Towards Integrated GRC

Isabel Smith
Director Internal Audit | Johnson & Johnson

**2015 - Case Study**

MetricStream
GRC
SUMMIT 2015
May 11-13, 2015
ARLINGTON, VA
WASHINGTON, DC AREA

Maximize Business Performance Through GRC Journey

Agenda

1. Organization Overview: Vision and Key Facts

2. Organizational Structure: Lines of Business and Key Stakeholders

3. Business Challenge Identification: Top Challenges Facing Organization and Industry

4. GRC Program Objectives and Strategies

5. Overcoming Business Challenges

6. Technology as an Enabler

7. Successes and Benefits

8. Key Learnings and Best Practices

9. Audience Questions and Discussion

Key Facts About the Organization

Johnson & Johnson has more than 250 companies located in 60 countries around the world with 128,000 employees. Our Family of Companies is organized into several business segments comprised of franchises and therapeutic categories.

Consumer

Medical Devices & Diagnostics

Pharmaceuticals
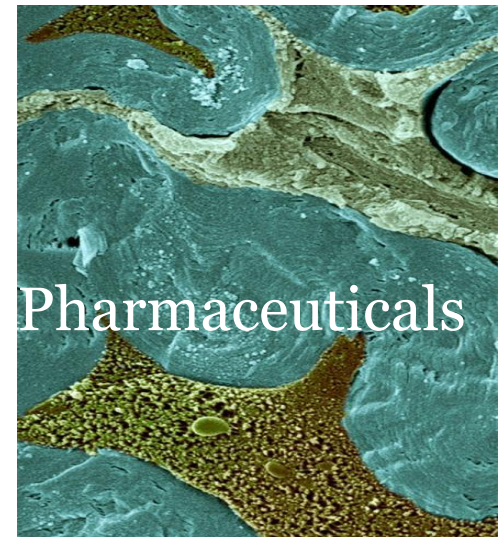
A Strong Business
Largest and Most Diversified Health Care Company in the World

31 Consecutive years of adjusted earnings increases*

53 Consecutive years of dividend increases**

AAA RATED

~70% of sales from #1 or #2 global market share position

~25% of sales from products launched in past 5 years

~70% of 10 year Free Cash Flow returned to shareholders

* Non-GAAP measure; excludes special items
** Inclusive of the April 2015 dividend declaration
*** Non-GAAP measure; Cash Flow from Operations less Capital Expenditures
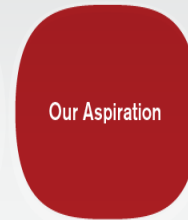
Our Enterprise Strategic Framework

The success of our enterprise
is built on Our Credo and a unique set
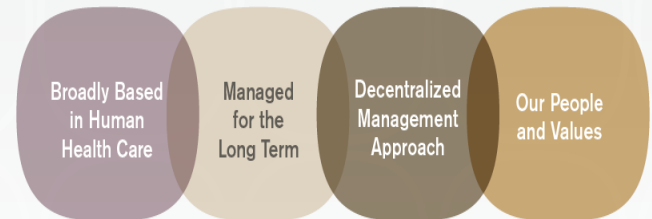of strategic principles

Our Aspiration

By caring, one person at a time,
we will help billions of people live
longer, healthier, happier lives.

Our Credo

- We provide **patients and consumers** with high quality health care products, services and solutions driven by their needs and insights

- We provide our **employees** with training and development programs and strive for a diverse, inclusive environment to better serve the needs of our patients and customers

- We work to strengthen **communities** by offering our training, developing medicines for neglected diseases, funding grant
and donations, and collaborating with third parties

- We commit to our **shareholders** by running our business
in a financially sound and responsible fashion, so that our shareholders should realize a fair return on their investment

Our Credo is a constant in a time of remarkable change

Our Credo

Framework for Enterprise Risk Management

J&J Enterprise Risk Management Framework Components

Goal

Foster a culture of risk management to help the enterprise maintain the provision of quality products, protect patient safety and ensure appropriate relationships with customers.

