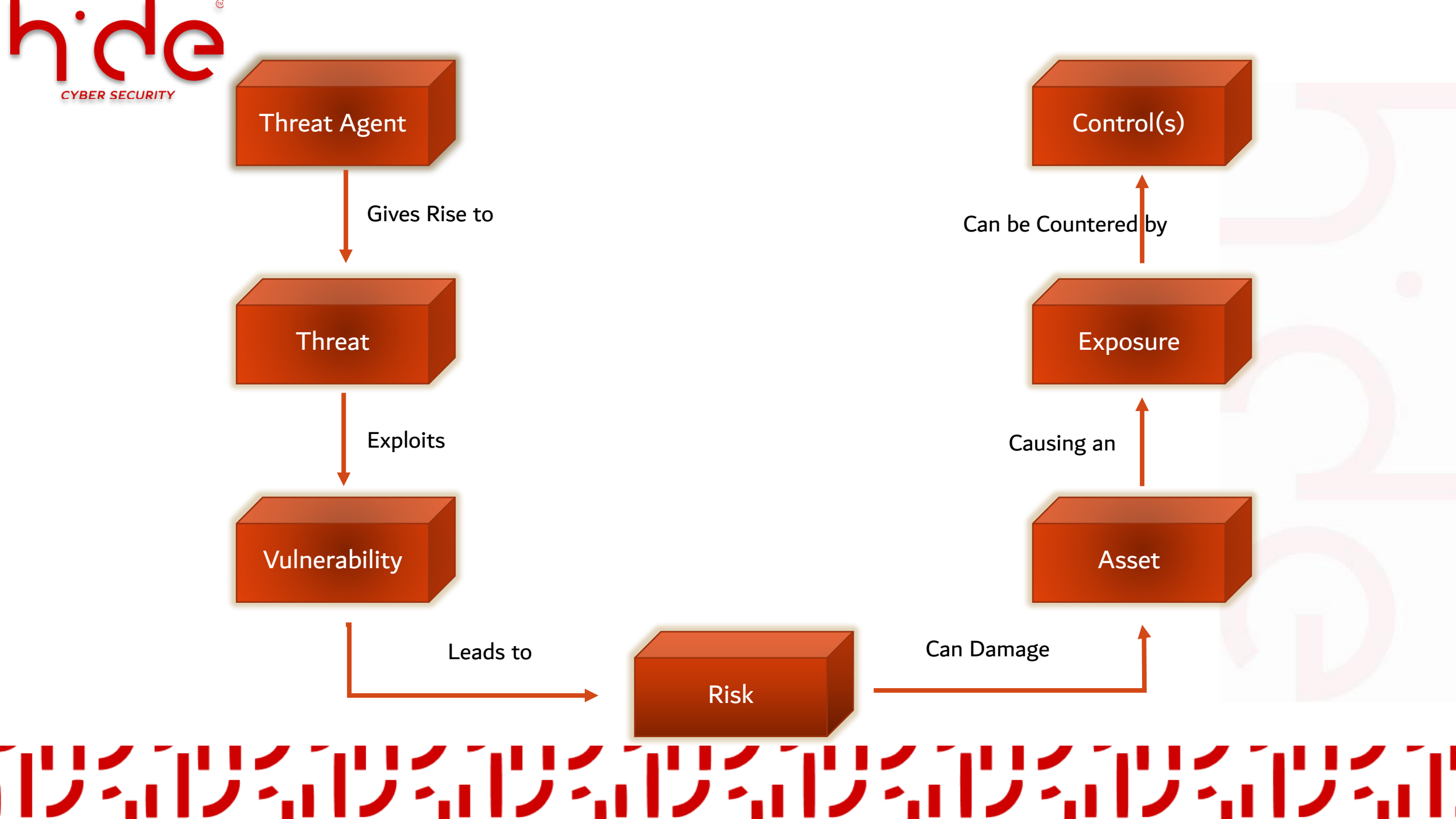
1. Take Corrective / Preventive Action (CAPA)

