Introduction to ERM
(Enterprise Risk Management)

ProMedica | Your health. Our mission.

Jonathan Burns

- Director of Finance for Paramount Health Care since November 2014
- Relocated to NW OH from Lexington, KY
- Prior roles in higher education and banking/finance
- Learned about ERM due to compliance regulations and implemented Paramount's ERM structure and process

- Jonathan.Burns@ProMedica.org
- 419-887-2500

Agenda

- Define ERM
- Benefits of ERM
- Components of ERM
- Governance Structure
- Define SRM

Define ERM

Enterprise Risk Management (ERM):

"A process effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Source: ermInsights and John Bugalla and
COSO (Committee of Sponsoring Organizations)

Define ERM

- **ERM** is the process of planning, organizing, leading, and controlling the activities of an organization in order to minimize the effects of risk on an organization's capital and earnings.
- **Strategic Risk Management** (SRM) is a business discipline that drives deliberation and action regarding uncertainties and untapped opportunities that affect an organization’s strategy and strategy execution.

Source: ermInsights and John Bugalla

Define ERM

ERM consists of active and intrusive processes that:

1) are capable of challenging existing assumptions about the world within and outside the organization;
2) communicate risk information with the use of distinct tools (such as risk maps, stress tests, and scenarios);
3) collectively address gaps in the control of risks that other control functions (such as internal audits and other boundary controls) leave unaddressed; and, in doing so,
4) complement - but do not displace - existing management control practices.

Source: ermInsights and John Bugalla and
COSO (Committee of Sponsoring Organizations)

Agenda

- Define ERM
- Benefits of ERM
- Components of ERM
- Governance Structure
- Define SRM

Benefits of ERM

- Enhance board risk oversight responsibilities
- Required in certain industries (financial, insurance)
- Executive risk-informed decision making
- Individual risk silos do not work
- Create new measurable value

Source: ermInsights and John Bugalla

Benefits of ERM

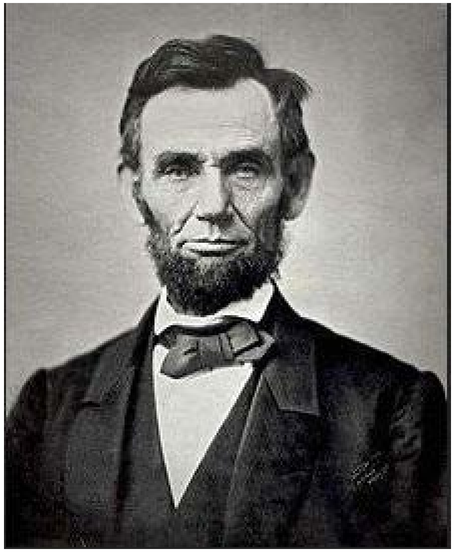
- Volatility and uncertainty abound
- Competitive advantage is critical for future success
- Avoid the strategy-execution gap
- Enhance audit and compliance
- Lessen the impact of adverse events

Source: ermInsights and John Bugalla

Benefits of ERM

Planning for Performance:

- “Give me six hours to chop down a tree and I will spend the first four hours sharpening the axe.”
  - Abraham Lincoln

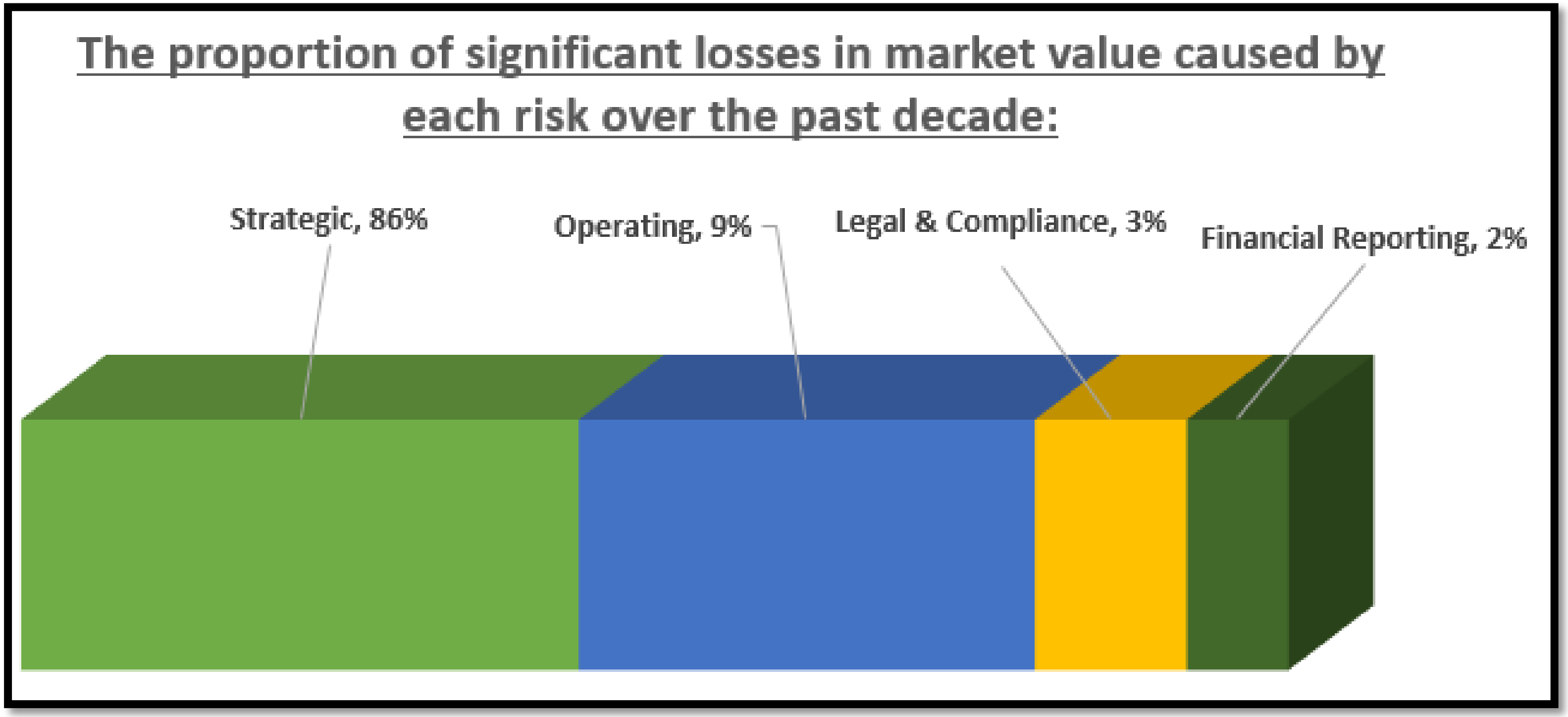


- The process of getting there will ultimately determine your final result. Planning is a very important step to business strategy.

