### **Towards Pervasive GRC**



HEAM

### **Business Resilience Management** MetricStream Implementation Framework

### Ihsan Ul Haque

Coordinator Business Resilience Management Bahrain Petroleum Company Bahrain





- **1**. Organization Overview
- 2. Management Commitment
- 3. Challenges
- 4. Business Response
- 5. Business Resilience Model
- 6. Technical Response
- 7. MetricStream as an Enabler
- 8. Key Learnings
- 9. Audience Questions and Discussion

Risk Management is an integral and critical ( and often invisible) part of Good Governance



Bahrain Petroleum Company (Bapco) is engaged in exploration and prospecting for oil, drilling, production, refining, distribution of petroleum products and natural gas, sales and exports of refined products. Established in 1929, Bapco contributes around 70% to the national economy. Its 268,000 bpd refinery process 60% of its crude pumped from Saudi Arabia's Abu Saafa offshore field via a 54 km pipeline, half over land and half sub-sea.

Refining Capacity	268,000 BPD
% Of Product Exported	<b>Over 95%</b>
Workforce	2270
% Bahrainization:	78%
Contribution to Economy	>70%



Bapco is fully committed to its mission of managing and operating oil and gas business, supplying crude oil, petroleum products and gas to local and international markets with the aim of maximizing contribution to the national economy.

- The company will exercise a high level of diligence in understanding and effectively preventing, reducing or managing risks to its business. Hence an Enterprise Risk Management Program is in place for the management of critical risks in all areas of the company.
- 2. Bapco recognizes the importance of having action plans if any of the threats to business materialize. Accordingly, Crisis and Business Continuity Management Plans will be developed for all high risk and critical areas of the company with effective readiness to react and a rapid capability to recover.
- 3. There will be management Oversight and an independent Internal and External audit program to <u>verify due diligence</u> in mitigating critical risks and that appropriate crisis and continuity response plans are developed, communicated and maintained

# 3. Challenges

- 1. Multitude of Risk Assessment techniques and procedures
  - **1.** Hazops (Process and Projects)
  - 2. Business Continuity
  - 3. Risk Based Work Selection (Maintenance) 8. Internal/External Audits
  - 4. Environmental Affairs
  - 5. Occupational Hygiene
- 2. No formal "Business Risk Assessment"
  - 1. Independent Risk Assessments by business units
- 3. Several "Risk Mitigation Oversight" organizations
  - **EHS Committee** 1.
  - **Compliance Committee's** 2.
  - 3. ...
- 4. Risk Mitigation and Risk Response strategies not integrated
- Independent & standalone Crisis Management and Business Continuity Management 5. Plans
- Good business must be supported by good technology 6.

- 6. Fire, Health & Safety
- 7. Incidents
- 9. Compliance Assessment
- 10. Strategic Planning and **Projects**





# 4. Business Response



### **Principles**

- 1. A standardized technique and process for Risk Assessment for technical or business risks
- 2. A structured and common approach to business risk identification, assessment, mitigation, tracking and reporting
- **3.** All enterprise risks are covered: business, technical, compliance, strategic planning and information
- 4. Clear and demonstrable link between Risks and readiness to respond (Crisis and Business Continuity plans)
- 5. Risk Oversight process and organization, including Board of Directors is established with clearly defined roles and responsibilities