1. External Audit for Certification

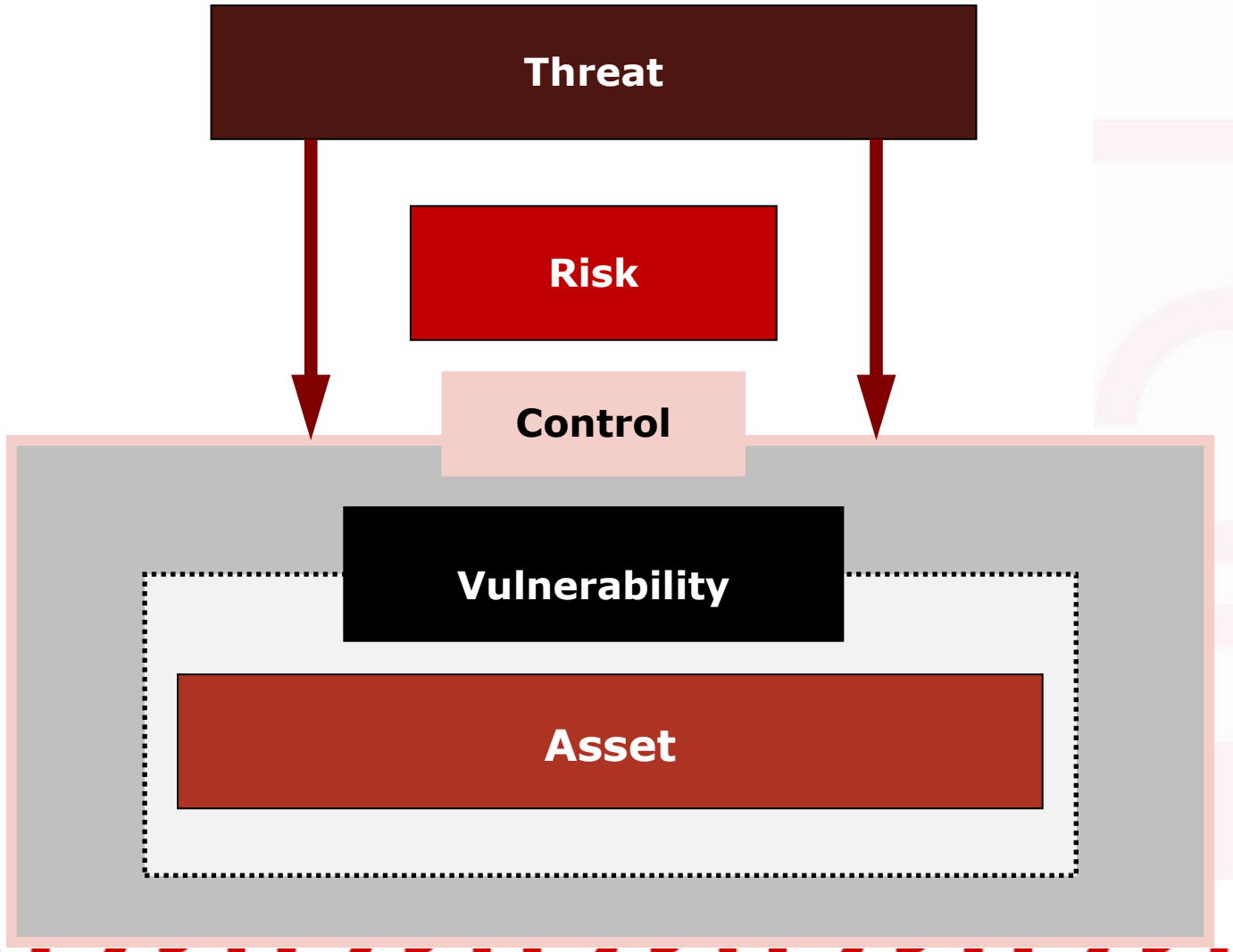
RISK MANAGEMENT

Risk [Noun]

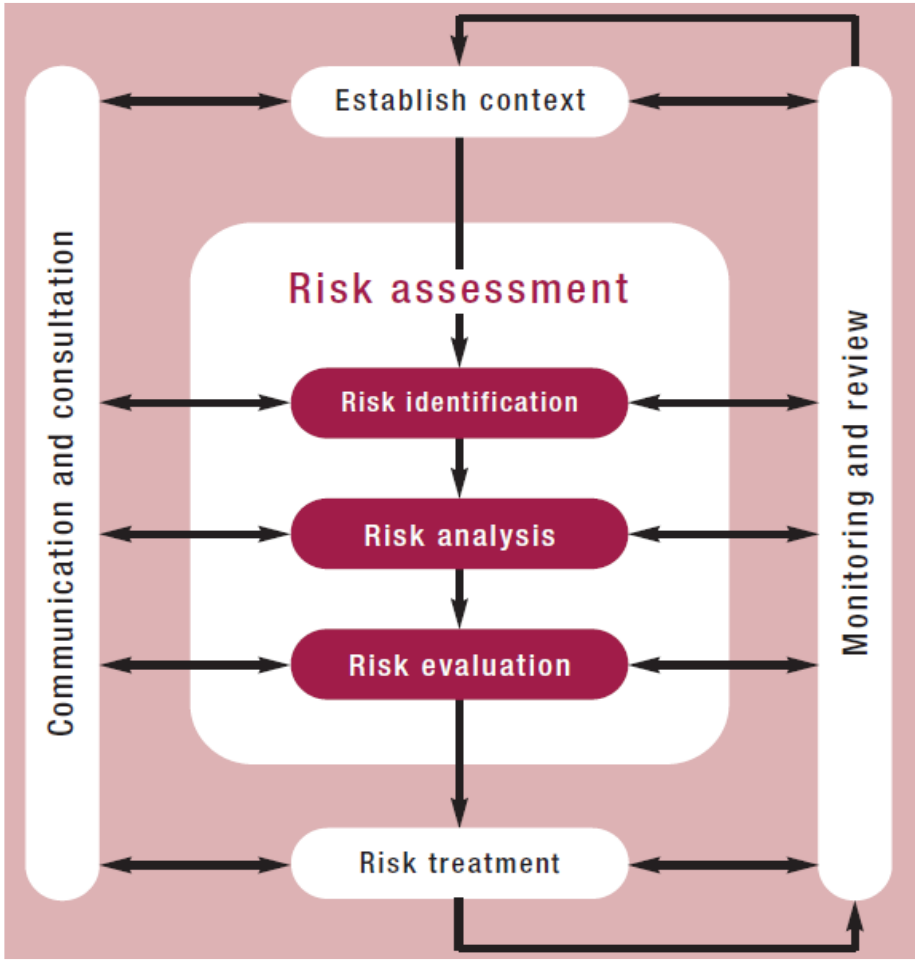
- A situation involving exposure to danger.


Threat Agent
Gives Rise to
Threat
Exploits
Vulnerability
Leads to
Risk
Can Damage
Asset
Causing an
Exposure
Can be Countered by
Control(s)