Source: ermInsights and John Bugalla

Benefits of ERM

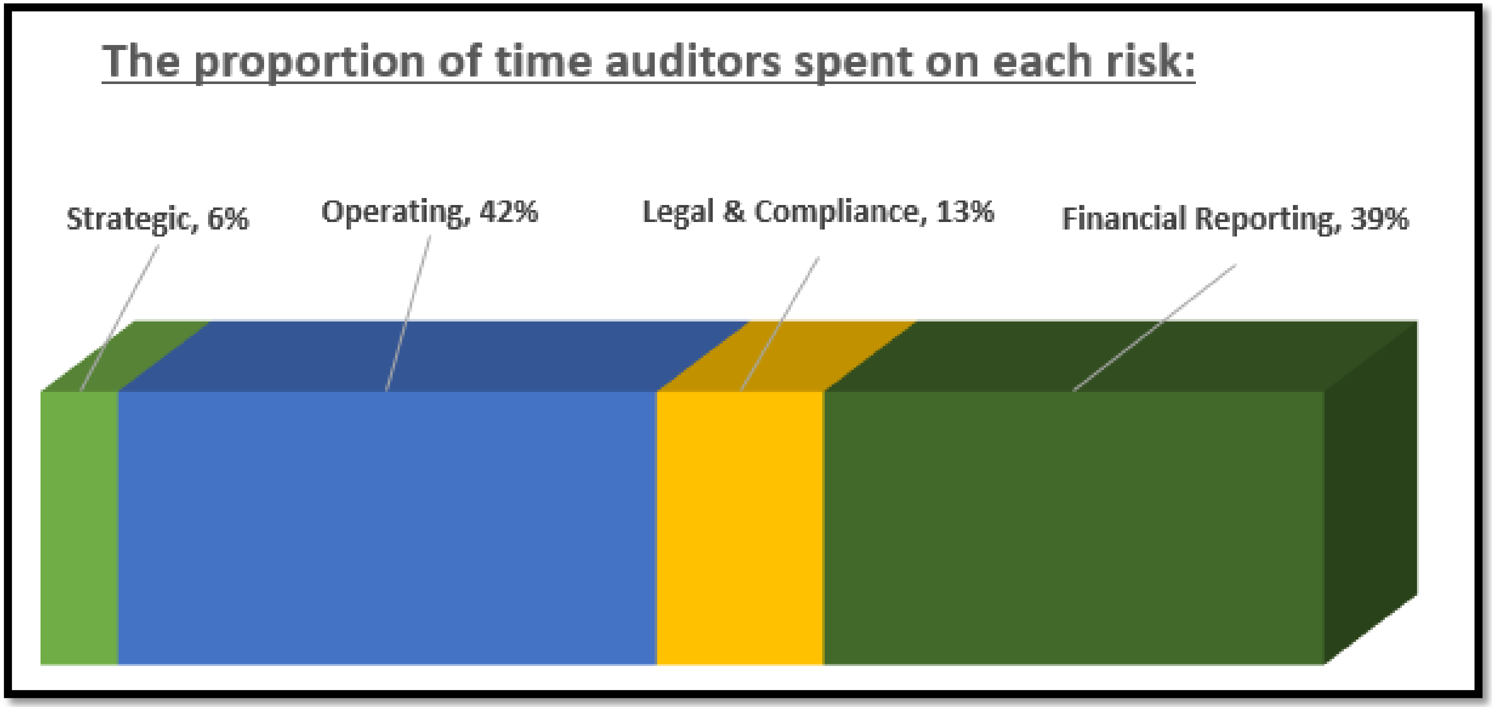
Strategy-Execution Gap:



Source: ermInsights and John Bugalla; CEB, Harvard Business Review

Benefits of ERM

Strategy-Execution Gap:



Source: ermInsights and John Bugalla; CEB, Harvard Business Review

Benefits of ERM

Sample Risk Categories:

- Underwriting
  - Model Risk
  - Product Pricing
  - Reserves
  - Natural Catastrophe
- Strategic
  - Regional Concentration of Risk
  - Reputation
  - Global/National Economy
  - Competition
- Operational
  - Availability of Reinsurance
  - Regulatory Risk
  - IT Risk
  - Personnel Risk
- Market
  - Investment Market Risk
- Liquidity
  - Claims
- Credit
  - Reinsurer Credit

Source: Willis Re and Willis Towers Watson

Agenda

- Define ERM
- Benefits of ERM
- Components of ERM
- Governance Structure
- Define SRM

