ERM MASTERCLASS

Date: 21st May, 2021

Venue: Virtual

Presented by: CPA Dr. Hillary Wachinga

Trainer's profile - Hillary

Dr. Hillary is an audit, risk and governance professional with 15 years work experience gained from the Big 4, banking, insurance and reinsurance sectors.

Hillary holds PhD in Strategic Information Systems, a masters in information systems and a BSc Computer Science – all from the university of Nairobi. He is also a CPA(K), CISA, CISA, CRISC, CISM, CIA(1), CCA and CERM.

Hillary is grateful to ICPAK for the opportunity to share knowledge with you.

Contacts: T: +254 725 709 390, E: hillary.Wachinga@gmail.com

Training Program

TIME	MODULE	TOPICS	KEY AREAS TO BE COVERED	FACILITATOR
LUNCH BREAK 13.00-14. 00p.m				
14.00-16.00pm	Moving Forward	ERM Human Capital and Positioning of the role in public and private sector Emerging issues in ERM Future and adequacy of risk management	• Risk maturity assessment models and alignment of risk to corporate strategies • The evolving risk landscape and adaptation – economic, regulatory and technology • Creating resilience and flexibility in risk management frameworks • Proposed risk models for the future	CPA Dr. Hillary Wachinga *Risk Consultant*

Areas of focus

1

ERM Human Capital and Positioning of the Role in Public and Private Sector

- Ideal resource requirements
- Ideal placement in an organogram for effectiveness
- Legal and regulatory frameworks on positioning of ERM

2

Emerging Issues in ERM

- Evolving risk landscape and adaptation – economic, regulatory and technological
- Creating resilience and flexibility in risk management frameworks

3

Future and adequacy of Risk Management

- Proposed risk models for the future
- Risk maturity assessment models and alignment of risk management to corporate strategies

ERM Human Capital

Background:

- ❑ Effectiveness and efficiency of ERM pegged on human capital
- ❑ Competitive edge from ERM increase with adequate human capital
- ❑ Human as the weakest (and strongest) link in risk management
- ❑ Right resource, right positioning, doing right job in the right way at the right time.
- ❑ ERM not limited to ERM dept but across the enterprise (*corporate risk culture*)

ERM Human Capital

Requirements:

- Rapidly changing risk profiles – business models, technology, regulation, pandemic, etc
- What is needed: change in skills at personal level and in risk management approach .
- Forward-looking/visionary, leadership, management, business acumen (to identify potential risks and opportunities), analytical, agile, etc
- Performance management aligned to ERM objectives

Positioning of ERM

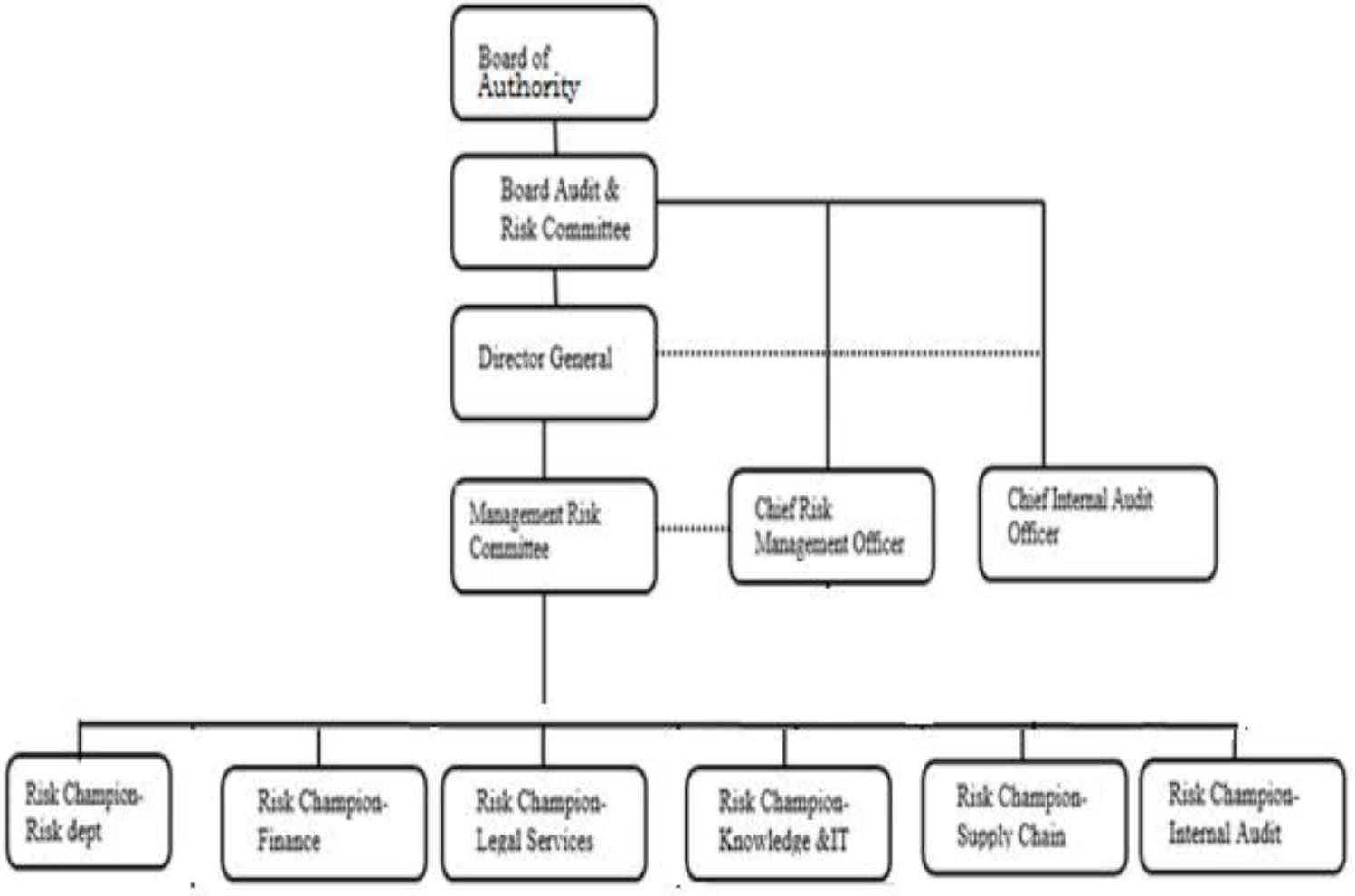
- Strategic leadership – align HC strategies to business strategies
- Strategic workforce planning (SWP)- embedding HC objectives to corporate strategy conscious of ERM objectives (*SWP maturity model*).
- Maximizing likelihood of meeting corporate and business objectives (*beyond ERM framework to ERM capabilities*)

Positioning of ERM

- (Consider) placing ERM at senior management level – functionally report to the Board and administratively to CEO
- 2nd level of defense – a balancing act (maintain some element of independence whilst adding value)
- Aim is to enhance ERM capabilities across the enterprise and ERM function influence corporate decision-making

Positioning of ERM

Example:



Positioning of ERM

Guidelines:

- Public sector- Treasury circular No. 3/2009 on IRMPF, PFMA (2015), *Mwongozo* code, PASB (draft) guidelines on risk management and ISO 31000 (2018).
- Private sector – COSO ERM, OECD, Prudential guidelines on risk management (CBK, IRA and SASRA).

Areas of focus

2

Emerging Issues in ERM

- Evolving risk landscape and adaptation – economic, regulatory and technological
- Creating resilience and flexibility in risk management frameworks

Emerging issues in ERM

- Rapid and increased changes in regulation
- Increased cost of weak governance, risk and control
- Rapid changes in business landscape and risk profiles – technology, business models, pandemic, environment, etc
- Need for improved operational excellence and resilience through proactive risk management (*think ORSA*)

Emerging issues in ERM

- Are traditional approaches to business management still relevant?
- Strategic planning (e.g. 5 yr corporate strategy and budget) on rapidly changing business, technological and regulatory environments.
- Risk-informed strategies & Risk Appetite Frameworks -RAFs

Emerging issues in ERM

- Focus now on management of emerging risks and quantitative risk management (*ORSA*)
- Creating resilience to key aspects of business (*IT- inclusive*)
- Cost-effective and timely compliance (*regtechs*)
- Embedding 4IRs into risk management– risks and opportunities (*cognitive GRCs*)

Evolution of GRC Automation

(Rasmussen, 2019)

Cognitive GRC

- using agile, embedment of cognitive/artificial intelligence technologies into the GRC. i.e. Machine learning, natural language processing, and predictive analytics.
- Already, some early adaptors in developed countries are benefiting from this.