RISK



ISO 31000
ISO/IEC
27005:2011

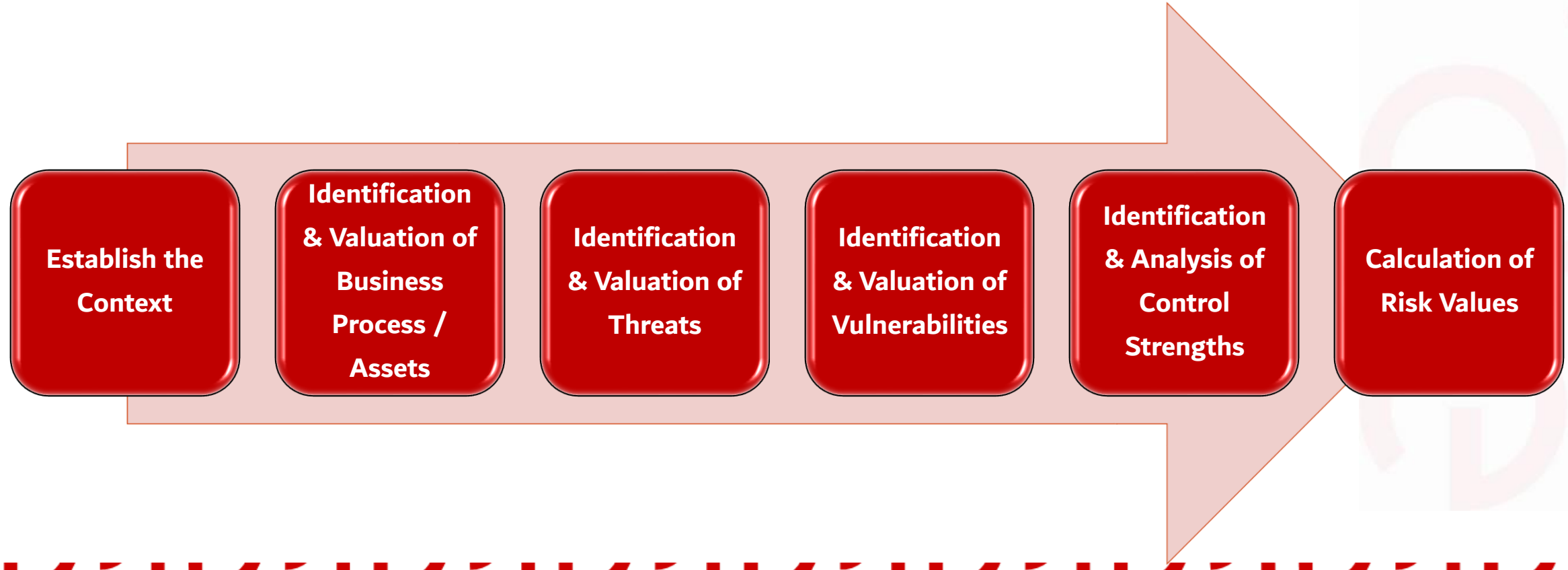


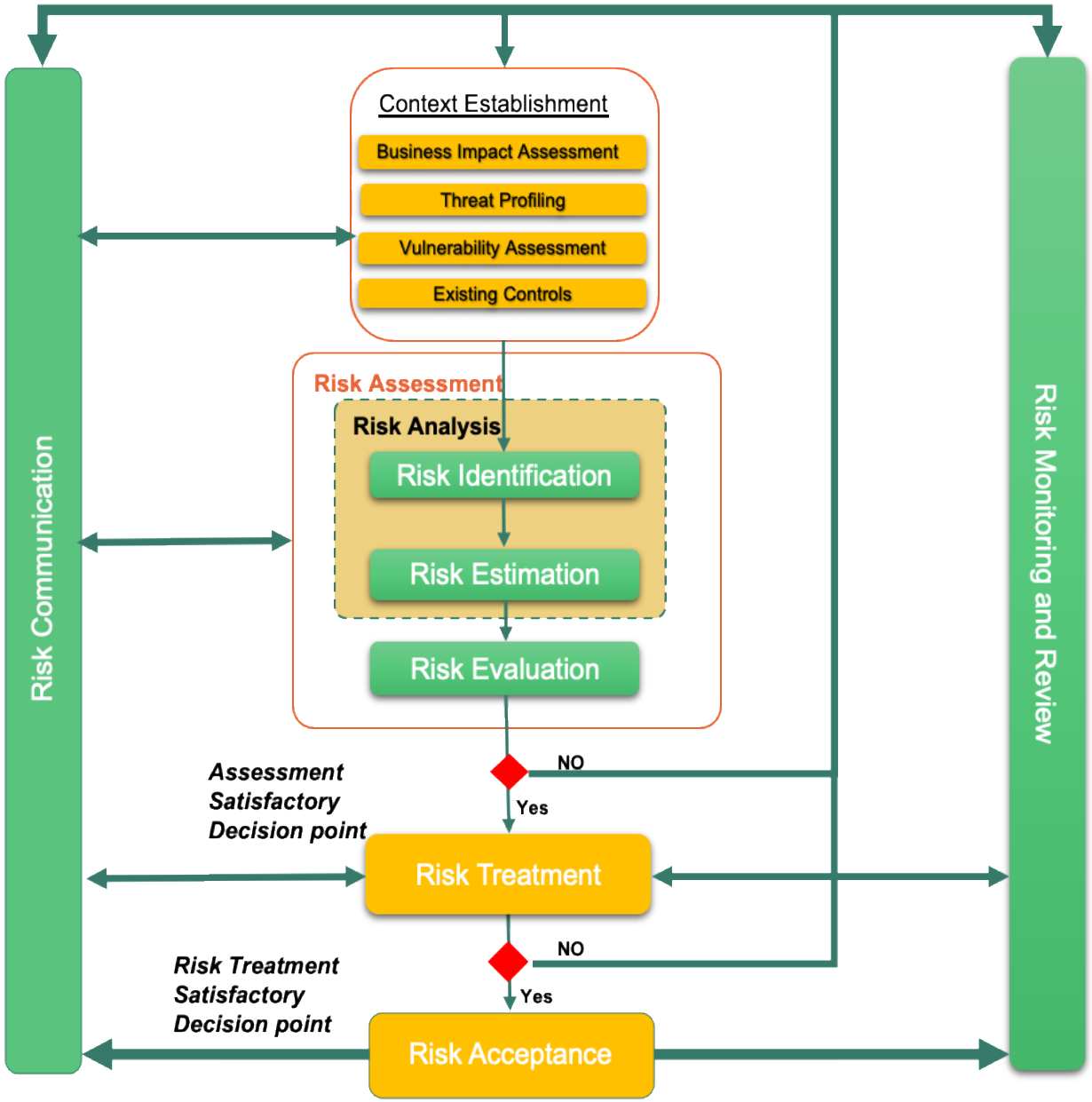

Inherent Risk
Risk without taking into account any risk response
Current Risk
Actual risk today, i.e., inherent risk with current risk responses applied
Residual Risk
Equal to current risk with additional risk responses applied; additional risk responses are identified based on risk analysis of current risk