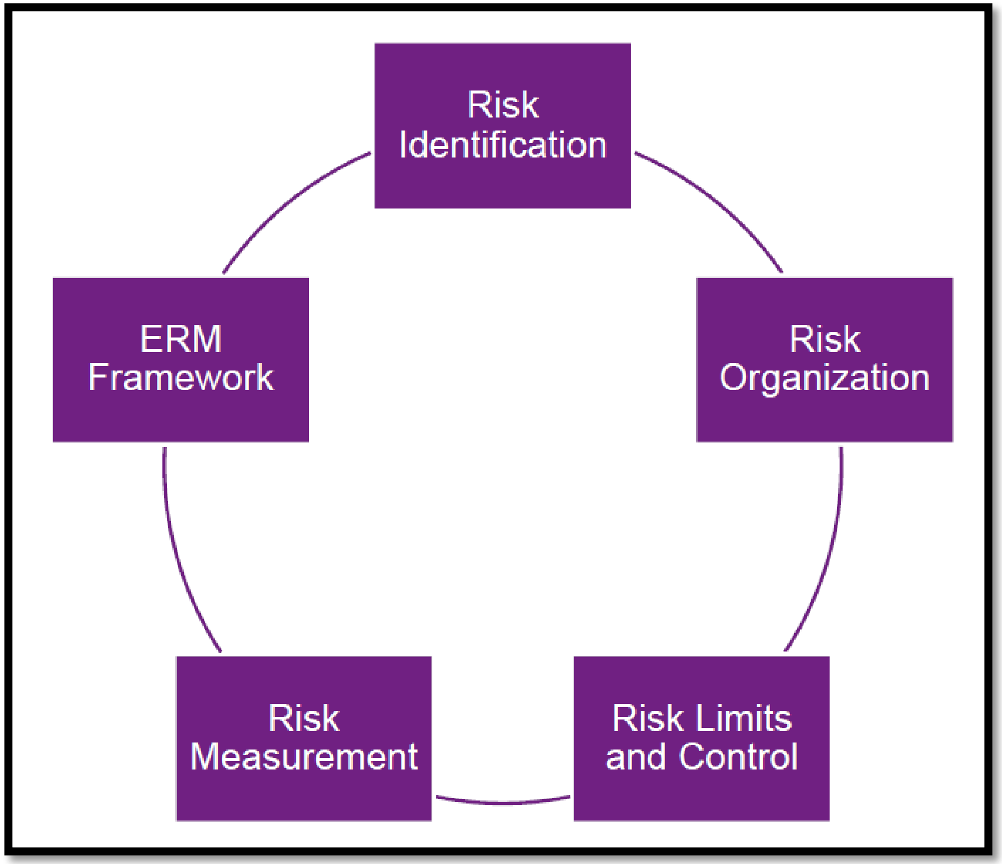
Components of ERM

Steps to design an ERM:

- Define desired program
- Implement ERM charter
- Establish risk appetite
- Define tolerance levels
- Start risk assessment process

Components of ERM

Five Key ERM Practices:



Source: Willis Re and Willis Towers Watson

Define desired program:

- Use a gap analysis to survey leadership for desired outcome of ERM

Source: ermInsights and John Bugalla

Components of ERM

Criterion 1: Risk Organization & Governance

Foundational — **Common Practice** — **Best in Class**

Foundational

- Risk management function centered on compliance, audit and controls
- Silo-based risk management processes

Common Practice

- Commitment to ERM from top management and Board
- Established risk officer or head of risk position (may not be solely focused on risk)
- Functioning cross-functional senior management risk committee
- Risk management viewed as a "partner" by the business units
- Resources dedicated to risk management at the enterprise level
- Existence of some risk policy documentation
- Management "working group" forum for discussion of risk issues
- A more holistic/enterprise view of risk
- Risk management roles and risk ownership formally defined
- Training provided to risk management staff and risk owners

Best in Class

- Functioning cross-functional senior management risk committee
- Risk management viewed as a "partner" by the business units
- Established CRO with authority at a senior level, reports to the CEO and with independent access to the Board
- ERM roles and responsibilities established and defined including ERM staff, risk owners, committees and Board
- Committee charters defined — roles, responsibilities, membership, reporting
- Clearly documented risk policies, procedures, and risk baring capacity and appetite
- Formal information flow from functions to ERM, senior management, and the board
- ERM/SRM duality is recognized - upside gains
- Strong risk owners at function level identifying both risks and opportunities
- Emerging threats and opportunities identified and analyzed
- ERM/SRM integrated and aligned with corporate strategy
- Strategic information reported to board

Source: ermInsights and John Bugalla

Components of ERM

Criterion 2: Risk Appetite and Tolerance

Foundational

- Individual risk limits (e.g., trading, credit, operating, investment), mostly based on management intuition and/or tradition
- Limited monitoring and reporting of violations to risk tolerances but not tied to corrective action and/or revised risk tolerances, as needed

Common Practice

- Early stage development of risk appetite statement articulated by senior management, but lacks robustness
- Inclusion of risk appetite in risk identification and assessment process
- Risk limits for individual risk categories articulated at functional level
- Understanding of risk profile in relation to risk appetite
- Clear limits defined and exception management process in place, but not enforced

Best in Class

- Risk appetite statement articulated (quantitative and qualitative) and incorporates multiple stakeholder viewpoints in defining metrics
- Risk appetite and tolerances validated through quantitative modeling
- Annual approval and sign-off by the Board of Directors of key material risks
- Communication of strategy, risk appetite and tolerances throughout the organization
- Modeling/reconciling top-down risk appetite with bottom-up risk limits
- Formal process for vetting models and new products
- Applying risk appetite to decision making, capital deployment, resource allocation
- Enforcement of risk and reward decisions with linkage to compensation/performance
- Incorporation of reputation impact into risk appetite and tolerance statements
- All corporate functions understand purpose of ERM/SRM

Source: ermInsights and John Bugalla

Components of ERM

Criterion 3: Metrics & Measurement

Foundational

- Metrics based on accounting/regulatory reporting requirements
- Measurement techniques for financial and event risks
- Metrics for evaluating risk and reward at operational level exist but are inconsistent and not defined as part of the ERM process

Common Practice

- Robust measurement of some key risks (e.g. pricing models for all transactions)
- Risk prioritization through qualitative and quantification of key risks (heat map)
- Use of internal SMEs and root cause analysis
- Simplified approach to stress testing capital adequacy
- Limited scenario planning and/or SWOT analysis
- Some risk metrics at the function level, but inability to aggregate at the enterprise level
- Company metrics are established and used to prioritize opportunities and support the evaluation of an individual opportunity

Best in Class

- Measurement metrics for all risk categories with aggregation capabilities
- Modeling key risks in common terms
- Metrics for evaluating risk and reward at operational level exist and are consistent and defined as part of the ERM process
- ERM embedded in strategic planning and decision making
- Consistent approaches to risk measurement and impact on value
- Ability to produce results accurately and quickly
- Robust use of scenario planning, analysis and stress testing
- Risk metrics included in individual performance objectives and compensation
- Macroeconomic indicators considered in predictive financial performance

Source: ermInsights and John Bugalla

Components of ERM

Criterion 4: Risk Management Process, Procedures & Controls

Foundational

- Risk management function centered on insurance and other traditional risks
- Internal audit focused on compliance, audit and controls
- Existence of control structure
- Risk-adjusted decisions process in place
- Risk prioritization based on qualitative information
- Silo-based management of key risks
- Business continuity plans developed
- Operational risk controls defined and in place

Common Practice

- Consistent risk identification and assessment process
- Enterprise-wide view of key risks to the strategy
- Risk treatments and options developed for key risks
- Standardized process for insurance, financial risk management (credit, market and operational)
- Regular monitoring and analysis of extreme events
- Risk management knowledge exists at the senior management level
- Risk policies are clearly defined and communicated, and have influence on functional management
- Management and risk owners understand importance of and role in managing risk within the operations
- Formal approach to identifying, quantifying and monitoring operational risks