Creating resilience and flexibility in ERM frameworks

EY model (2020)

Creating resilience and flexibility in ERM frameworks

- Own Risk and Solvency Assessment (*ORSA*) framework – strategy and risk governance
- Business continuity and disaster recovery planning (BC/DRP)
- Cybersecurity risk management (NIST framework)

Creating resilience and flexibility in ERM frameworks

ORSA framework

- financial resilience – *risk and capital*

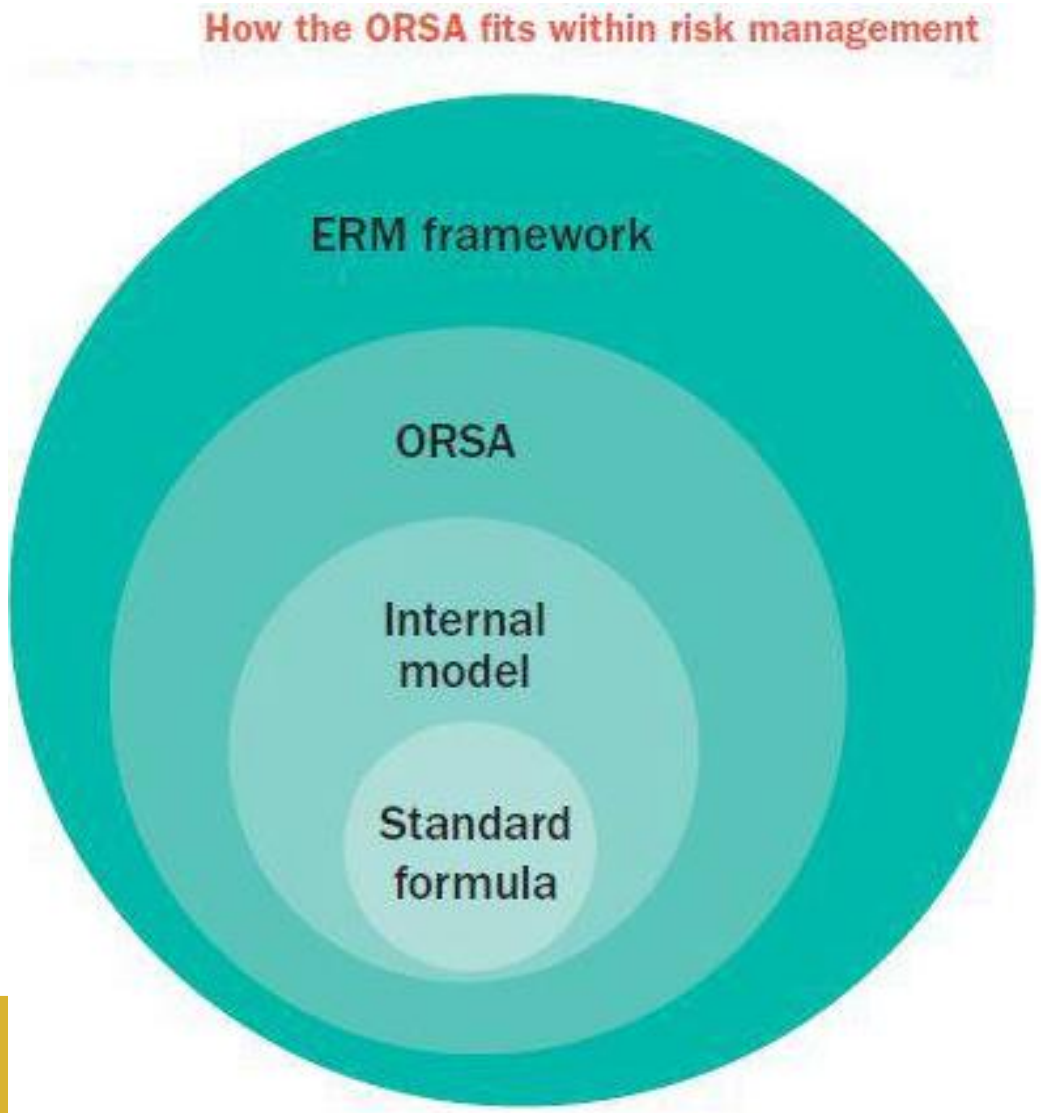
Creating resilience and flexibility in ERM frameworks

ORSA

- Business strategy and Risk appetite Framework (RAF)
- assess the adequacy of ERM (*current & future risks*) and **solvency** positions under both normal and severe stress scenarios.
- Capital requirements - normal and severe stress scenarios

Creating resilience and flexibility in ERM frameworks

Creating resilience and flexibility in ERM frameworks



Creating resilience and flexibility in ERM frameworks

BC/DRP

- operational resilience

Best practices

a) Local key BCM regulations- Banking Act, Insurance Act, Sacco Act :

- CBK via Banking Circular No.1 of 2008 effective 1st March 2008,
- IRA Guidelines on Business Continuity Management, 2018
- SASRA Guidelines on Good Governance Practices for Deposit-Taking Saccos, July 2015

b) International: ISO 22301 (Business Continuity), ISO 28002 (Supply Chain Resilience), NIST 800, NFPA 1600 and FISMA

BCM framework

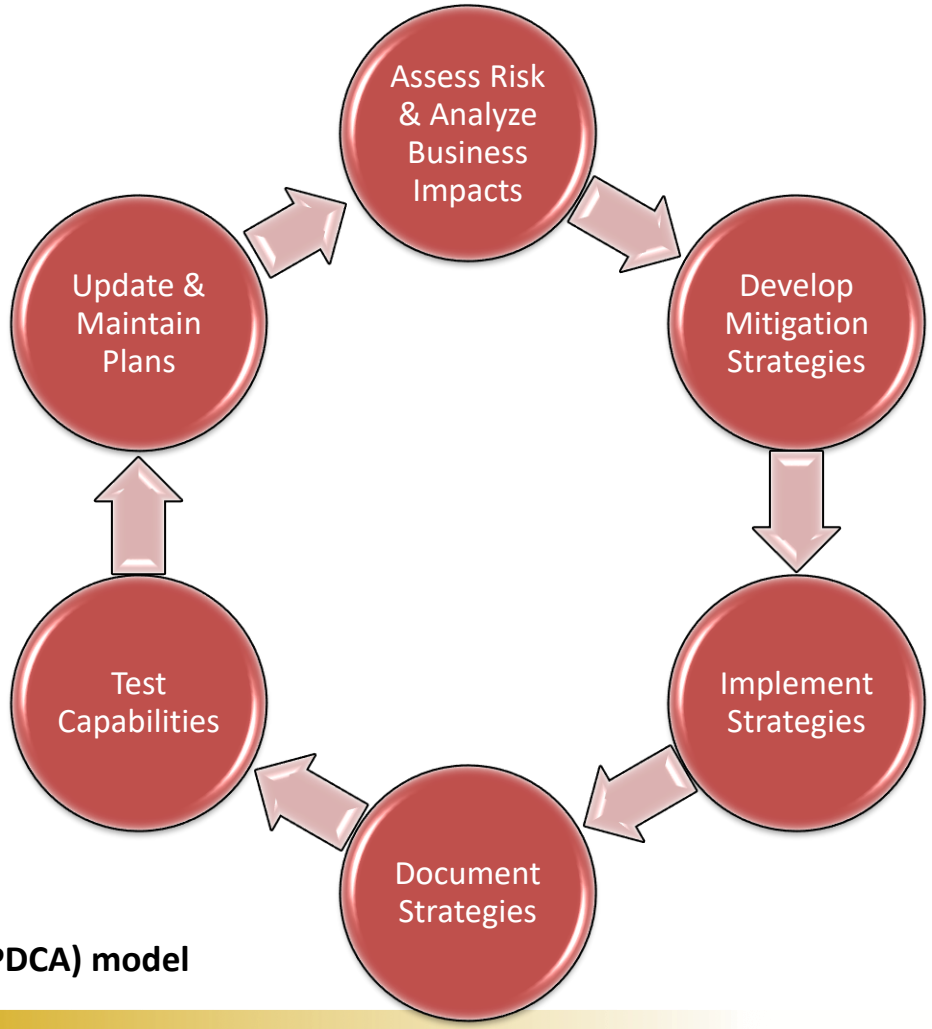
BCM = BCP (non-IT Ops) + DRP (IT Ops)