Risk Management Methodology

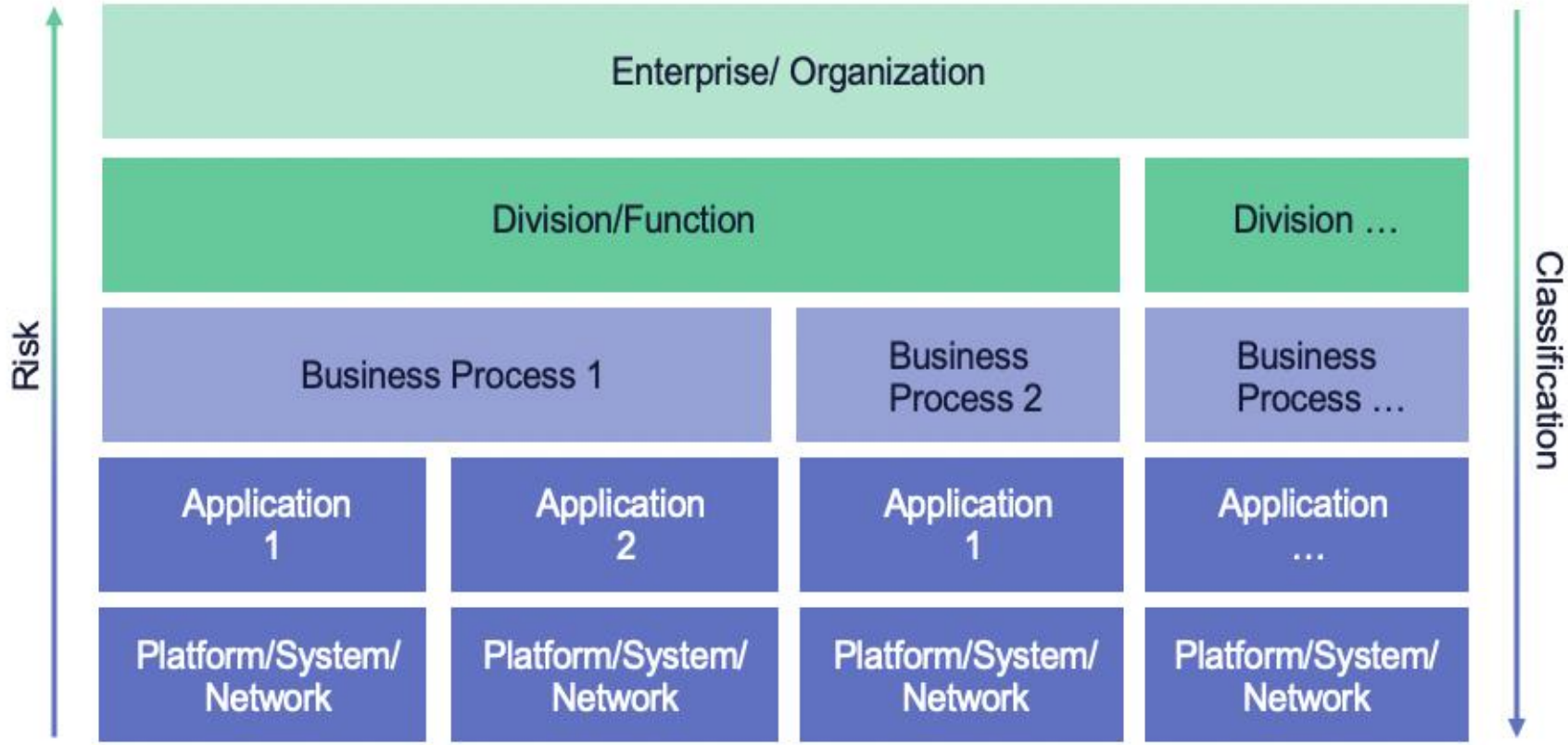

Risk Management Policy
• Risk Appetite
Risk Assessment Methodology
Risk Assessment procedure
Reference Catalogs
• Relevant threats
• Relevant vulnerabilities
• Applicable controls
Resources
• Requester
• Assessor
• External resources
Communication
Monitoring
Risk Management Framework

The Risk Assessment Process




Context Establishment
Business Impact Assessment
Threat Profiling
Vulnerability Assessment
Existing Controls
Risk Assessment
Risk Analysis
Risk Identification
Risk Estimation
Risk Evaluation
Risk Communication
Risk Monitoring and Review
Assessment Satisfactory Decision point
NO
Yes
Risk Treatment
Risk Treatment Satisfactory Decision point
NO
Yes
Risk Acceptance

Risk & Classification Context



Sample Calculations

Threat Valuation

Threat Score			Likelihood					
			Unlikely	1	Could happen	2	Very likely	3
Impact	Low	1	1		2		3	
	Medium	2	2		4		6	
	High	3	3		6		9	
	Very High	4	4		8		12	

Threat Score	Threat Value	
1	Low	1
2		
3		
4	Medium	2
5		
6		
7	High	3
8		
9		
10	Very High	4
11		
12		

Vulnerability Value

Ease of Exploitation	Vulnerability Value	
Very Difficult	Low	1
Difficult	Medium	2
Easy	High	3
Very Easy	Very High	4

Risk Calculation BASELINE = 8

risk score = asset value x threat value x vulnerability value

	Threat Value	Low				Medium				High				Very High			
	Vulnerability Value	L	M	H	VH	L	M	H	VH	L	M	H	VH	L	M	H	VH
Asset Value	Low	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
	Medium	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
	High	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
	Very High	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

risk value = risk score / control strength

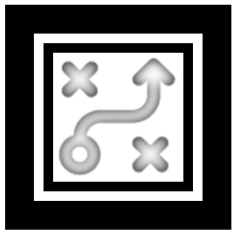
1	2	3	4	6	8	9	12	16	18	24	27	32	36	48	64

Acceptable Risks

Non Acceptable Risks

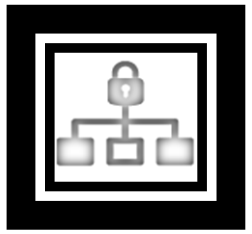
Prioritization of Non Acceptable Risks	
Low	1 to 11
Medium	12 to 23
High	24 to 31
Very High	32 to 64

The UCF (Unified Control Framework)