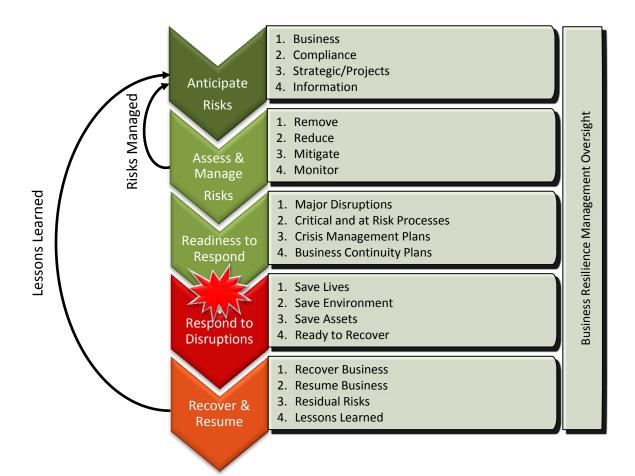
### Steps

- **1.** Business Risk Management (ERM) initiated in 2004
- 2. Standardized Risks Assessment method introduced in 2009
- 3. Standardized Business Continuity Planning method introduced in 2010
- 4. Unified Crisis and Emergency Response system developed in 2011 incorporating all old MIPs (Major Incident Plans) into one system (ICS)
- 5. A Business Resilience Model (incorporating ERM, CMP and BCP) developed in 2013
- 6. ERM Committee (from 2004) transformed to Business Resilience Management Committee and BoD charter amended to include BRM oversight in 2013



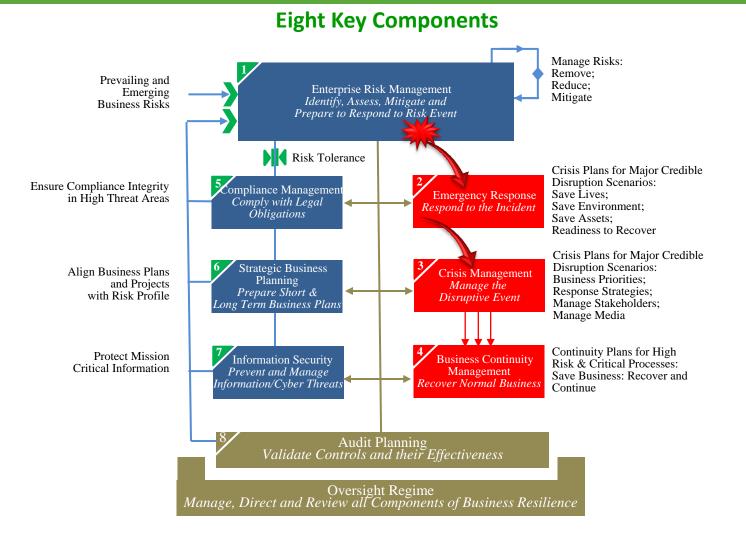
### What is Business Resilience Management

"The ability of an organization's business operations to rapidly adapt and respond to internal or external dynamic changes – opportunities, demands, disruptions or threats – and continue operations with limited impact to the business" ... IBM



7





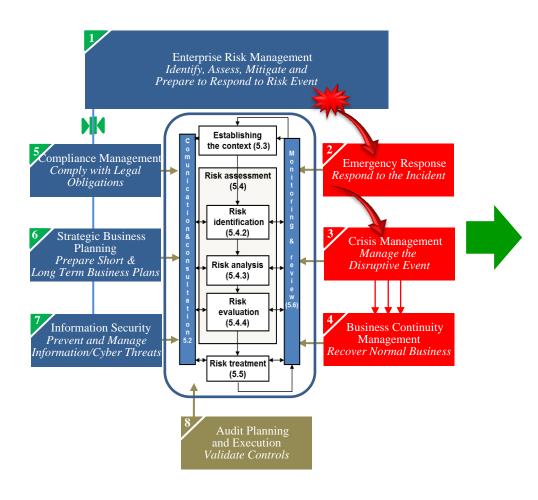
#### Regular review and agreement by Key Stakeholders: Risk Appetite; Mitigation Strategies and Measures; Performance Measures

This document is property of Bahrain Petroleum Company

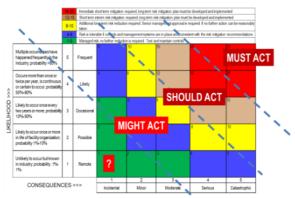
MetricStream GRC Summit Middle East 2014