Where **BCP** = Business Continuity Plan

DRP = Disaster Recovery Plan

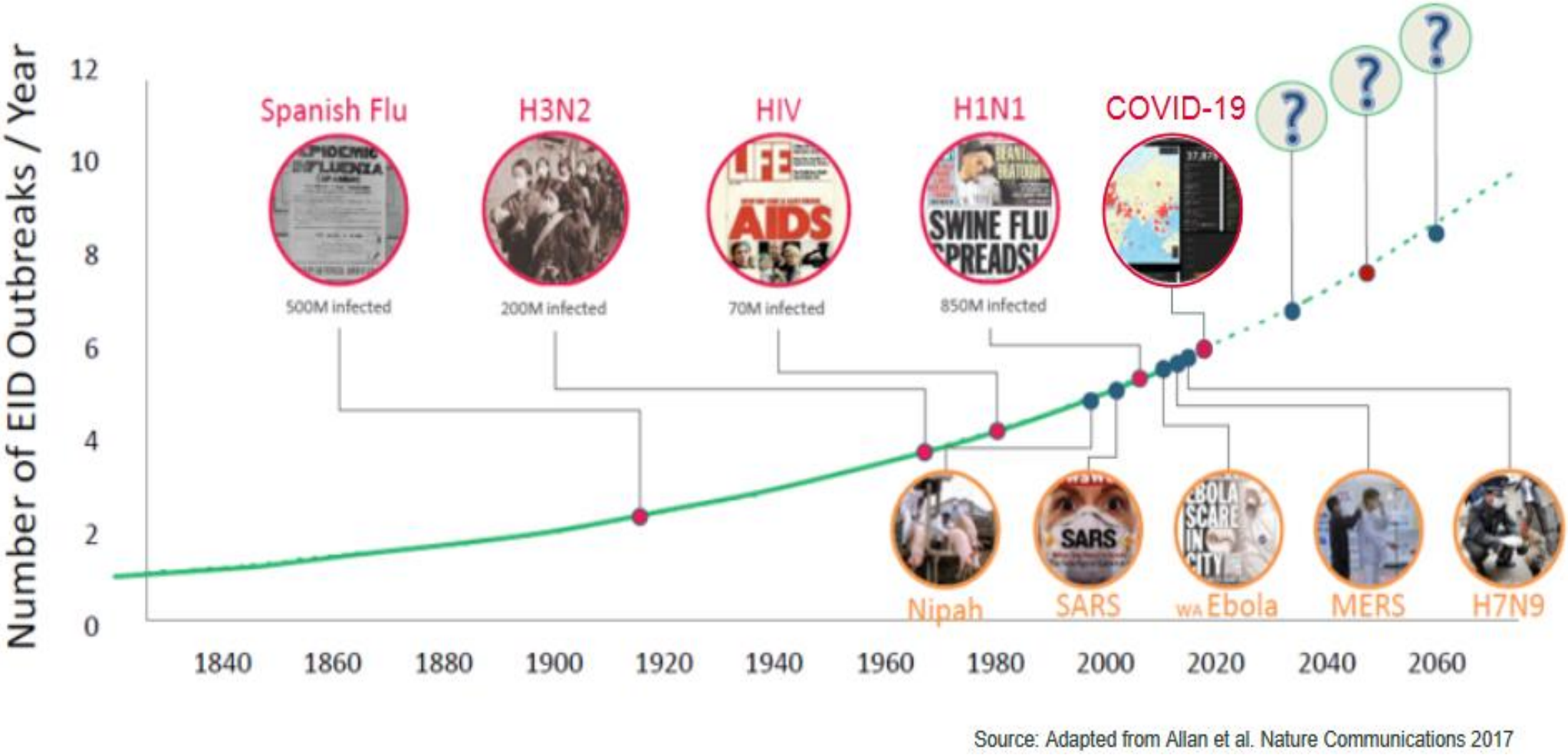
And business **disruption** => **disaster**

Lifecycle of BCM



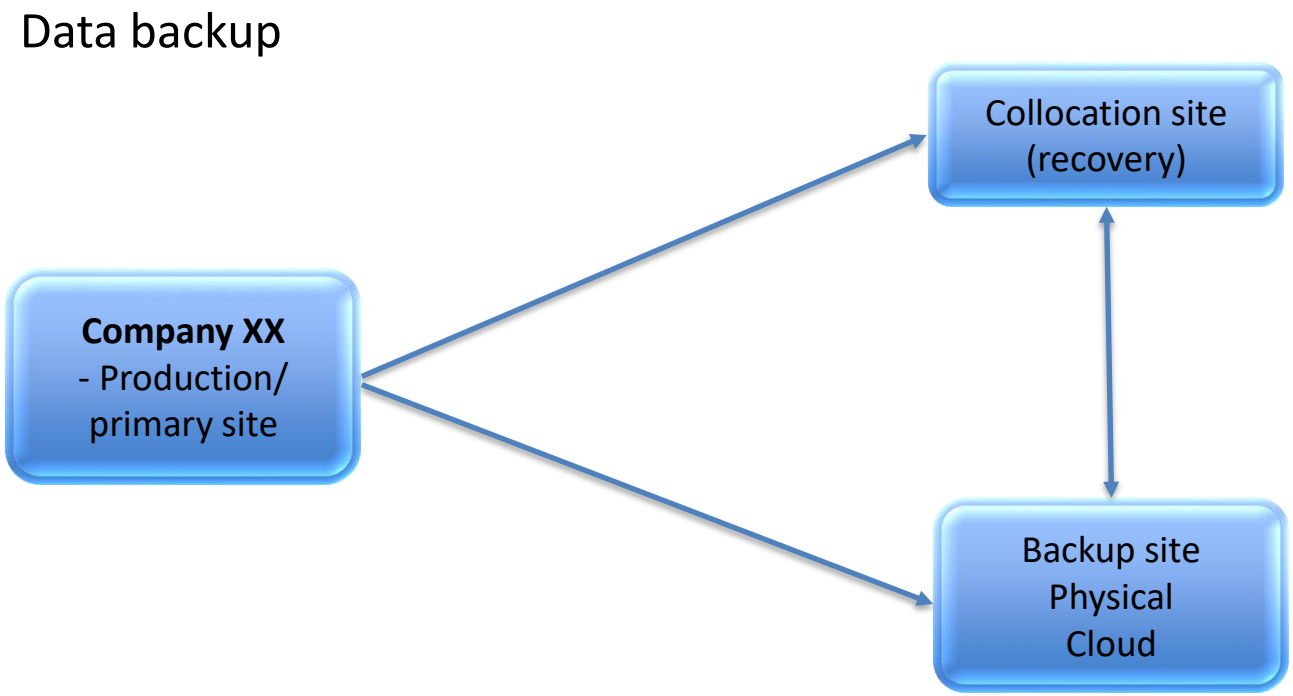
Based on Plan-Do-Check-Act (PDCA) model

Pandemics..