Best in Class

- Enterprise-wide view of key risks to the strategy
- ERM goals and objectives articulated and aligned with business strategy and objectives
- Risk-adjusted decisions process in place
- Value driver analysis in place
- Appropriate risk and control processes (identification, measurement, reporting and checkpoints against risk tolerances) in place
- Robust framework for stress testing and scenario analysis models
- Use of value mapping tools
- Risk culture aligned and implemented
- Understanding the portfolio effect of risk
- Risk financing options clearly understood
- ERM/SRM collaborating with compliance and audit

Source: ermInsights and John Bugalla

Components of ERM

Criterion 5: Risk Monitoring, Reporting & Communication

Foundational

- Ad hoc reporting. although there may be significant lag time
- Reactive response to risk events and reports
- Existence of risk reporting by business line and for the enterprise
- Reporting developed for regulatory compliance
- Management reports developed for audit findings and controls
- Financial disclosure requirements

Common Practice

- Risk management dashboard that includes reporting metrics linked to risk appetite and tolerances
- Existence of risk reporting by business line and for the enterprise
- Ability to produce reports based upon timely and useful information that allow for actionable decision making
- Reporting is data-oriented vs. information oriented and not easily actionable
- Quarterly or monthly ERM reporting to executive management
- Annual reporting of key risks to the Board
- Reporting is tailored appropriately to the audience to whom it is delivered
- Annual third-party stewardship reports
- Technology is used to support the business strategy and the implementation and monitoring of risk tolerances

Best in Class

- Risk management dashboard that includes reporting metrics linked to risk appetite and tolerances, and strategy
- Ability to produce reports based upon timely and useful information that allow for actionable decision making, and adaption to new strategy
- Flexible reporting and ability to drill down into risk information
- Integration of ERM components, data, systems
- Reporting is tailored appropriately to the audience to whom it is delivered
- Emerging threats and opportunities included in reports
- Strategic risks are reported to board on quarterly basis
- Risk management is a competitive advantage
- Risk owners report to board and audit verifies
- All corporate functions understand purpose and support ERM/SRM

Source: ermInsights and John Bugalla

Components of ERM

<u>Steps to design an ERM:</u>

- Define desired program
- Implement ERM charter
- Establish risk appetite
- Define tolerance levels
- Start risk assessment process

Components of ERM

<u>Implement ERM charter:</u>

- Developed to formally establish the ERM function
- Based on the desired state as learned via the gap analysis
- Must be approved by the Board or appropriate committee
- Must include:
  - Definition of ERM for the organization
  - Mission
  - Sponsor
  - Frequency of meeting
  - Framework (i.e. COSO 2013)
  - Responsibilities of the committee
  - Focus on key risks & integration with operations

Source: ermInsights and John Bugalla

Components of ERM

Establish risk appetite:

- Determining risk appetite starts by determining the organization's risk capacity
  - An organization's ability to withstand risk when it becomes fact while avoiding unwanted effects

Source	Risk Appetite	Risk Tolerance
ISO Guide 73:2009 *Risk management vocabulary*	Amount and type of risk that an organization is willing to pursue or retain.	Organization's or stakeholders readiness to bear the risk after risk treatment in order to achieve its objectives.
COSO *Strengthening Enterprise Management for Strategic Advantage, 2009*	A broad-based description of the desired level of risk that an entity will take in pursuit of its mission.	Reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve.

Source: ermInsights and John Bugalla

Components of ERM

Risk Appetite:

- Is strategic and is related to the pursuit of organizational objectives
- Should form an integral part of organizational governance
- Should guide the allocation of resources
- Is multi-dimensional, looking at short-term and long-term goals of the strategic planning cycle
- Requires effective monitoring of the risk itself and the organization's continuing risk appetite
- Should directly link to the organization's objectives
- Should be stated precisely enough that it can be communicated throughout the organization, effectively monitored, and adjusted over time
- Helps with setting acceptable tolerances for risk thereby identifying the parameters of acceptable risks

Source: ermInsights and John Bugalla

Components of ERM

Generalized Statement:

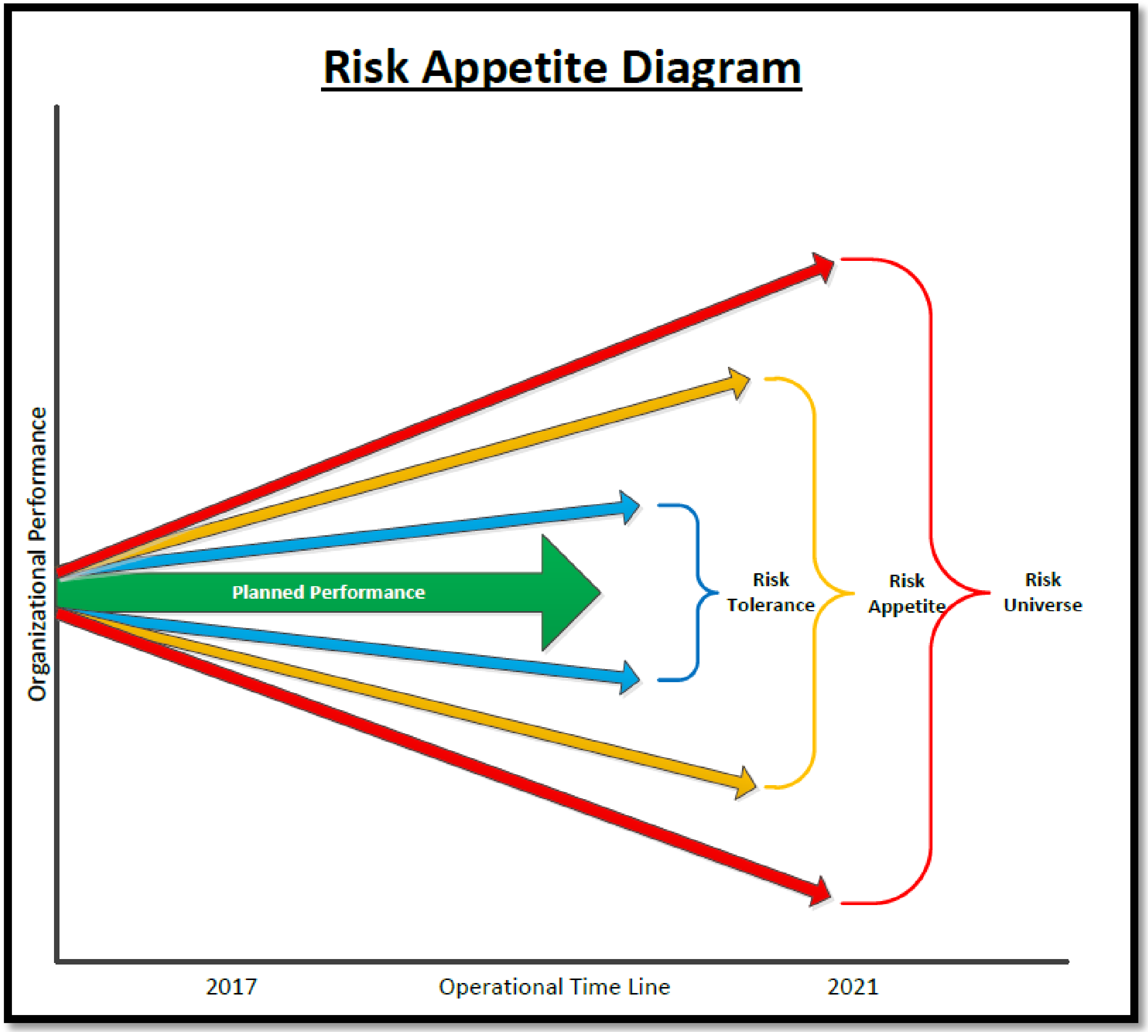
- We take risks to build and grow our business, but only if those risks:
  - Fit our business strategy and can be understood and managed;
  - Do not expose the enterprise to any significant single loss events, we do not bet the firm on any single acquisition, business or product;
  - Do not risk harming our brand