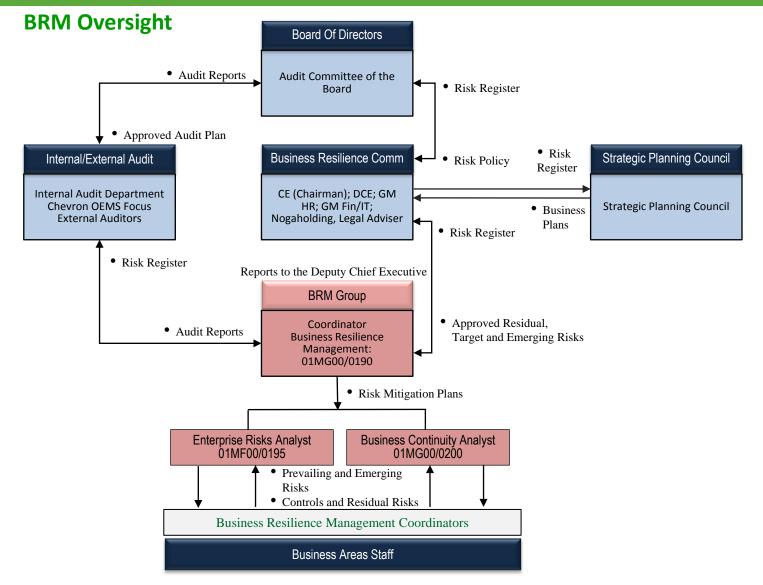
### **Unified Risk Assessment Standard**