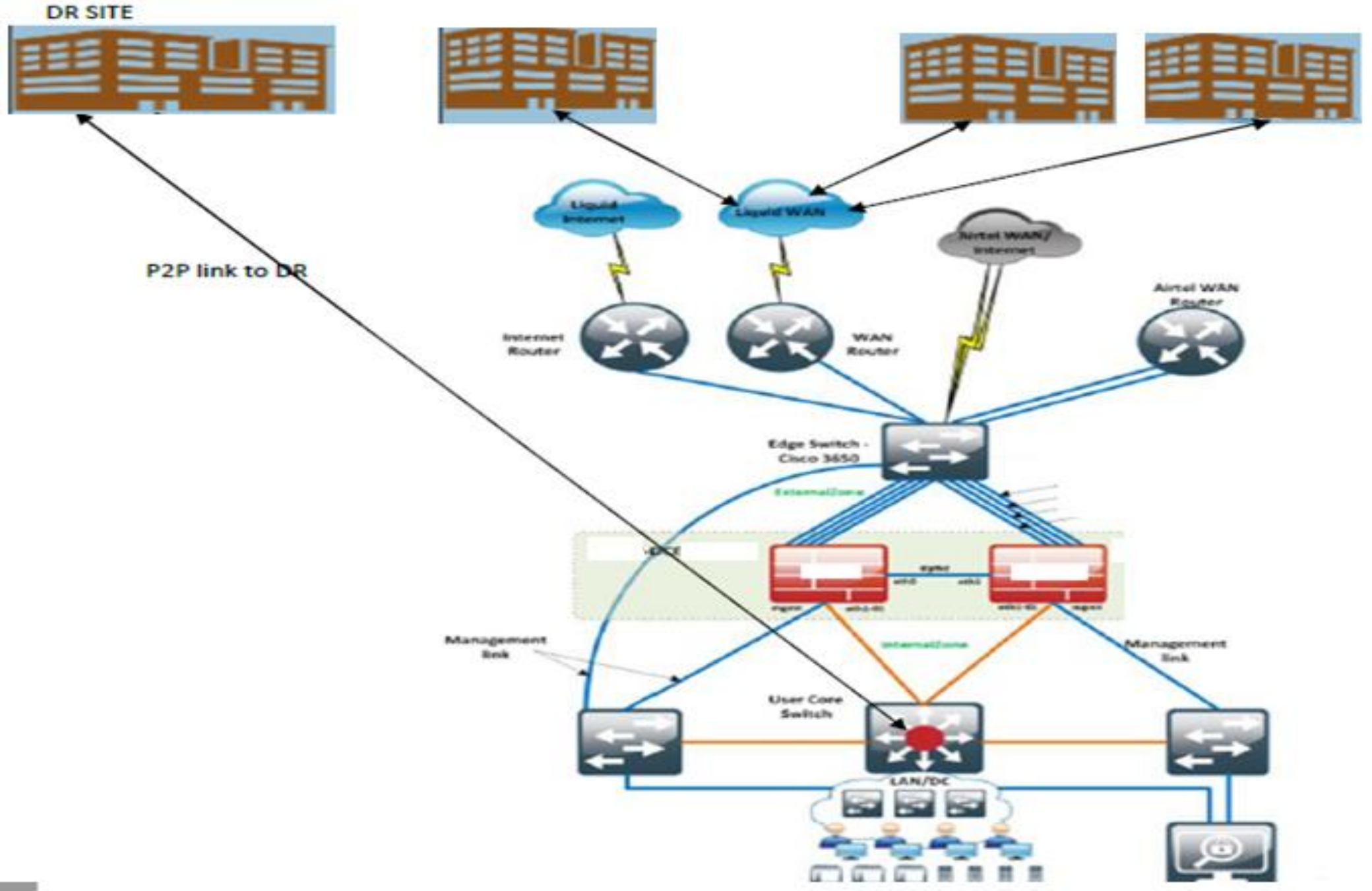


Source: Adapted from Allan et al. Nature Communications 2017

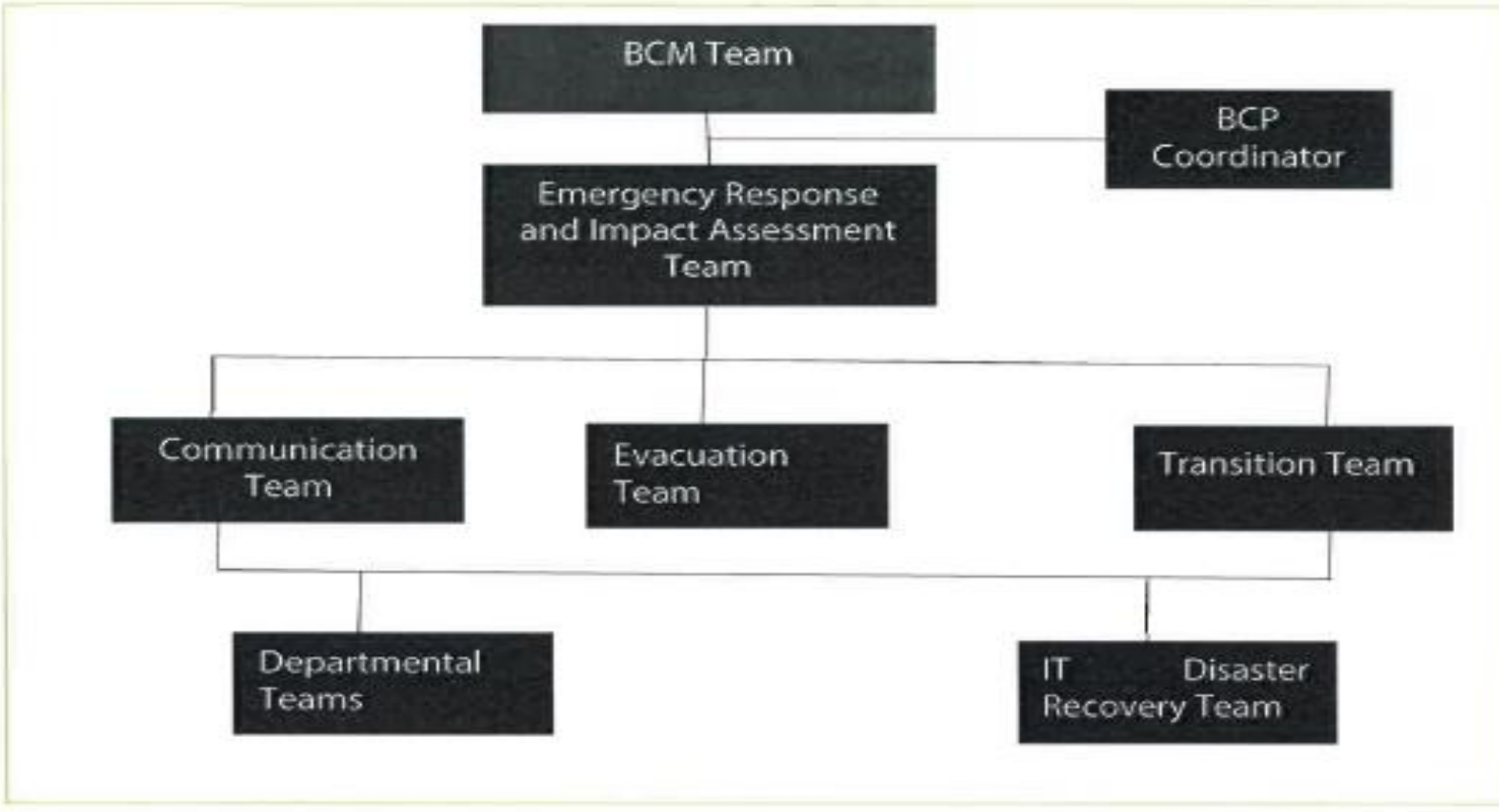
High level DRP structure



Detailed DRP structure



Governance structure of a BCM



BCM – to do..

- Approve BCM policy framework, relevant risk appetite and manage BCM risks
- Ensure compliance to regulatory requirements on BCM
- Set right-tone-at-the-top on BCM, including alleviating BCM culture by creating awareness on BCM
- Give oversight on BCM framework – approve activation of the BCP, communication to key stakeholders

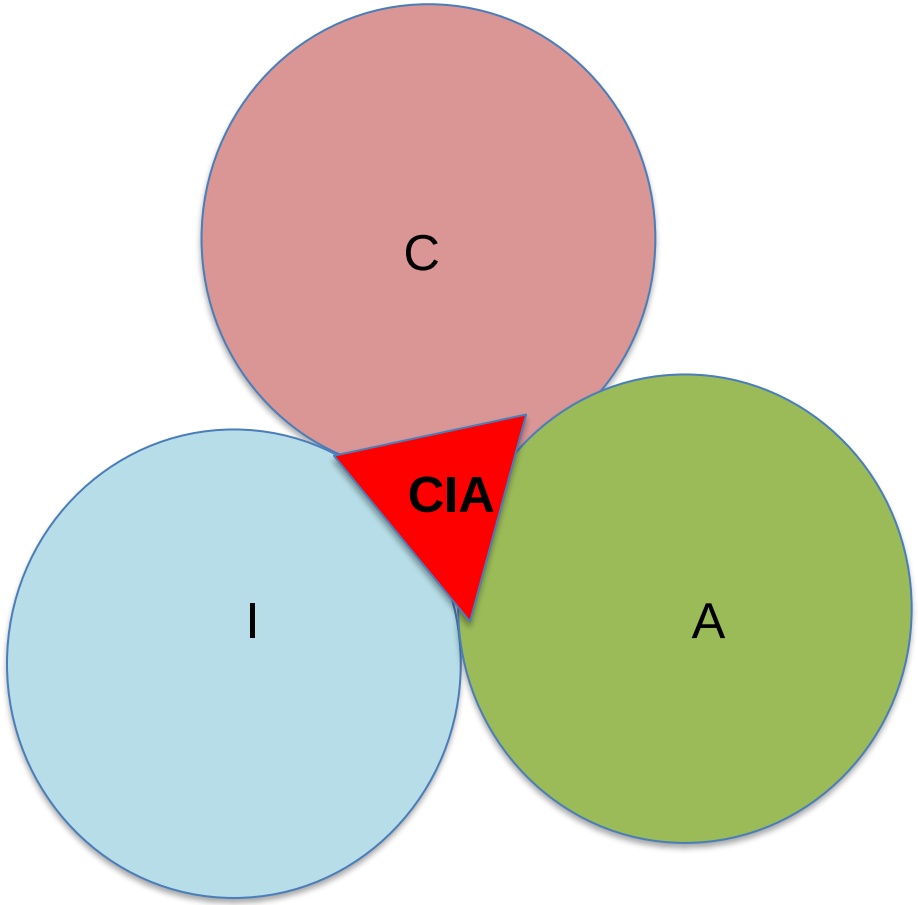
Creating resilience and flexibility in ERM frameworks