Specified Scoring:

Financial Impact		Reputation Impact	
Cash Flow (US$)	**Dividend Coverage Ratio**	**Customer Satisfaction**	**Score**
CATASTROPHIC >$75MM (Greater than 50% of Cash Flow)	Negative Deviation to Coverage Ratio greater than 13% (more than 87%)	How many complaints would it take generate a serious concern? Accumulation of operational incidents leads to loss of key client; and/or SLA credits requiring Board approval	Very High = 5
MAJOR $37.5MM - $75MM (25 - 50% of Cash Flow)	Negative Deviation to Coverage Ratio from 7 - 13% (from 81 - 87%)	How many complaints would it take to generate a major concern? Accumulation of operational incidents leads to critical client relationship status; and/or SLA credits requiring ELT approval	High = 4
MODERATE $15MM - $37.5MM (10 - 25% of Cash Flow)	Negative Deviation to Coverage Ratio from 5 to 7% (from 79 - 81%)	Critical operational incident impacting multiple clients at a single site; and/or SLA credits requiring Division approval	Medium = 3
MINOR $7.5MM - $15MM (5 - 10% of Cash Flow)	Negative Deviation to Coverage Ratio from 2 - 5% (from 76 to 79%)	Critical operational incident impacting single client at a site; and/or SLA credits requiring Department approval	Low = 2
No Material Impact < $7.5MM (0 - 5% of Cash Flow)	Negative Deviation to Coverage Ratio less than 2% (up to 76%)	Multiple operational incidents that impact a single clients or multiple clients; and/or minimal to no SLA credits	Very Low = 1
No Material Impact < $7.5MM (0 - 5% of Cash Flow)	Favorable Deviation to Coverage Ratio less than 2%	Achieving SLA targets for customers at a site	Very Low = 1
MINOR GAIN $7.5MM - $15MM (5 - 10 % of Cash Flow)	Favorable Deviation to Coverage Ratio from 2 - 5%	Achieving occupancy and retention targets	Low = 2
MODERATE GAIN $15MM - $37.5MM (10 - 25% of Cash Flow)	Favorable Deviation to Coverage Ratio from 5 - 7%	Consistent Net Promoter Score of 9-10 at single site	Medium = 3
HIGH GAIN $37.5MM - $75MM (25 - 50% of Cash Flow)	Favorable Deviation to Coverage Ratio from 7 - 13%	Consistent Net Promoter Score of 9-10 across multiple sites and product platforms	High = 4
GOLD MINE >$75MM (Greater than 50% of Cash Flow)	Favorable Deviation to Coverage Ratio greater than 13%	Superior customer service reputation leading to growth of location capacity and product platforms	Very High = 5

Source: ermInsights and John Bugalla

Components of ERM



Source: ermInsights and John Bugalla

Components of ERM

<u>Define tolerance levels:</u>

- To evaluate a new risk/opportunity/program:
  - What is the worst/best case scenario?
  - What does it cost/return if it happens?
  - What is the mitigation strategy?
  - Based on a cost comparison, do you mitigate or accept the risk?
- Does the evaluated risk remain within the established risk tolerance levels?
  - If yes, leadership may make the decision to move forward or not.
  - If no, is it within the risk appetite (all known risks combined still within the appetite range)?
    - Yes, go to risk council (internal management) for final approval
    - No, go to risk committee of Board for final approval