Risk Assessment Matrix						_	16-25	Immediate short term mitigation required, long term risk mitigation plan must be developed and implemented Short term interim risk mitigation required, long term risk mitigation plan must be developed and implemented				
Definitions						-	12-15	Short term interim nak mitigation required, long term nak mitigation plan must be developed and implemented Adoitional ong-semi nak reduction required, semior management approval is required. If no turner action can be reasonably				
LIKELHOOD							4-6	token. Risk is tokeable if controls and management systems are in place and consistent with the risk mitigation recommendations.				
The likelihood of consequences occurring: Index					Index	Ē	1-3	Managed risk, no further reduct				
Multiple occurrences have happened hequerity 5 Frequent 5				5	10	15	20	25				
CODUTE HORE THEN STOLE OF TAKON per year. It continuous or certain to accur; probability 50%- 4 Likely 80%					Likely	8		8	12	18	20	
Likely to accur once every two years or none; 2 Docasional pobability 10%-50%					Occasional	DOCHT BYT	3		9	12	15	
Likely to accur once or more in life of 2 Possible to Rity to gan basic probability 155-105.						â	2				90	
38	kely to acco subility . 1%	ar but know -1%	in in industry;	1	Renate		1	2	3			
FOR ORTEGORES FOR ASSESSING CONSIGNERS							CONSEQUENCES					
FOR ASSESSING CONSEQUENCES						Incidental	Minor	Moderate	Serious	Catastrophic		
Strategic	Learning & Gruth Knowlegh Manganeer, Hitsel Sikhel, Mindowe Planches Researce. Fizancial Incessed Cast Efficiency and Congetherenix, Standard Trade (Frit), Edinance Francial Streight, Lossand Pandady, Centime: Tage Excellence, Entrance Coguete ApJr, Costly Plancing, Contemp. Neuroima Stances, Coguete ApJr, Costly Neuroima, Contemp. Neuroima Stances, Stag and EM					Incidential and minor impact on business		Limited and selatively small impact on the achievement of business ubjectives	Moderate impact or temporary delay in the action-sense to business objectives; short term butlinish repution damage limited impact on controre metacion (imited increase in costs; short term increase) in costs or lass of revenue	Constained ability to achieve business signatives with significant but recoverable loss of contonensialitances, oscibilityingutation; toos of significant explicitant assets; toos of significant number of long personnel	Serious impact or long term viability of company resulting in loss of major business capability, company spacetistics and long term professibility of its operations	
		th & Safety	Workforce				s impact or minor Finit Aid injury	First aid injury (e.g. minor cuts and bruises, eye initiation from dust) or very minor health effect	Lost Time/Non Lost Time kýsty (k.g. sprains, fischure, c.d. lacestricos, burns or brukes) or health effect (i.e. deshees or demattik)	Major injuries: angustations, major foscturas, multiple injuries, or health effects: severally like abstancing diseases, occupational illness	Multiple faculties or Multiple permanent daabilities	
	P eccle	Health	Public			N	public impact	Creates minor public attention but ro injuries	Results one injury to any public but not serious	Causa several serious injuries that can cause public panic	Single-or more tutalities that can create huge public panic	
		Human	Resource Manage	ine	-	Ur	-roticeable impact on workbroe crale, efficiency and competence	Very insignificant inpact on workbroe mousie, efficiency and competence	Some by rst sarious inpact on workforce morale, efficiency and competence	Norse, efficiency and competence of some of the onlical workforce at tak	Norse, efficiency and competence of the entire workforce is at major fak	
Operators	Environment					2.5	gigble inpact no measurable pact to the environment	Sight environmental damage meshing from localized contentination of all, water or lend, but no lasting effect. A single breach of relativity or presched linits. Siznage and disposal of small quantifies of hozarchas wasts.	Moderate and limited damage to the environment and/or no leading effect. Repeated breaches of statutory or prescribed limits. Stratege and disposal of waters represent a moderate link or moderate specifing cost.	Severe & potentially long term demoge to the environment, may requise semantic measures to restore damage. Extended brackete of statutry or prescribed limits. Currar wate storage/signous methods are a significant in its ground & ground water.	Pensistent and severe damage to the environment with major financial consequences. Release to air, water or land continuously branch-majolatory or prescribed limits. Na locophile disposed facility for water. Potential impact on ground and groundwater.	
	Aasada						gigble dowrline of assets	Some asset loss; damage or downline	Serious asset loss and downline	Severa and serious assets loss, demage to facility or significant downline	Tatal damption or damage; potential for permanent loss of production	
	Public Image					No	a atverse publicity or perception	Advense perception but little or no public and/or regulatory concern. Some advense attention in the local media.	Considerable adverse perception and public/regulatory concern. Moderate adverse attention in the local media.	Serious public and/or regulatory concern. Extensive adverse attention in the local media and potential restrictive measures by Government	Catestrophic deterioration in public and Government relations. Extensive adverse attention in local and regional media.	
ance	Business Conduct					ine go	significant lapse in good vernance	Some minor oversight in good governance	Some violations with some but not so important consequences	Significant violations of good governance, guidelines & norms with serious consequences	Serious violations of good governance: accountability, ethics, and accial responsibility	
Complia	Regulatory and Legal Standards					Insignificant technical elokation of Standards, but comply in split – so need to amend Standards		Technical violation of Standards, but comply in split - medium term aim is to amend Standards to accommodate	Mnor violation of Standards – interim solution can be found untilful compliance is achieved	Technical violation of Law but comply in spirit – medium term aim is to obtain a waiver to accommodate	Violation of Law - need to initiate changes immediately	
Varida	Margins and Interest Rates and Liquidity & Credit					Ma ah	ngins on one product declines for of period; No funding insues	Margins on one or two products reduced for initial period Banks have temporary liquidity issues, only able to provide partial funding of capital requirements	Margins on some products at lower leasts for up to 6 months. Backs only able to provide partial (indep of capital requirements	Hargins on mijority products low for short period unable to cover fixed & operating costs. Banis unable to extend credit for a limited period, including Latens of Credit for Cuatoness	Illagins on ALL products low or negative for exitended period meeting in negative cash fours. Banks unable to lend any funds for an extended period, including Latters of Oresit for Customers	
	Controla					-	e or insignificant breach of financial ritrols	Some but not significant breach of feancial controls, very small feancial losses.	Some breach of financial controls resulting in some financial losses.	Serious breach of financial controls resulting in significant financial losses	Major breach of financial controls resulting in catestrophic financial losses	
	\$					đ	millon	<13 miliat	10-100 million	100-250 million	x250 million	
FIRSTING CONTROLS						F	5	4 2		2	1	
		ERS	TING CONTROLS	1			Very Effective	Effective	Limited Improvement Needed	Significant Improvement Needed	Ineffective	
1 Design						Controls are designed and operating in excess to basic requirements		Controls are properly designed	Controls design is adequate however limited improvement is needed	There are significant opportunities for the improvement of design	Design of controls is not fit for purpose at all, will require a totally new-design	
2	2 Application					Controls are applied and operating in excess to basic requirements		Controls are properly applied as intended	Controls are in place however limited improvement is needed	Key controls in place, but there are significant opportunities for further improvement	Controls are non-existent or have major deficiencies, don't operate as intended	
3	3 Effectiveness					20	ontrols are designed well of are being applied fectively	Some improvement is needed in the application of controls	Minor improvement is needed in the application of controls	Significant but not major improvement is needed in the design and application of control	The design and application of controls is highly ineffective; needs a major redesign and application	