1. Identify and Assess Internal and External Risks
2. Determine Appropriate Risk Response
3. Establish Policies and Procedures, Controls, Systems and Accountability to Support Response
4. Communicate Risks and Mitigation Plans
5. Monitor Effectiveness of Mitigation Efforts

Business Challenges Faced

Challenges related to People:

- 'Decentralized' environment
- Consensus oriented

Challenges related to Processes:

- Process priorities varied between different compliance domains
- Highly Regulated

Challenges related to Systems:

- Multiple systems with various data structures
- Decentralized

Challenges related to Resources:

- Duplication of effort in disparate processes and systems
- Subject Matter Expertise tied up with Lower Value Add Activities

Overcoming Business Challenges

Organization and Business Line Approach:

- Matrix Model

- Top down – Bottom Up

Adopted Frameworks:

- COSO Framework

- Practices Influenced by GAMP, CoBiT, ISO31000, ISO27000, etc.

Execution Enablers:

- Committed Leaders

- Part of Enterprise Management Framework

- Cross Functional Governance

- Willingness to 'Walk the Talk'

Technology as an Enabler

With either Point Solutions or Integrated Solutions

- Design the reporting hierarchy with the end in mind
- Build out Risk Libraries
- Governance team owns the platform decisions
- Business /IT partnership

Leveraging the platform is an opportunity not a mandate

MetricStream areas of focus

- Audit-Assessment - Sarbanes-Oxley, Internal Audit and R&D QC groups
- Issue Management –Sarbanes-Oxley, Internal Audit, IT Q&C, Supply Chain Risk Management and R&D QC Enterprise SCRM (Supply Chain) leading Risk management

Other point solutions exist

GRC Program Objectives and Strategies

Program Objectives:

- Common Framework Used to Identify and Manage Risk

- Develop Holistic picture of Risk Coverage

Program Strategies:

- Build on the Credo

- Inform and Influence

Role of Technology in Program

- Driving a more "apples to apples" comparison across risk management functions

- Consistent, cohesive reporting around risk (e.g., types of information, dashboard structure) across risk management functions

Successes and Benefits

Success Metrics and KPIs:

- Enterprise Risk Framework Message Penetration
- Limit the Number of Disparate GRC Systems
- Survey Results from Defined Leadership Group
- Adoption of the Shared Platform meets plan

Key Process Improvements and Efficiencies Gained:

- Alignment on Risk Hierarchy
  - Strategic, Operations, Regulatory, Financial
- Ability to Leverage an Enterprise Technology Platform
- Limited Resources able move up the Value Chain
  - e.g. Sarbanes-Oxley Global standard process across all entities enables continuous monitoring

Key Learning's and Best Practices

Key Learning's:

- Impact of the Company Culture
- Impact of Readiness to Accept
- No one changes without incentives
- Impact of a highly regulated industry

Best Practices:

- Start small and build on success
- Communicate, Communicate, Communicate
- Process streamline first if possible, but…..

The Road Ahead:

- Use data to accelerate the 'journey'