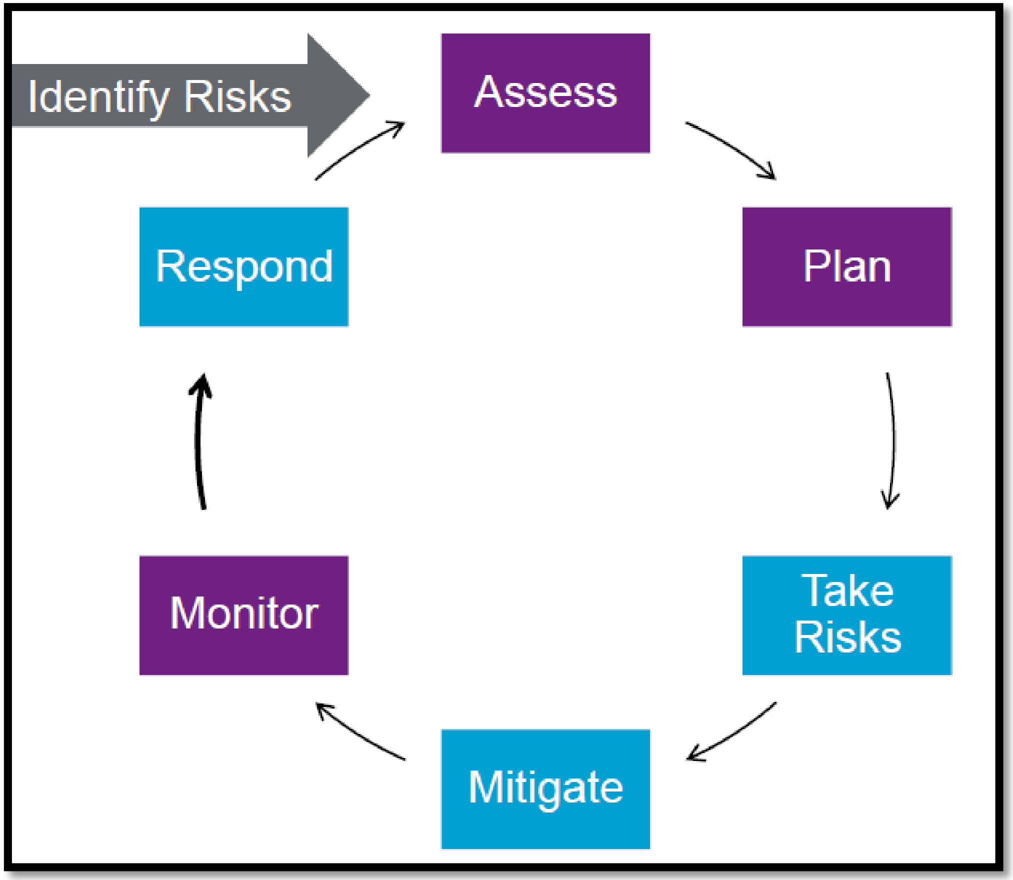
Components of ERM

Risk Tolerance:

- Typically a financial indicator (i.e. % of revenue)
- Good benchmark is at what threshold is reporting outside the organization required
  - Bond covenants
  - Change in bond rating
  - Risk Based Capital (RBC) level
  - MediCare STAR rating

Components of ERM

Start risk assessment process:



Source: Willis Re and Willis Towers Watson

Components of ERM

Sample Annual Risk Assessment Cycle:

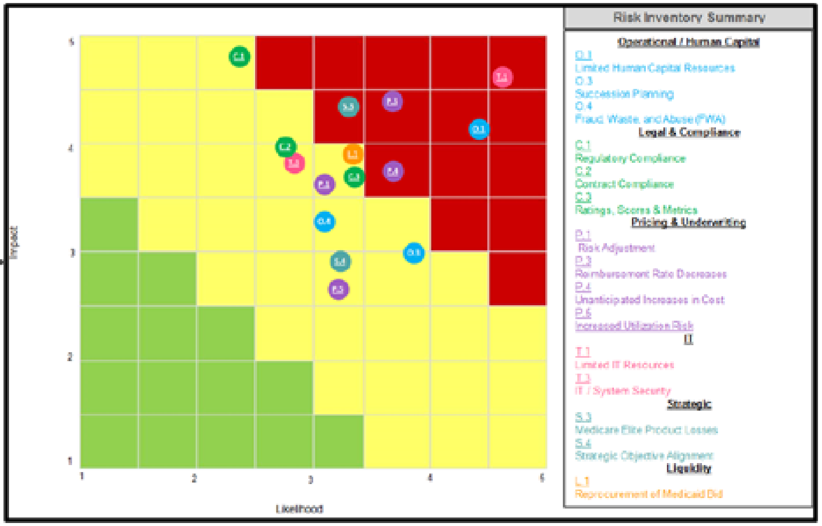
ERM/SRM Process Begins

Risk Surveys: survey SMT to identify different risks within their unit/company (market, credit, reputational, strategic, legal & compliance, IT, operational, HR, liquidity, pricing)

Consolidation of Survey Responses: identify top (most common) risks and emerging risks

Voting/Ranking: SMT members vote on likelihood and financial impact of top risks for each entity

Heat Map: develop for each entity based on voting results



Risk Owners: Vice Presidents and above identify risk owners

Mitigation Strategies: risk owners identify current and future activities that mitigate the identified risks

Quarterly Reporting: mitigation strategies are updated by risk owners quarterly with updates to what was proposed and any new activity

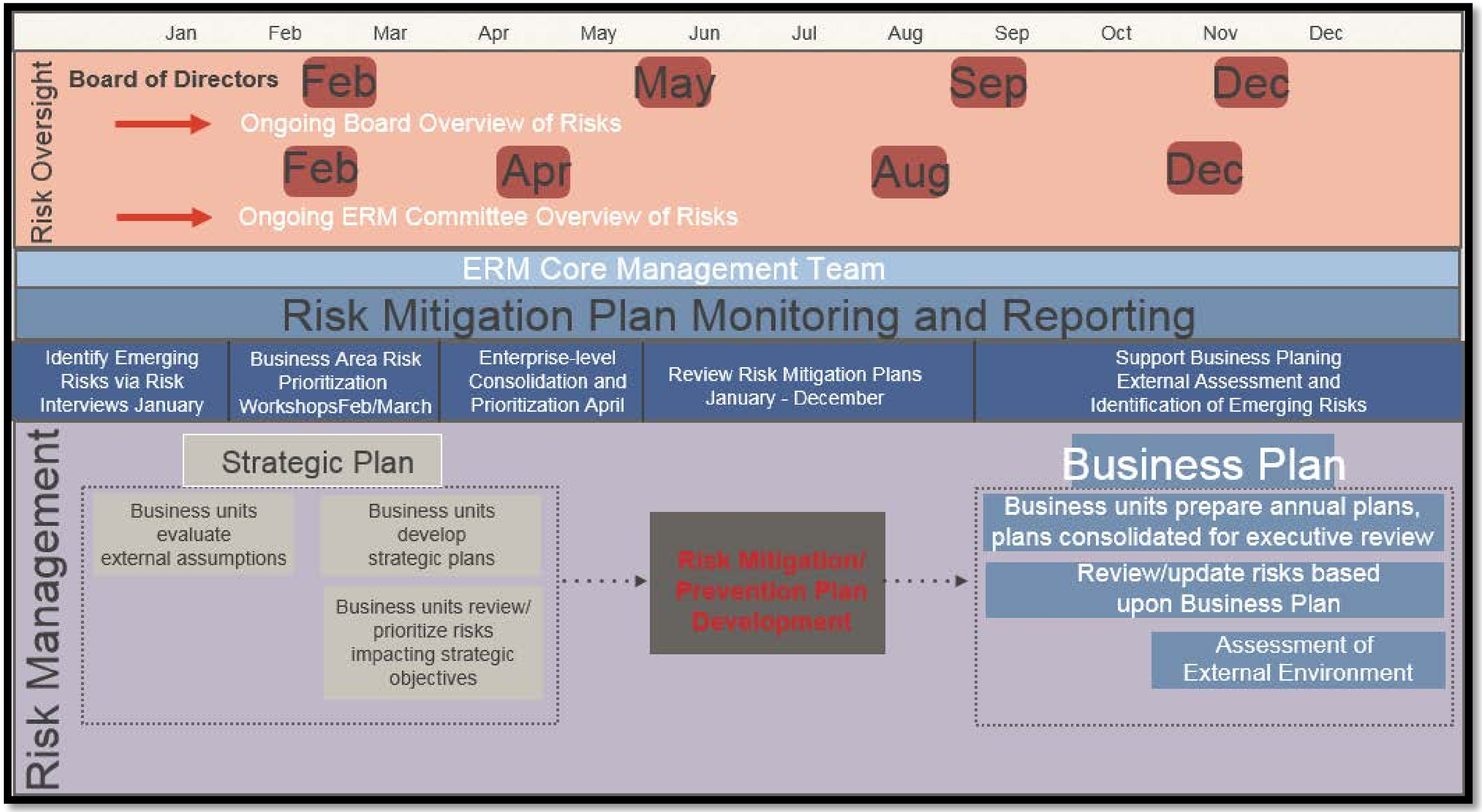
Stress Testing: identify and test scenarios for stress testing and financial performance/solvency