10 Towards Pervasive GRC

MetricStream GRC Summit Middle East 2014

# 6. Technical Response



### **Principles**

- **1.** A single source database with consistent, uptodate and reliable data
- 2. Reporting contents and look-and-feel should be same at all levels: Risk Owners, BRM Committee, and BoD
- 3. A secure database, with at-source updates and audit trail
- 4. Consistent and common data terminology as per company standards
- 5. One system for all risk mitigation actions: origination, tracking, reporting and closure
- 6. Data and system should be secure
- 7. No data duplication within or across systems

### **Steps**

"Implement an integrated Business Resilience Management System based on a proven GRC solution"

- 1. Common Database with BRM Registers: Business Risks; Compliance; CM and BCP; Information Security; Projects and Audit
- 2. A wizard to assist with Risk Assessment data capture based on the standardized Risk Matrix
- 3. Workflow to manage corrective and preventive actions from inception to closure
- 4. Integration with Corporate Systems (like HR)
- 5. Common look-and-feel reporting system including KPIs
- 6. Selected MetericStream solution

# 6. Technical Model



### **MetricStream Solution**

#### 1. Functionality

- 1. <u>Enterprise Risk Management</u> Anticipate, assess and mitigate key risks to business
- 2. <u>Compliance Assurance</u> Comply with government, industry and company regulations and standards.
- 3. <u>Information Assurance</u> Ensure security and privacy of Infrastructure and data Business or Operational
- 4. <u>Business Continuity Planning</u> Prepare and rehearse plans to respond to major threats
- 5. <u>Strategic Planning</u> Strategic Plans and Major project Risk
- 6. <u>Crisis & Emergency Response Management</u> Being prepared for credible disruptions
- 7. <u>Audit Program:</u> Documentation and validation of Controls

#### 2. Process

- 1. Risk Assessment Procedure: Bapco Risk Matrix with drop-down menus
- 2. Approval by Stakeholders
- 3. Email based reporting and escalation

#### 3. BRM Registers

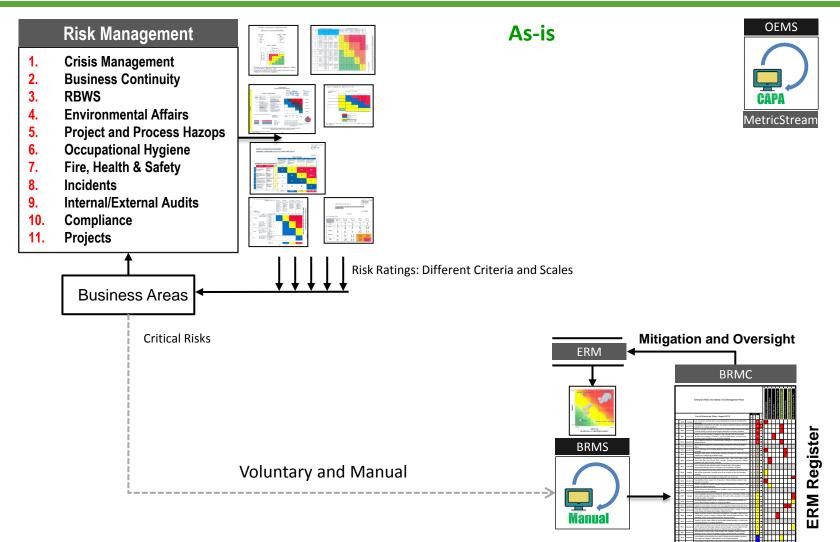
- 1. ERM
- 2. Crisis Management Plans
- 3. Business Continuity Plans
- 4. Audit Program
- 5. Compliance

#### 4. Reporting

- 1. Risk Dashboard including KPIs
- 2. Stakeholders, BoD, BRMC Reports (Bapco templates