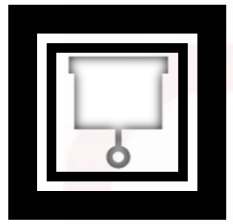
Strategy & Management

Governance & Compliance



Security Architecture

Risk Management



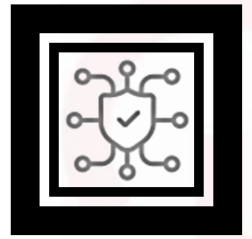
Training & Awareness

Endpoint Security

Data Protection & Privacy

Identity & Access Management

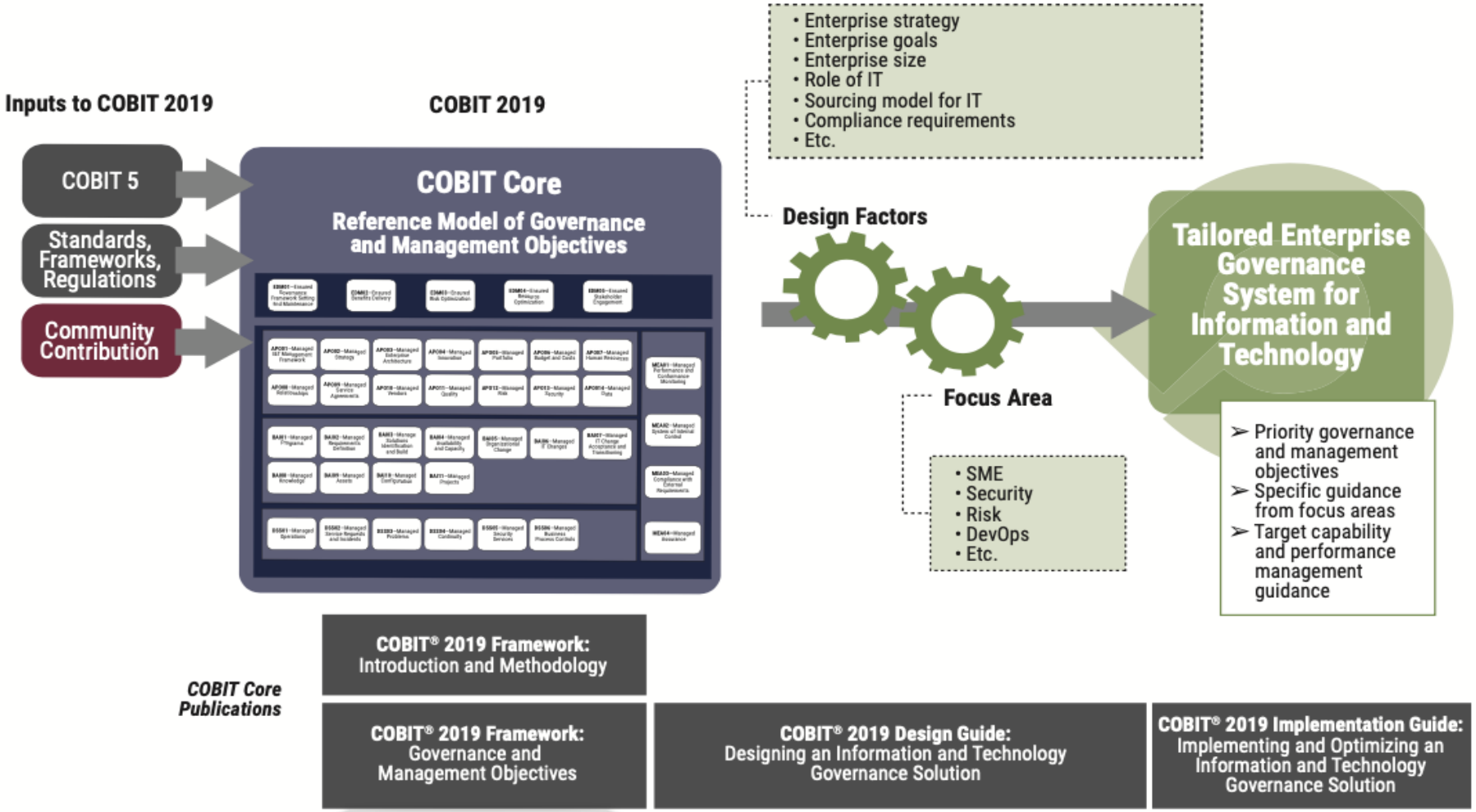
Application Security



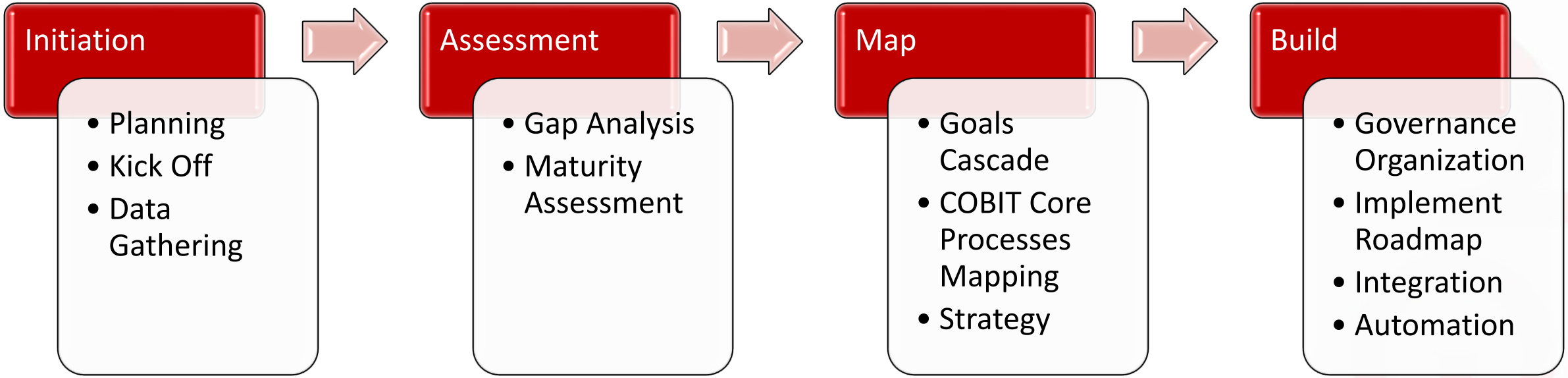
Defense & Intel

GOVERNANCE OF ENTERPRISE IT

COBIT 2019


Inputs to COBIT 2019
COBIT 2019
COBIT 5
Standards, Frameworks, Regulations
Community Contribution
COBIT Core
Reference Model of Governance and Management Objectives
• Enterprise strategy
• Enterprise goals
• Enterprise size
• Role of IT
• Sourcing model for IT
• Compliance requirements
• Etc.
Design Factors
Focus Area
• SME
• Security
• Risk
• DevOps
• Etc.
Tailored Enterprise Governance System for Information and Technology
➢ Priority governance and management objectives
➢ Specific guidance from focus areas
➢ Target capability and performance management guidance
COBIT Core Publications
COBIT® 2019 Framework: Introduction and Methodology
COBIT® 2019 Framework: Governance and Management Objectives
COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution
COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution

Methodology



Evaluate, Direct & Monitor

- EDM01 Ensure Governance framework setting & maintenance
- **EDM02 Ensure Benefits Delivery**
- EDM03 Ensure Risk Optimization
- EDM04 Ensure Resource Optimization
- EDM05 Ensure Stakeholder transparency

Align, Plan & Organize

- **APO01 Manage the IT Management Framework**
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- **APO08 Manage Relationships**
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- APO12 Manage Risk
- **APO13 Manage Security**

Build, Acquire & Implement

- **BAI01 Manage Programs & Projects**
- BAI02 Manage Requirement Definition
- BAI03 Manage Solutions Identification & build
- BAI04 Manage Availability & Capacity
- BAI05 Manage Organizational Change enablement
- BAI06 Manage Changes
- BAI07 Manage Change acceptance & transitioning
- BAI08 Manage knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

Deliver, Service & Support

- DSS01 Manage Operations
- DSS02 Manage service requests & incidents
- DSS03 Manage problems
- DSS04 Manage Continuity
- DSS05 Manage Security services
- DSS06 Manage business process controls

Compliance

- 75-100 %
- 50-74 %
- 25-49%
- 1- 24%
- % 0

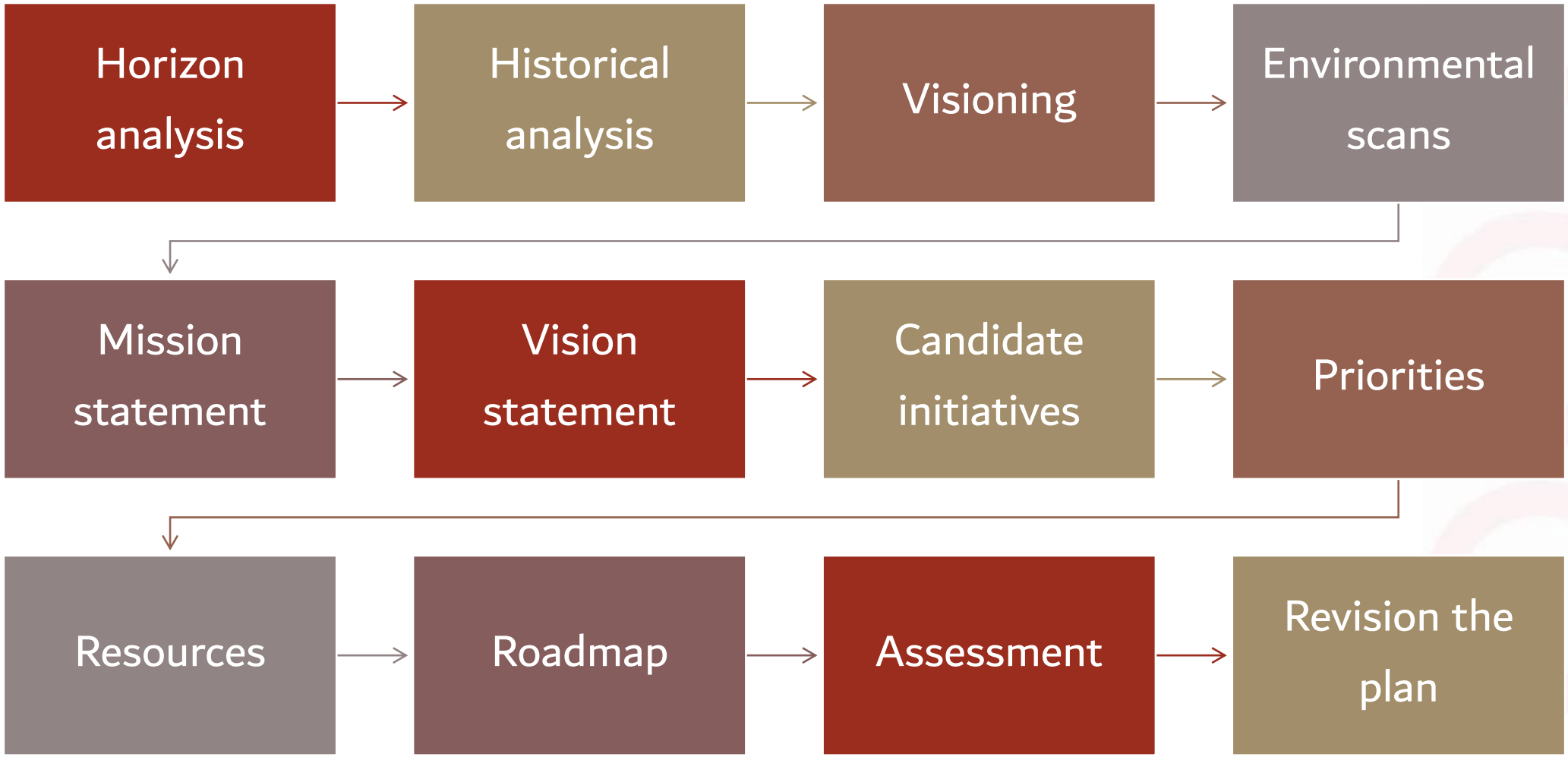
Monitor, Evaluate & Assess

- MEA01 Monitor, Evaluate & Assess Conformance and Performance
- MEA02 Monitor, evaluate & assess the system of internal control
- MEA03 Monitor, evaluate & assess compliance with external requirements