Consolidation for PHS: consolidate entity risks, create heat map, etc. for PHS level

Reporting: report to Board (A/C Committee) based on risk appetite and tolerance levels

End
(begin survey process again)

ERM Model Example:



Source: ermInsights and John Bugalla

Agenda

- Define ERM
- Benefits of ERM
- Components of ERM
- Governance Structure
- Define SRM

Governance Structure

Risk Officer

Responsible for:

- Risk Policy
- Risk Analytics and Reporting
- Business Unit CRO's
- Communication

Member of Capital Management Committee

Leader of Risk Management Committee

Risk Committee

- Review & approve risk policy
- Oversee enforcement
- Ensure ERM objectives are met
- Approve ERM Strategies of business units
- Periodic review of ERM programs
  - Especially focusing on effectiveness of programs in changing environments

Objective: Make sure that people have clear responsibilities.

Risk Owners

Responsibilities:

- Risk Identification
- Risk Measurement and Reporting
- Create plan for risk
  - Propose Risk Limits
  - Risk Mitigation
- Implement Plan

Audit - Internal

Ongoing assurance of Compliance with Risk Policies

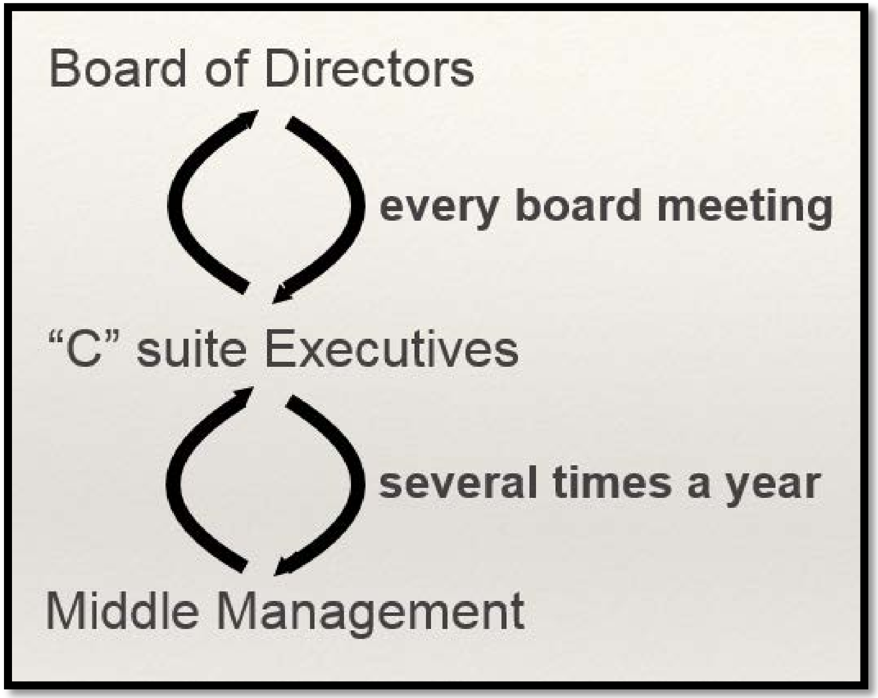
Audit – External

Periodic review of entire ERM program

Source: Willis Re and Willis Towers Watson

Governance Structure

<u>Suggested Model / Best Practice:</u>



- Top-down risk identification
- Strategic analysis drives technical analysis and quantification
- Fewer, more aggregated risks
- Dynamic risk perspectives include opportunities
- High level of board engagement

Source: ermInsights and John Bugalla

<u>Risk Culture:</u>

- The norms of behavior for individuals and groups within an organization that determine the collective ability to identify and understand, openly discuss and act on the organization's current and future risks.
- "No matter which approach to ERM is taken, it is the organizational talent who will have to execute it – people are the strategic plan because human capital has become the fundamental advantage of competitive advantage." – John Bugalla

Source: ermInsights and John Bugalla

Agenda

- Define ERM
- Benefits of ERM
- Components of ERM
- Governance Structure
- Define SRM

Define SRM

<u>Strategic Risk Management:</u>

- A business discipline that drives deliberation and action regarding uncertainties and untapped opportunities that affect an organization's strategy and strategy execution.
- Strategy – is the set of resource allocation decisions that help a firm create and sustain a competitive advantage.
- "It is not the strongest of the species that survives, not the most intelligent that survives. It is the one that is most adaptable to change." - Charles Darwin

Source: ermInsights and John Bugalla

Define SRM

- The primary difference between ERM and SRM is the degree of integration with strategic planning and the focus on *upside risk/opportunities* vs. just risk reduction.
- Some of the key benefits/reasons for SRM:
  - Outside forces are creating volatility and uncertainty at a faster pace, risks are more complex and interconnected, and industry consolidation amplifies the effect.
  - An integrated SRM program may provide a competitive advantage by identifying/realizing opportunities.
  - SRM helps avoid the strategy-execution gap.

Source: ermInsights and John Bugalla

Define SRM

Strategic Planning:

- A survey at the 2014 Chief Strategy Office summit showed that only 13% of 132 respondents felt they achieved 80% or more of the expected value of their strategic initiatives.
- 82% of Fortune 500 CEOs feel their organization did an effective job of strategic planning. However, only 14% of those same CEOs indicated that their organization did an effective job of implementing the strategy.