Cybersecurity risk management

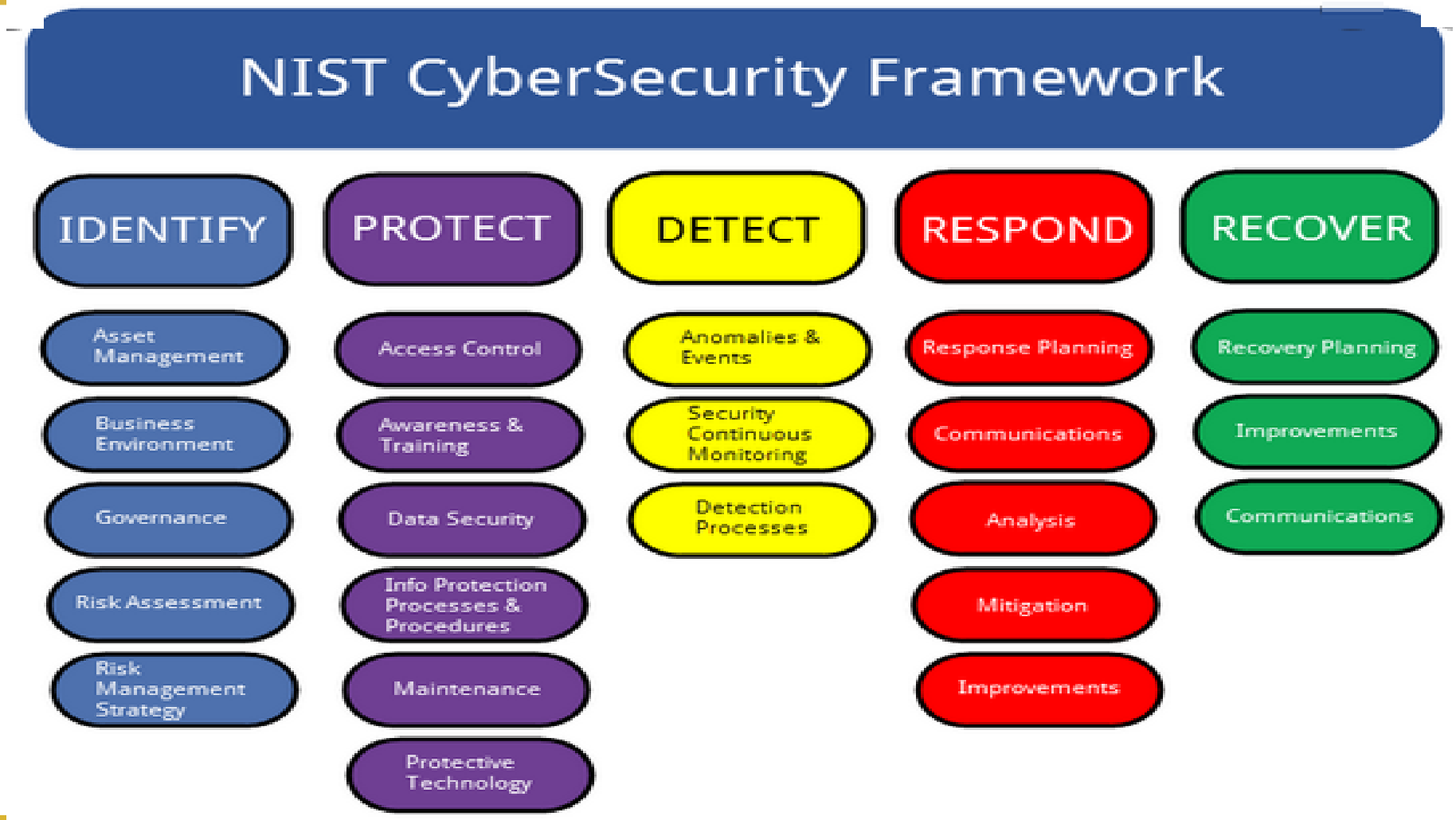
- IT-business resilience

CIA triad ….

- **Confidentiality**
- **Integrity**
- **Availability**



Cybersecurity risk management: The NIST framework


NIST CyberSecurity Framework
IDENTIFY
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
PROTECT
Access Control
Awareness & Training
Data Security
Info Protection Processes & Procedures
Maintenance
Protective Technology
DETECT
Anomalies & Events
Security Continuous Monitoring
Detection Processes
RESPOND
Response Planning
Communications
Analysis
Mitigation
Improvements
RECOVER
Recovery Planning
Improvements
Communications

e.g. implementation of the NIST framework

1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

Cybersecurity risk management – to do…

- Create infosec awareness across the enterprise
- Propose to the board the necessary budgetary support for effective cybersecurity management – patch mgt, tools and relevant activities such as regular PTVA
- Implement adequate cybersecurity infrastructure
- Monitor evolution of the cyberthreats and update the risk profile accordingly

References - ORSA

- https://www.erminsightsbycarol.com/orsa-regulation-answers/
- https://www.actuarialpost.co.uk/news/insights:-own-risk-and-solvency-assessment-372.htm

References - cybersecurity

- https://phoenixnap.com/blog/cybersecurity-best-practices
- https://www.bleepingcomputer.com/news/security/only-half-of-those-who-paid-a-ransomware-were-able-to-recover-their-data
- https://www.nist.gov/itl/smallbusinesscyber

References - BCM

- https://wsvma.site-ym.com/page/695/Seven-Key-Elements-of-Business-Continuity-Planning.htm
- https://www.ey.com/en_gl/strategy-transactions/companies-can-reshape-results-and-plan-for-covid-19-recovery
- https://www.mckinsey.com/industries/advanced-electronics/our-insights/a-post-covid-19-commercial-recovery-strategy-for-b2b-companies#
- https://www.continuitycentral.com/feature0178.htm

Areas of focus

3

Future and adequacy of Risk Management

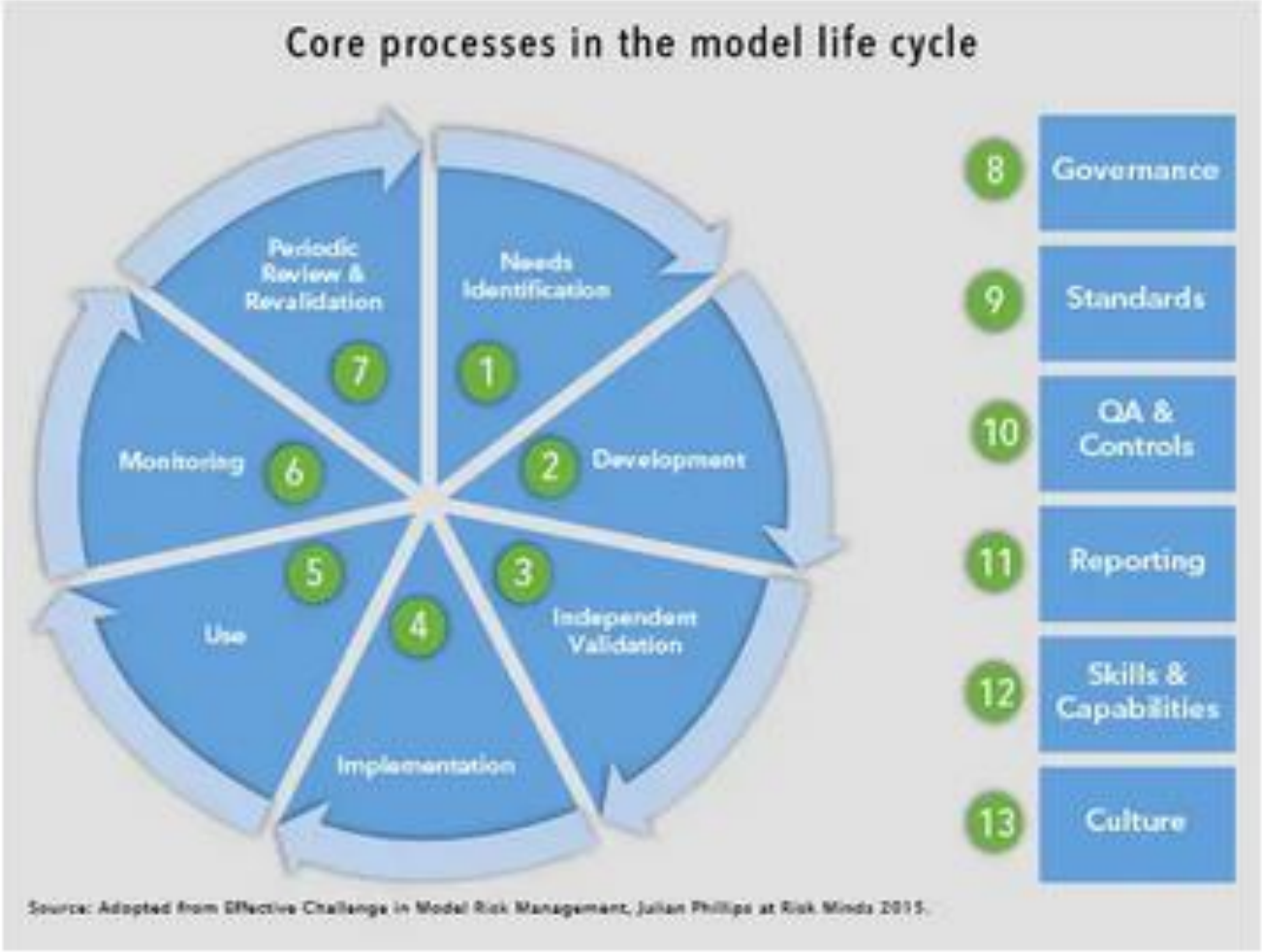
- Proposed risk models for the future
- Risk maturity assessment models and alignment of risk management to corporate strategies

Risk modelling

- Mainly to protect capital and earnings – stress testing and scenario analysis (*different from* ***model risk***)
- Guide in making risk-informed decisions – risk mgt strategy
- New approach to regulation and strategic planning
- Critical success factors:
  - Model Risk Management (MRM) framework (*see model lifecycle below*)
  - Data (quality/integrity) policy & Good risk culture

Risk modelling

Lifecycle



Risk modelling

Examples (*– use of VaR-99.5%, 12 months*):

- External capital models – mainly in financial sectors e.g. Banking (Basel II/III) and Insurance (Solvency II) for management of market risks and credit risks
- Internal risk models – mainly for managing risk exposures on capital (internal capital models – ICMs), earnings (Asset-liability matching – ALM models) and compliance (IFRS9)
- Risk governance (Risk maturity models, BCM/HC maturity, etc

Risk modelling

Proposed risk models for the future:

- Fundamentals will remain the same
- Changes in modelling approach – assumptions, 4IRs (big data and advanced analytics).
- Sophisticated modelling in emerging fields e.g. CRM, fraud mgt and AML/CFT

Risk modelling

Proposed risk models for the future:

- ❑ Ascertain MRM maturity (*McKinsey & Company*)

Model risk management has three evolutionary stages.

