ISE Central Executive Forum and Awards
Nominee Showcase Presentation

June 9, 2010

Company Name: Northrop Grumman Corporation

Project Name: Governance, Risk, & Compliance

Presenter: Lee Parrish

Presenter Title: Director, Information Assurance

Company Overview

- Northrop Grumman Corporation is a leading global security company that provides innovative systems, products and solutions in aerospace, electronics, information systems, shipbuilding and technical services to government and commercial customers worldwide.

- 120,000 employees

- Revenue: $33.8 billion

- Global Presence

- www.northropgrumman.com

Presentation/Project Overview

- Business Drivers in Risk & Compliance
- Service Delivery
- Key Strategic Initiatives
- Deploy an Enterprise Solution
- NGC GRC Universe
- Project Results
- Lessons Learned/Best Practices
- Q&A

Business Drivers in Risk & Compliance

- Highly Regulated Industry
  - DFAR, ITAR, and SOX represent only three critical regulations that an A&D company must comply with

- Complex solutions entail a highly distributed Supply Chain
  - Managing supply chain risk is becoming increasingly challenging in the A&D industry

- Reputation as a reliable partner is only "table stakes" in this business
  - Managing risk and compliance effectively is an opportunity for competitive advantage
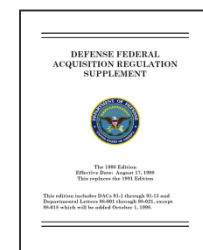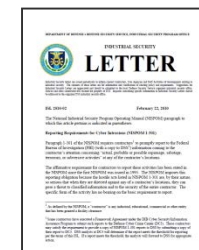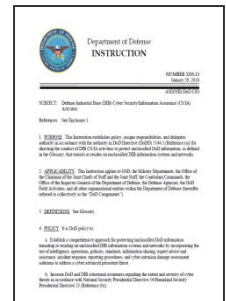
Service Delivery

- Prior to any strategic RM execution, NGC created an effective security service delivery lifecycle.

- Created a GRC Service Catalog Lifecycle: ITIL v3
    - Service Strategy; Service Design; Service Transition; Service Operation

- Key Components:
    - Portfolio of Services; Cost Baseline; SLA/Metrics; Roadmaps
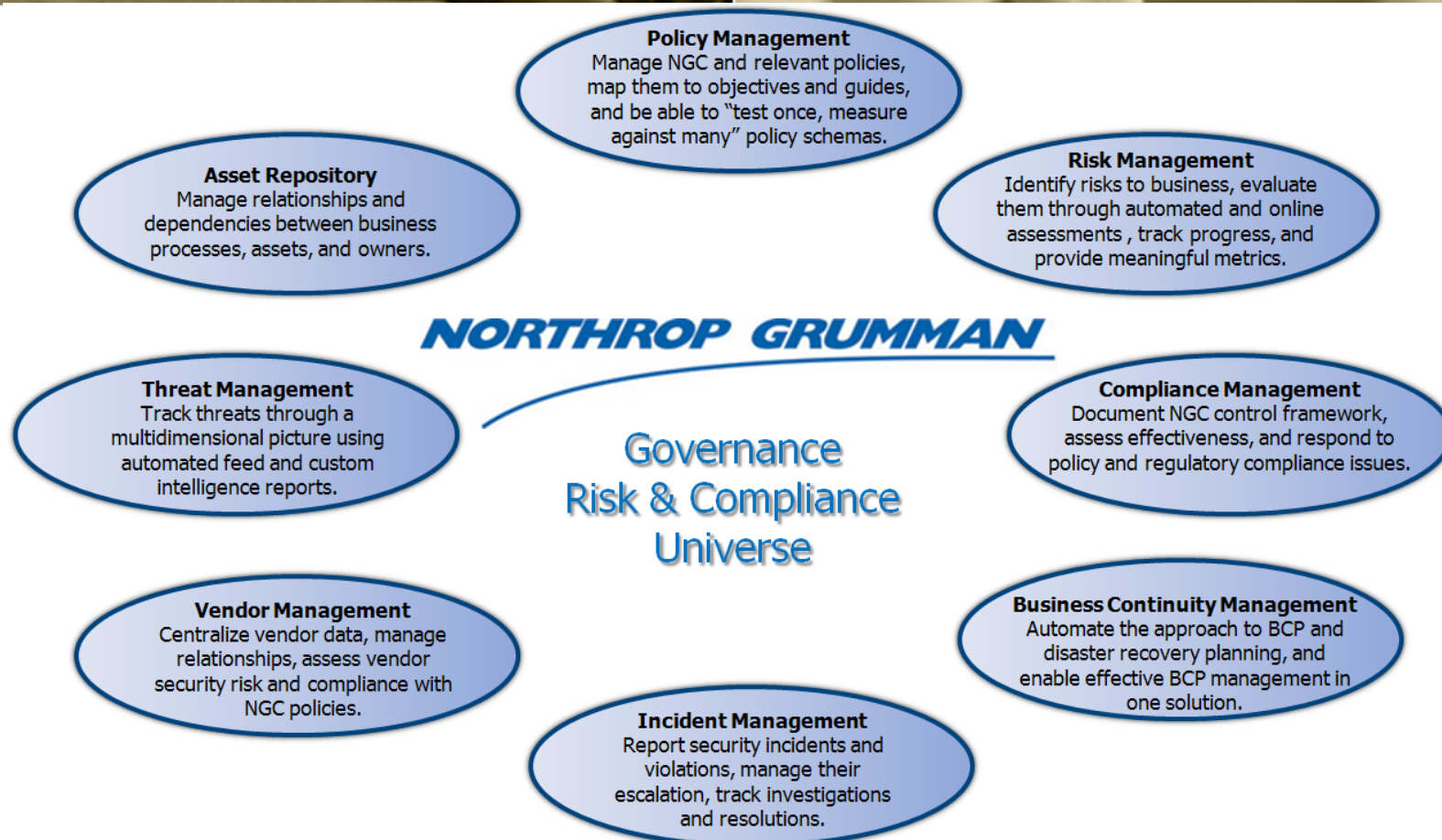
Key Strategic Initiatives