GRC/Quality/Supplier Management Program Objectives and Strategies – early stages

People – one worldwide organization

- Local application

Process - end to end simplification & harmonization
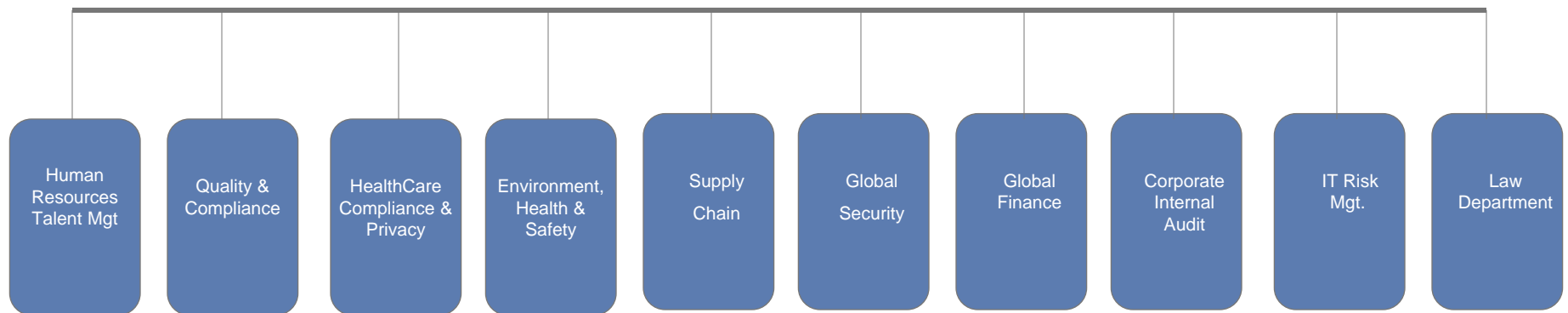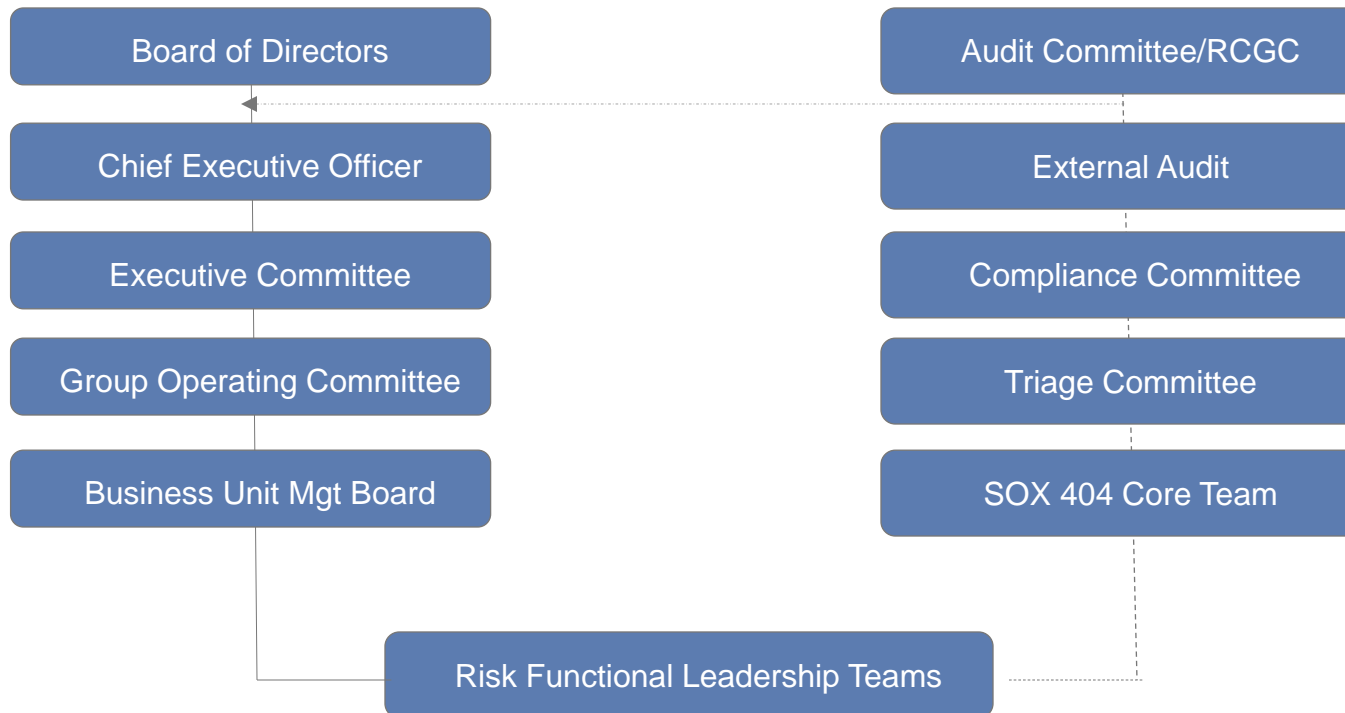
- Internal

- External

Terminology - harmonize risk terms and ratings

Technology

- Align with Enterprise SCRM MS deployment

- Share master vendor data

Governance & Oversight

MetricStream

GRC
SUMMIT 2015
May 11-13, 2015
ARLINGTON, VA
WASHINGTON, DC AREA

QUESTIONS AND DISCUSSION

2015 - Case Study