Cyber Security Strategy Development

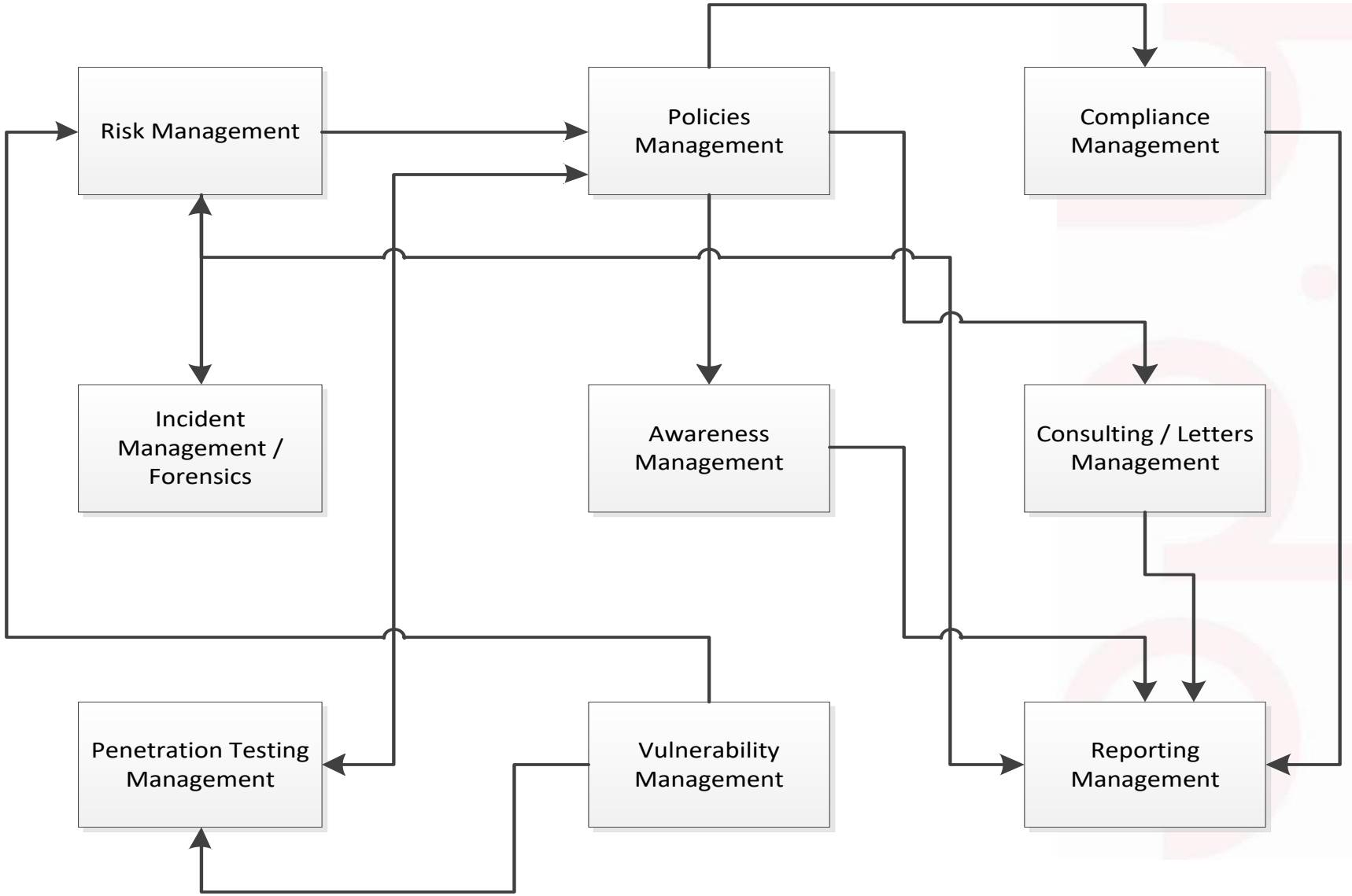
strat·e·gy: a plan, method, or series of manoeuvres or stratagems for obtaining a specific goal or result