- Initiative 1 – Recognize a Risk Management Lexicon.
- Initiative 2 – Establish a Risk Management Framework
- Initiative 3 – Define Asset Categorization
- Initiative 4 – Develop or Convert Policy
- Initiative 5 – Implement Risk & Compliance Process
- **Initiative 6 – Deploy Enterprise Solutions**
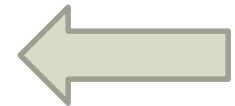
Deploy an Enterprise Solution

- **Risk assessments: we want an automated approach that:**
  - Correlates assets to processes efficiently and effectively
  - Associates vulnerabilities to company assets
  - Integrates data feeds for assets, vulnerabilities, and organizational sources
  - Allows for risk-based assessments for campaigns of varying attributes: asset type, devices, applications, programs, etc.
  - Supports self assessment campaigns by application/device owners.

Policy Management
Manage NGC and relevant policies, map them to objectives and guides, and be able to "test once, measure against many" policy schemas.

Asset Repository
Manage relationships and dependencies between business processes, assets, and owners.

Risk Management
Identify risks to business, evaluate them through automated and online assessments, track progress, and provide meaningful metrics.

NORTHROP GRUMMAN

Threat Management
Track threats through a multidimensional picture using automated feed and custom intelligence reports.

Compliance Management
Document NGC control framework, assess effectiveness, and respond to policy and regulatory compliance issues.

Governance
Risk & Compliance
Universe

Vendor Management
Centralize vendor data, manage relationships, assess vendor security risk and compliance with NGC policies.

Business Continuity Management
Automate the approach to BCP and disaster recovery planning, and enable effective BCP management in one solution.

Incident Management
Report security incidents and violations, manage their escalation, track investigations and resolutions.

Project Results

- <u>Current Security Metrics</u>
  - Performance
  - Informational

- Key Security Indicators
- Key Risk Indicators
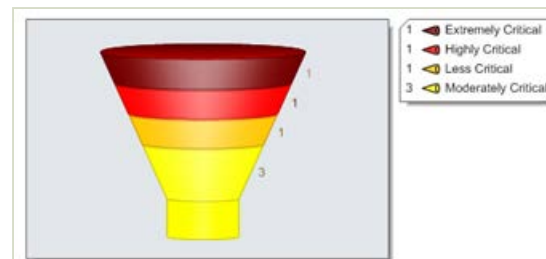
Lessons Learned/Best Practices

- Key Success Factors
  - **Clear Goals**: The IT organization articulated how GRC would enable monetary savings and a better understanding of risk.
  - **Simplicity**: The plan was easy to understand and executable.
  - **Sponsorship and Buy-In**: At the strategic, operational and tactical levels, GRC was recognized as valuable capability.
  - **A Multidisciplinary Team**: The stakeholders contributed their thoughts about what mattered to them in a GRC platform.
  - **Good Supplier Relationships:** RFI & Proof of Concept to choose GRC vendor – key to a selection based on: "best value," mutual commitment to implementation success.

Thank you and Questions

- Questions?