	Stage 1 Foundational elements	Stage 2 Implementation and execution	Stage 3 Capturing value
Objectives	• Build foundation elements for model risk management (MRM)	• Implement robust MRM	• Gain efficiencies and extract value from MRM
Key elements	• MRM policy • Model inventory • Manual work-flow tool • Model governance and standards • MRM organization —Governance team —Validation team	• MRM policy • Control and process • Training for stakeholders • Automated work-flow tool	• Center of excellence for model development • Industrialized validation • Transparency in model quality • Process-efficiency tracking • Optimized resource management

Risk modelling

Proposed risk models for the future:

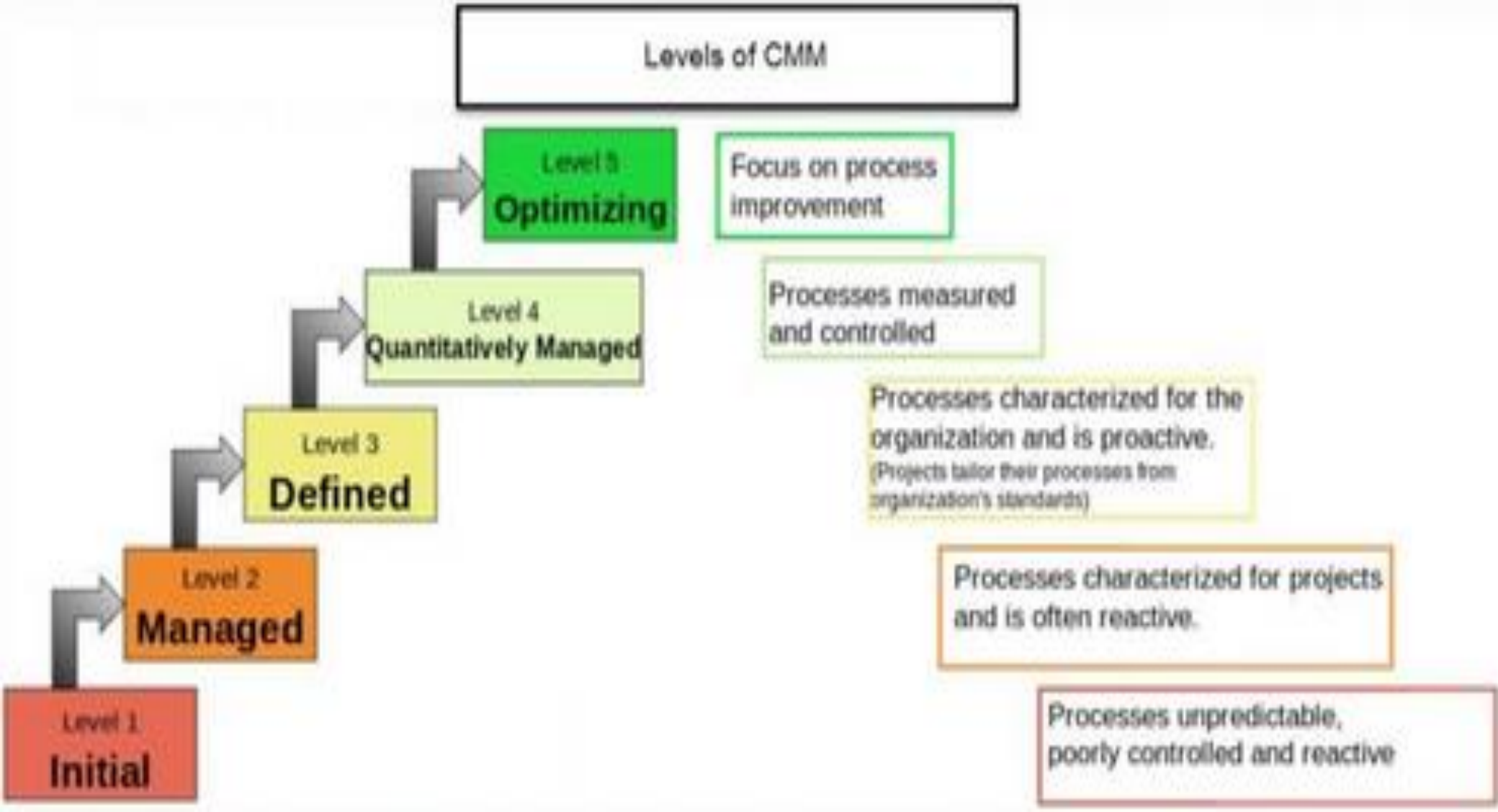
- Technology to ease management of model risk – e.g. through visualization
- With increasing uptake of 4IR(big data, AI, Machine Learning, IoT, etc), models expected to be more complex and give more value
- Effective MRM as number of models increase

Risk Maturity Assessment

- Based on capability maturity model (CMM) – *see next slide*
- Assess maturity of risk management processes
- Continual improvement of ERM (current, future states)
- Key driver for formulating, implementing and M&E of the ERM strategy
- Increased likelihood of attaining corporate objectives

CMM's 5 Maturity levels

(Software Engineering Institute, 1984):

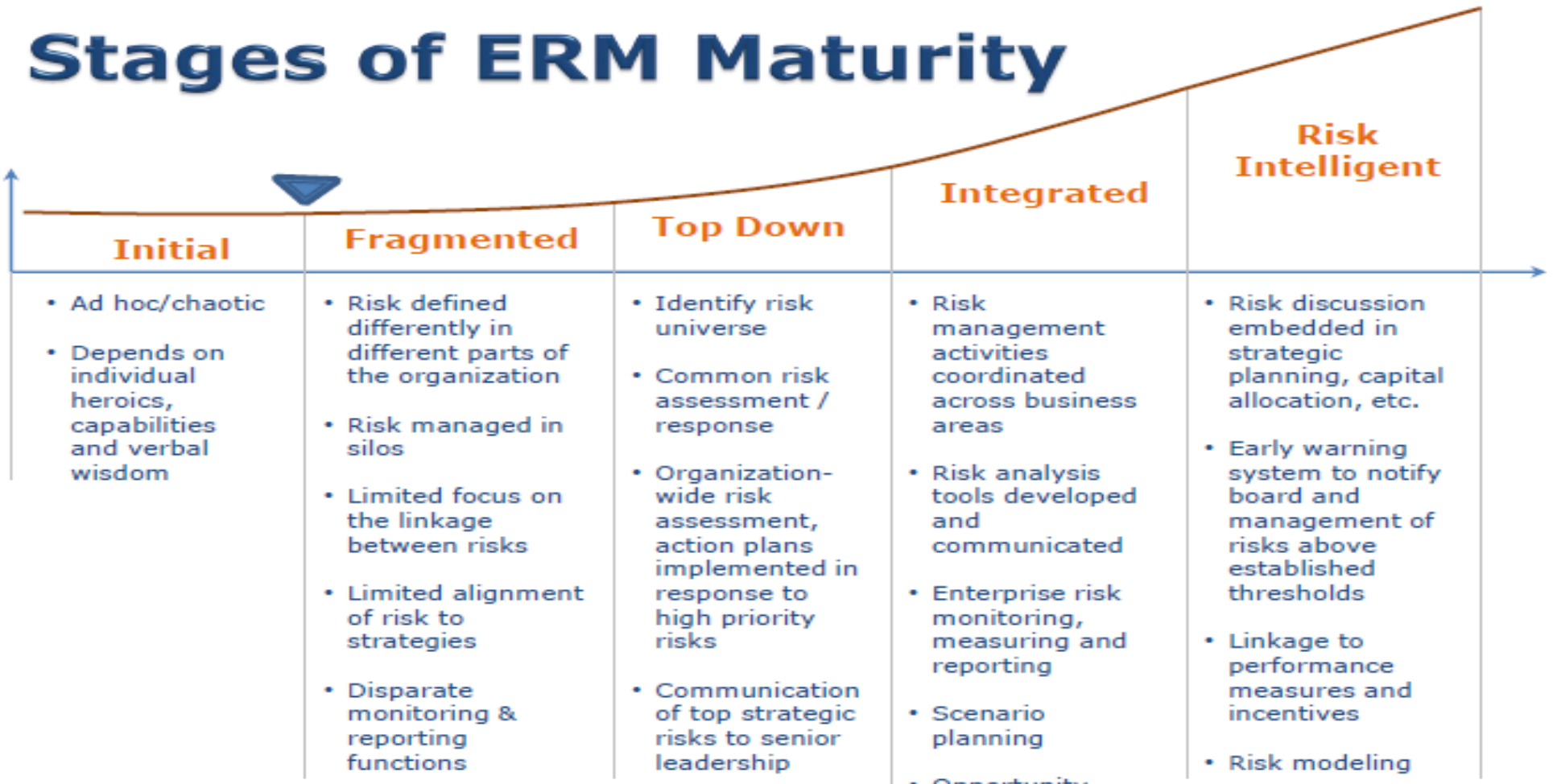


Risk Maturity Assessment

Examples informed by

- ISO 31000 risk maturity model
- COSO risk maturity model
- Leading practices – mainly from the Big 4, proactive regulators/firms and developed countries via forums such as OECD.