Strategic planning steps



Primary Inputs to Cybersecurity Strategy Development

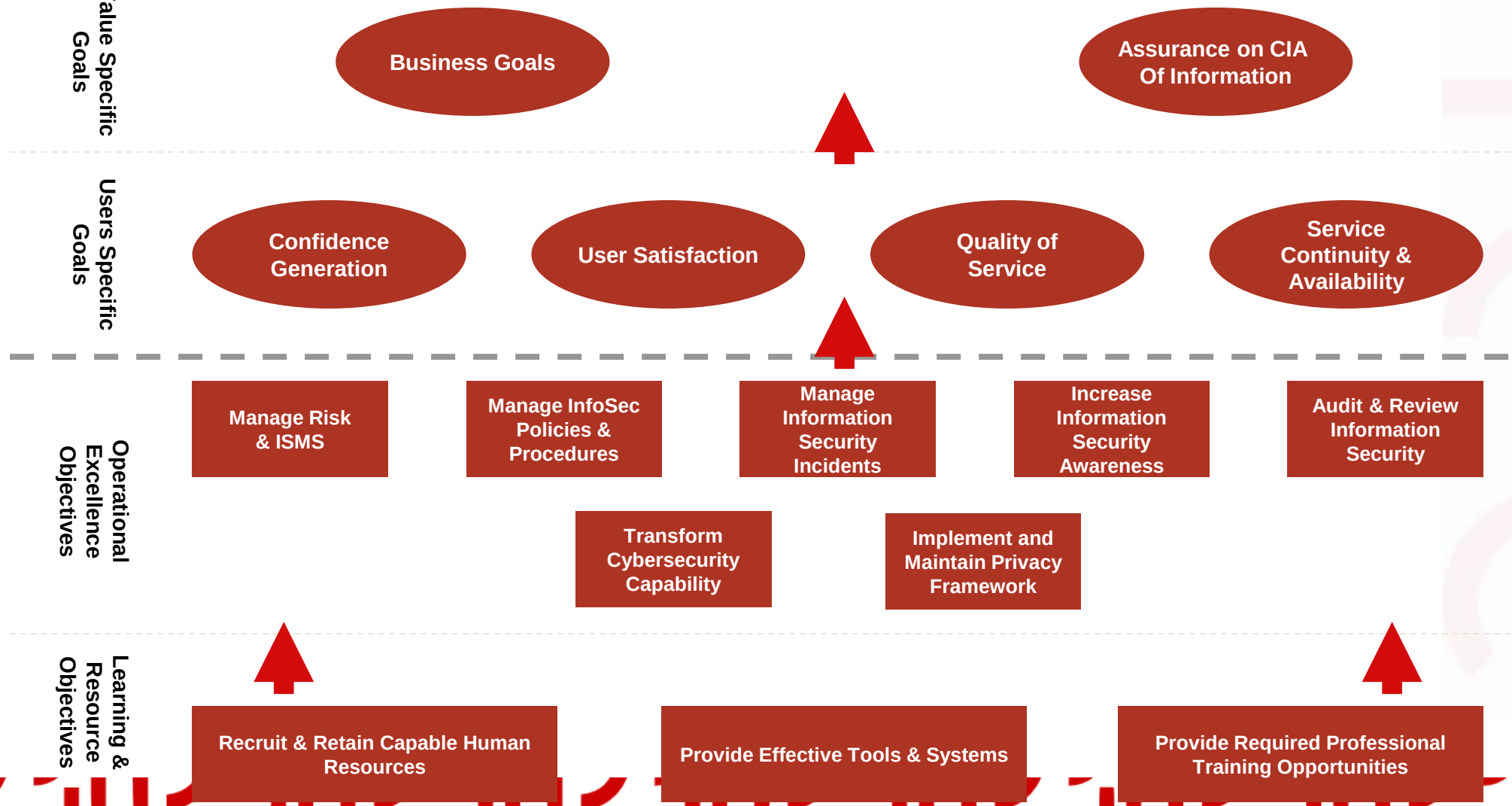
Sample Business Processes



Sample Goals Cascade to InfoSec Objectives

S. No.	STRATEGIC GOAL	STRATEGIC OBJECTIVE	CYBER SECURITY OBJECTIVE (SG)
1	Manage Risk and Maximize National Security	Maximize security	Manage Information Security Risk (SG-1-1)
			Manage Information Security Policies and Procedures (SG-1-2)
2	Maintain Excellence in Service	Improve services to customers and contribute to the strategy	Implement and Maintain Privacy Framework (SG-2-1)
			Increase Information Security Awareness (SG-2-2)
3	Enable Smart Services to Government, Business & Individuals	Provide effective decision support capabilities	Transform Cybersecurity Capability (SG-3-1)
4	Strengthen Standards and Governance	Improve IT service management maturity	Manage Information Security Incidents (SG-4-1)
			Audit and Review Information Security (SG-4-2)

Sample Objectives & Goals (BSC)



Cybersecurity Strategy Document: Sample Output

Cybersecurity
Vision & Mission

Cybersecurity
Organization Hierarchy

Cybersecurity
People & Skills

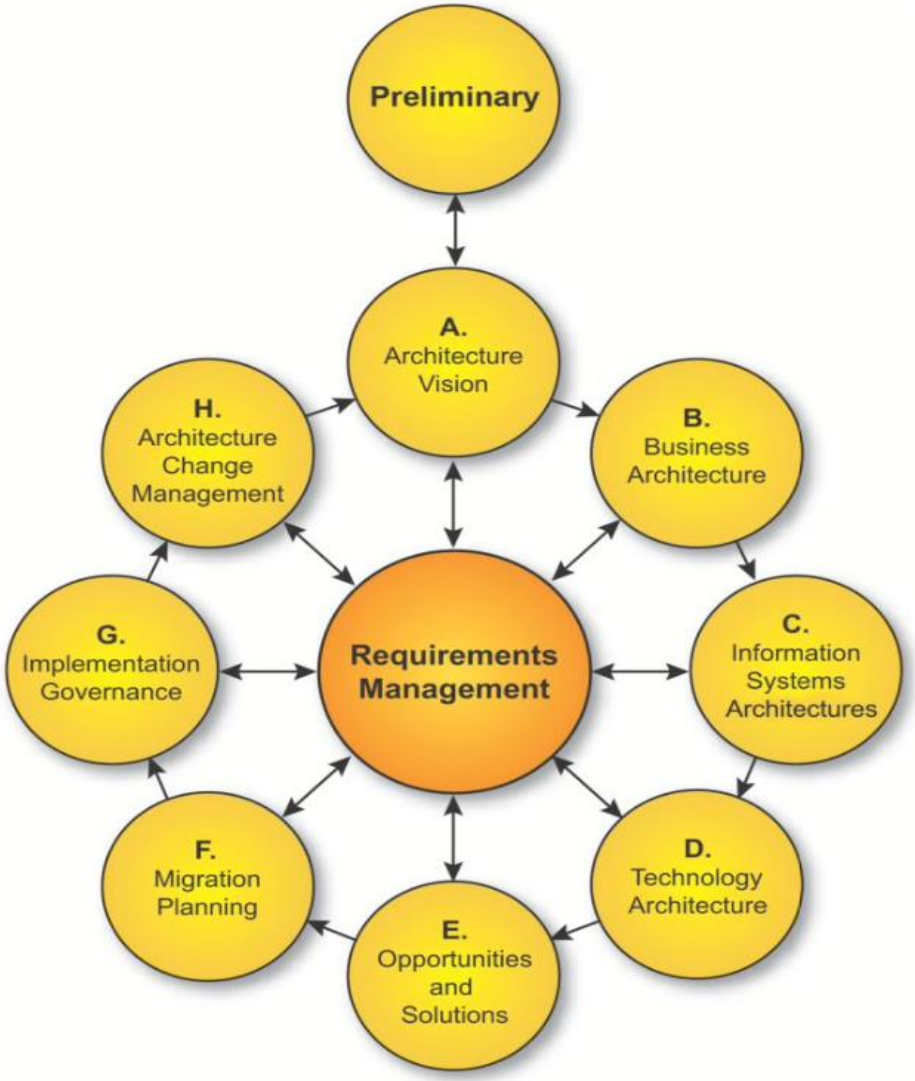
Cybersecurity
Initiatives & Roadmap

Cybersecurity
Operating Model

Cybersecurity
Metrics, KPI, BSC

Cybersecurity Architecture

Based On TOGAF…



h·de
CYBER SECURITY

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

& The SABSA Matrix

Cloud CCM v4

h·de
CYBER SECURITY

AIS	Application & Interface Security
AAC	Audit Assurance & Compliance
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control & Configuration Management
DSI	Data Security & Information Lifecycle Mgmt
DCS	Datacenter Security
EKM	Encryption & Key Management
GRM	Governance & Risk Management
HRS	Human Resources Security
IAM	Identity & Access Management
IVS	Infrastructure & Virtualization
IPY	Interoperability & Portability
MOS	Mobile Security
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management

h·de CYBER SECURITY

Our Partners

صندوق التنمية الوطني
NATIONAL DEVELOPMENT FUND

المركز الوطني لأمن المسافرين
National Travellers Security Center

KING KHALID UNIVERSITY

مصرف الإنماء
alinma bank

BARQ SYSTEMS

DataLexing™

إمكان
EMKAN

مستشفى قوى الأمن
SECURITY FORCES HOSPITAL
Dammam | الدمام

GCAM

الهيئة العامة للإعلام المرئي والمسموع
GENERAL COMMISSION FOR AUDIOVISUAL MEDIA

Thank you for your attention

For Contact

support@hidecybersecurity.com
www.hidecybersecurity.com