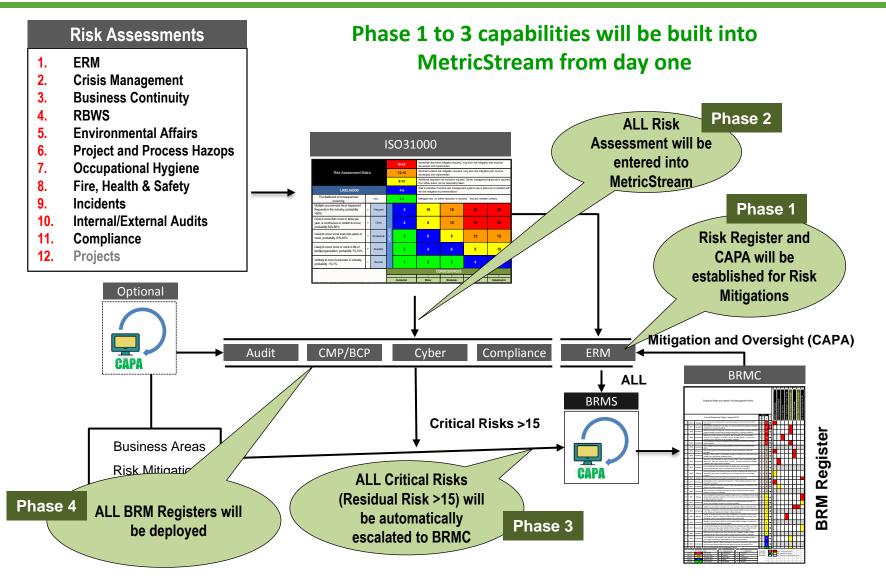
# 7. MetricStream as an Enabler





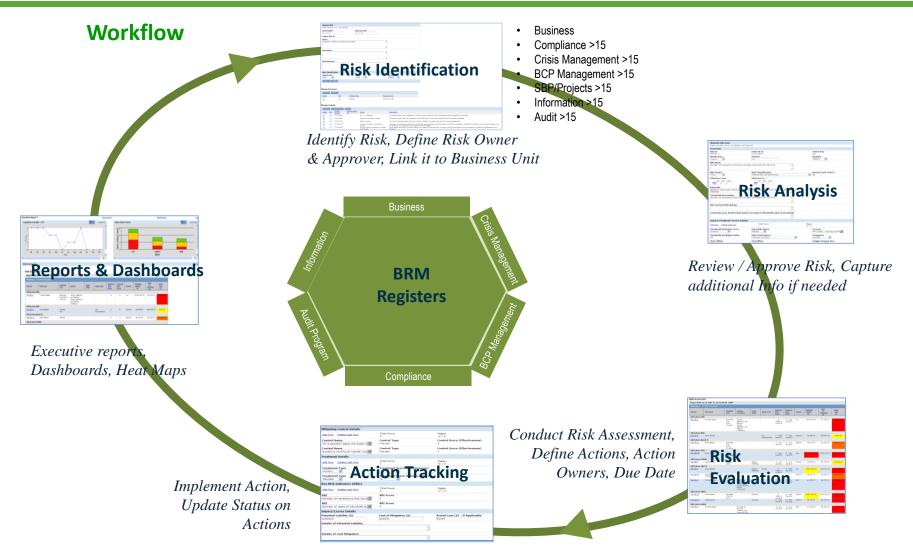
## 7. MetricStream as an Enabler





## 7. MetricStream as an Enabler









- 1. Think beyond traditional ERM
- 2. Business model precedes technical model Single framework but phased deployment
- 3. A consistent and standardized view of risks across the organization
- 4. Automated escalation and tracking of critical risks and associated mitigations
- 5. Common terminology and data
- 6. Proven IT solution

### **Towards Pervasive GRC**



MetricStream GRC SUMMIT 2014 MIDDLE EAST December 10-11, 2014 | Dubai, UAE

### Business Resilience Management MetricStream Implementation Framework

**Ihsan Ul Haque** Coordinator Business Resilience Management Bahrain Petroleum Company Bahrain

This document is property of Bahrain Petroleum Company

MetricStream GRC Summit Middle East 2014