ERM Maturity



Deloitte Development LLC, 2010

Risk Maturity Assessment

ERM attributes/elements

- ❑ Strategy
- ❑ Governance
- ❑ Culture
- ❑ Risk Identification
- ❑ Risk Analysis and Evaluation
- ❑ Risk Treatment
- ❑ Review and Revision
- ❑ Information, Communication, and Reporting

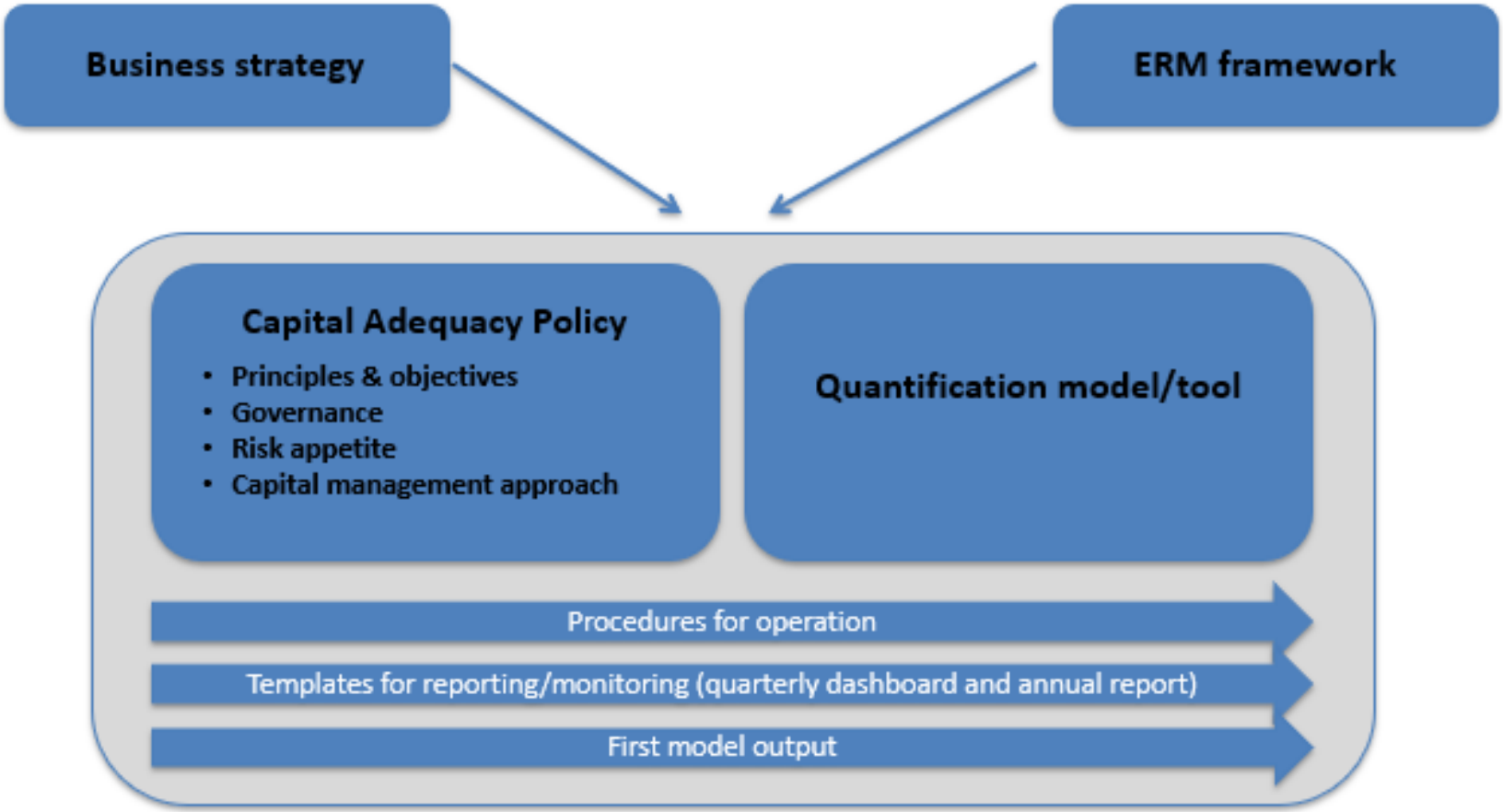
Risk Maturity Assessment

Maturity level	Component						
	Governance	Strategy	Risk processes				Systems & infrastructure
			Risk Assessment	*Risk Quantification*	*Risk Monitoring& Reporting*	*Risk & Control Optimization*	
Embedded	- Oversight (main board, Board Risk Committee) - Independence of risk personnel - Roles and responsibilities - Risk culture	- Risk management incorporated into strategic planning process - Risk management embedded into daily operations	- *Complex risk assessment tools* - *Risk-based strategic planning*	- *Capital allocation* - *Technical risk modelling*	- *Real-time risk reporting & monitoring* - *Integrated risk dashboard*	- *Integrating risk into key initiatives* - *Assessing upside of risk*	- Fully integrated and advanced ERM system - Use of sophisticated tools and data collection to quantify risks
Implemented	- Quality assurance reviews on risk mitigations - Control self-assessments	- Strategic and risk management plans drive action across firm - Risk resource is properly positioned	- *Trend analysis* - *Holistic portfolio & risk profile reviews*	- *Risk-informed performance indicators* - *Risk -resilience strategies*	- *Board committee reporting* - *Stakeholder reporting*	- *Risk control self-assessments (RCSAs)* - *Risk control policies*	- One main ERM system - High quality reporting of risk incidents through automated solution
Defined	- Risk appetite - Joint risk management forums - 3 lines of defense clearly defined	- Clearly defined risk strategy - Annual risk workplans - Risk methodology exists	- *Departmental risk registers* - *Corporate risk register*	- *Root cause analysis* - *Risk charts*	- *Emerging risk reporting* - *Incident reporting*	- *Quantify total cost of risk* - *Assess effectiveness of controls*	- Existence of some risk incidents reports - Risk analytics implemented across the firm
Initial	- Policy framework - Procedure manual - Separate risk management function from internal audit function	- Risk addressed as strategic opportunity - Firm provides some direction in risk management	- *Defined risk identification approach* - *Clear risk taxonomy*	- *Above average risk analysis* - *Clearly defined tolerance limits*	- *Key risk indicators (KRIs)* - *Management risk Committee reporting*	- *Action plans for improving controls* - *Risk optimization worksheets*	- Reports produced from various systems in MS Excel and Word - No capacity to track risk management via incidents and events
Overall risk maturity index							**19%**