Source: ermInsights and John Bugalla; Forbes

Define SRM

Competitive Advantage:

- Most strategic initiatives are:
  - The logical next step in existing strategic direction
  - Increased investment in our existing strategy in our immediate market segment
- And emerge from:
  - New ideas from existing management
  - New information about the business or marketing environment
- And take time:
  - 7 months to decide what to do
  - Additional 13 months for implementation

Source: ermInsights and John Bugalla;
McKinsey Global Survey

Define SRM

Strategic Plan Components:

- Describe the org.'s mission, vision, & fundamental values
- Target potential business arenas and explore each market for emerging threats and opportunities
- Understand the current and future priorities of targeted customer segment
- Analyze the company's strengths and weaknesses relative to the competitors and determine which elements of the value chain the company should make vs buy
- Identify and evaluate alternative strategies
- Develop an advantageous bus. model that will profitably differentiate the company form its competitors
- Define stakeholder expectations and establish clear and compelling objectives for the business
- Prepare programs, policies and procedures to implement the plan
- Establish support organizational structures, decision processes, information and control systems and hiring and training systems
- Allocate resources to develop critical capabilities
- Plan for and respond to contingencies or environmental changes
- Monitor performance

As Plans develop with SRM, the key questions to ask cover both the traditional downside risks and upside opportunities:

- What are the 1-3 *worst* things that could happen if we do this?
- What can we do to *reduce* both the probability of this happening and the impact of it happens
- What are the 1-3 *best* things that could happen if we do this?
- What can we do to *increase* the probability of this happening and the impact if it happens
- Debate the assumptions, not forecasts – understand the fundamentals and performance drivers.
- All assumptions should be risk informed and linked to SRM
- Allows all to speak a common language
- Discuss and understand resource deployments early
- Clearly identify priorities – not all are equally important
- Continuously monitor performance
- Reward and develop capabilities

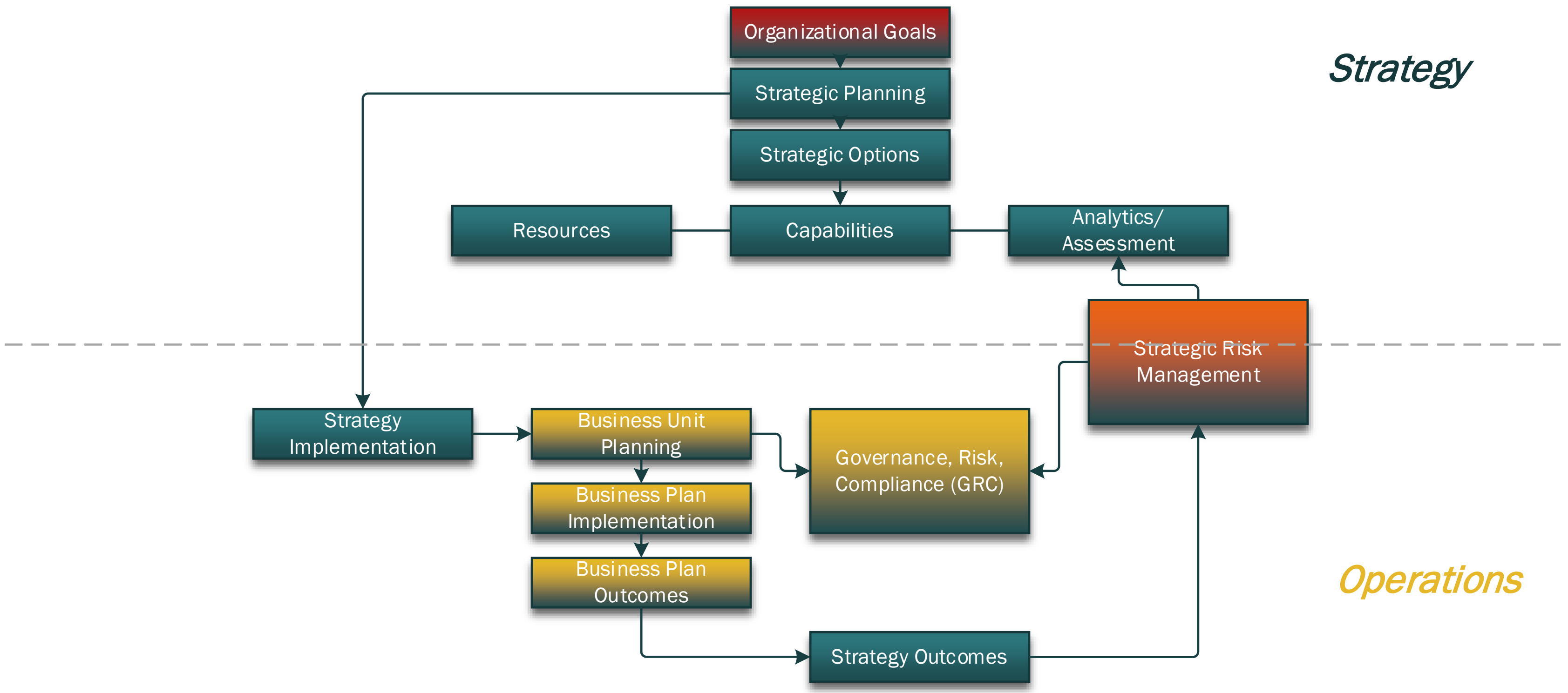
Source: ermInsights and John Bugalla

Define SRM

- **Board** – Provide to board the info that will assist them in performing their required risk oversight responsibilities and enhance their strategic understanding of the key performance indictors driving the business to better engage exec. mgt. in strategic decision making.
- **Execs** – Deliver to execs info that will assist them in making strategic decisions to grow the business and evolve the business model.
- **Leadership** – Provide the organizational leadership team with info necessary to monitor and evaluate the performance of the ERM program.
- **Business Unit Leaders** – Deliver to bus. unit leaders and middle management the risk-informed analysis to make tactical decisions that support the day-to-day transactions of running the business.

Source: ermInsights and John Bugalla

Define SRM



Source: ermInsights and John Bugalla

Summary

- Strategic Planning typically makes assumptions about the business, while risk management considers the uncertainties surrounding these assumptions during implementation.
- But if strategists do not think carefully and comprehensively about the risks that might be encountered in their plans, risks will be missed, more than any after-the-fact risk management can mitigate.
- “*Everyone has a plan ‘till they get punched in the mouth.*” - Mike Tyson

Questions?