Key:				
	Initial		Defined	
	Implemented		Embedded	

Alignment of risk management to corporate strategy

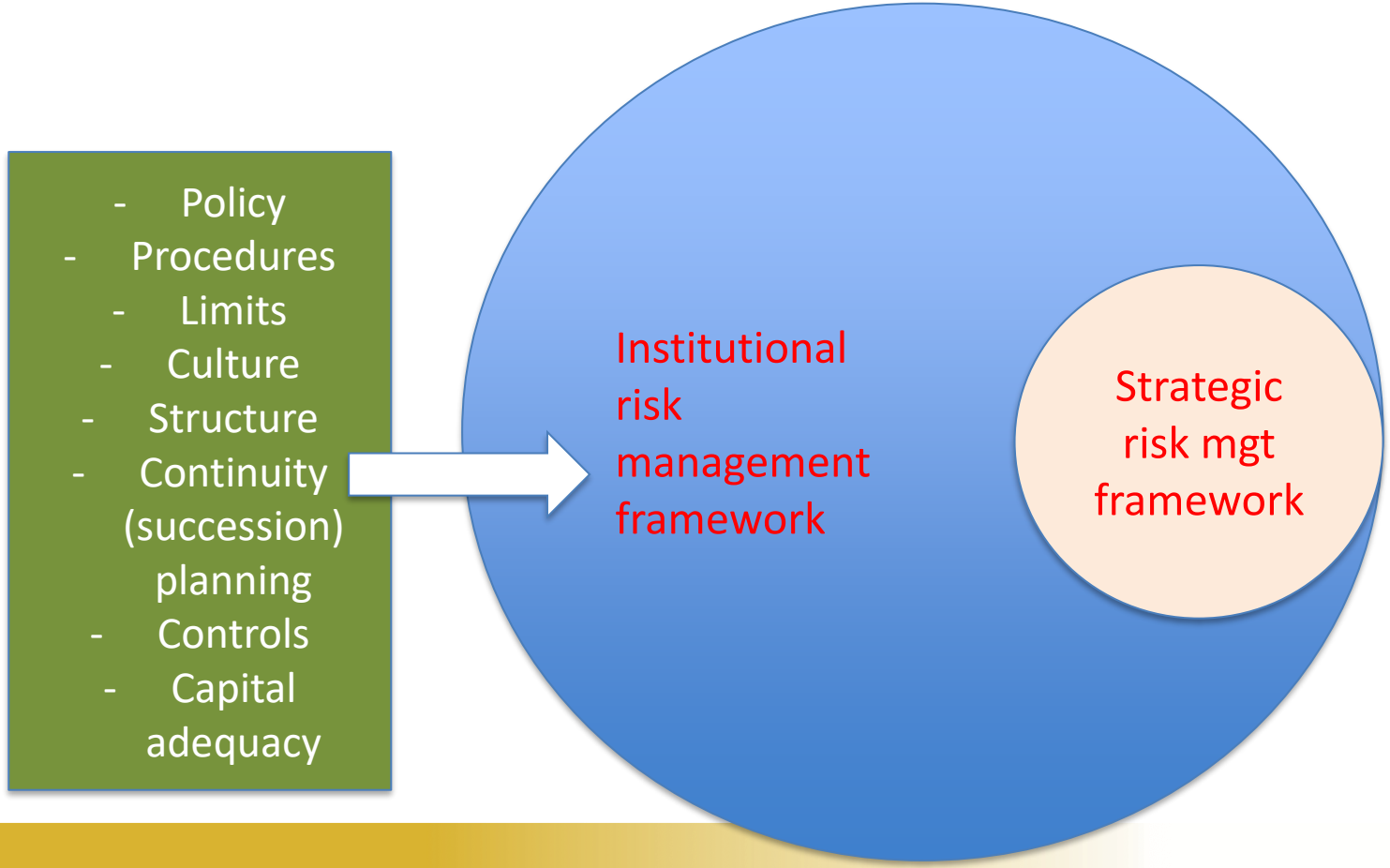
Linking Risk Management to Strategy….



Capital Adequacy Framework

Strategic Risk Management

- Strategic risk management framework (*board-approved*)



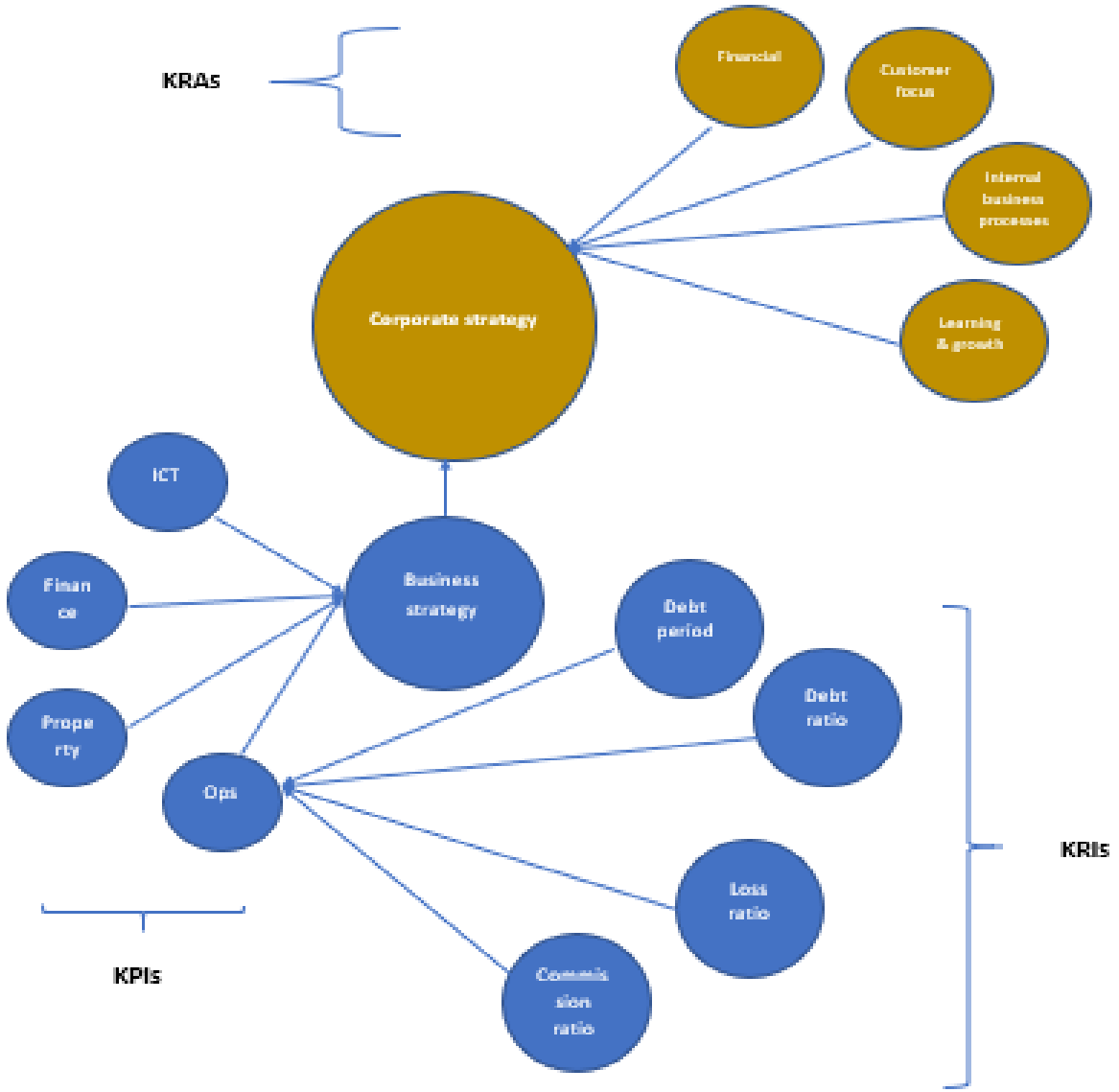
Strategic Risk Management

- Risk-informed strategic planning (**KRAs-KPIs-KRIs triad**)
- Resourcing implementation of the Strategic Plan.
- Embedding risk management in strategy implementation
- Creating and entrenching the right risk culture (**setting right tone-at-the-top** and in the middle)
- Risk-based M&E of strategy implementation

….the HOW

- Putting in place risk appetite framework (RAF) – convergence of Strategy and Risk Management
- Ensuring the RAF is cascaded across the organization via effective performance management => BSC
- ORSA – consistency between RAF and corporate governance framework
- Reviewing outputs of the M&E of strategy implementation and initiating board directives on corrective actions for any breaches

Linking Risk Management to Strategy….



Linking Risk Management to Strategy….

e.g…..

Corporate strategy		Business strategy - (re)insurance dept	
Pillars	Key Result Areas - KRAs	KPI	KRIs
-FINANCIAL	Efficient management of receivables	Debt collection period	90 days
		Debt ratio (debt collection)	20%
	Cost containment	Average loss ratio	58%
		Management expense ratio	13%
		Average commission ratio	27%
- CUSTOMER FOCUS			
- INTERNAL BUSINESS PROCESSES			
- LEARNING & GROWTH			

Linking Risk Management to Strategy….

- **e.g. of an extract from Risk Appetite Framework (RAF) – non capital KRIs**

List of Measures	Risk appetite limits	Deviations should be reviewed by the		
		Management risk committee	Board Risk Committee	Entire Board
	%/days	%/days	%/days	%/days
Debt ratio	20%	<=20%	20% - 36%	>36%
Impairment provisions	14%	<=14%	14% - 32%	>32%
Insurance Risk				
Loss ratio	53%	<=53%	53 – 63%	>63%
Combined ratio	87%	<=87%	87% – 103%	>103%

Risk Management Strategies

- Treat/mitigate/contain i.e. implement recommended controls (only for medium and high risks)
- Transfer/share/insure
- Accept/tolerate – especially for medium & low risks
- Avoid/terminate – especially for high risk items

References

- https://searchsoftwarequality.techtarget.com/definition/Capability-Maturity-Model
- https://www.itgovernance.asia/capability-maturity-model

Q & A

THANKS