GDF SUEZ E&P UK Ltd

Oil & Gas Cyber Security2011

GDF SUEZ E&P UK Ltd

Information Security Approach and Strategy

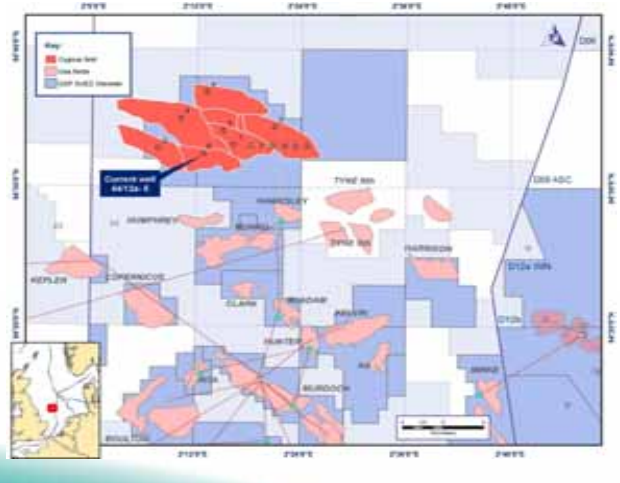
November 2011

Agenda

- Introduction to GDF SUEZ E&P UK
- Why is InfoSec important to GDF SUEZ
- Approaches & activity set
- Self-assessment and benchmarking
- The challenges

GDF SUEZ E&P UK Profile (1)

- Long-standing presence in UK North Sea since 1997
- Growing from non-Operated positions in SNS and CNS to a portfolio of more than 40 licenses.
- Both Operated and non-Operated in SNS, CNS and WoS
- High profile portfolio combining ongoing production, major operated developments and an extensive exploration programme.

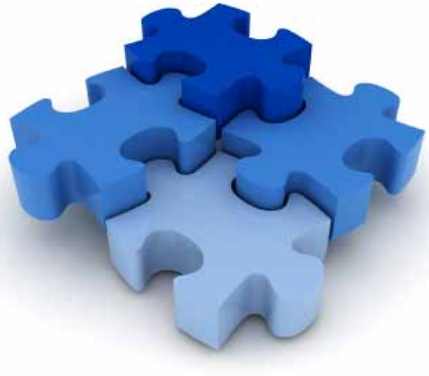


GDF SUEZ E&P UK Profile (2)

- Rapid expansion from 2009 onwards
- Two major operated North Sea projects in 2010-2013:
- Cygnus: Largest SNS discovery in 20 years, an additional ~1.4 tcf GIIP, equity 38.75%
- Juliet: Discovered Dec 2008, fast-track development, an additional ~90 bcf GIIP, equity 51.56%
- 50%+ operated production target
- Three offices, in London and Aberdeen
- Approximately 200 people

Why is Information Security important?

- Successfully becoming a world-class Operator requires us to have all the pieces of the puzzle in place
- Secure, quality information is invaluable for accurate, timely and value generating business decisions
- “Data is the next oil” (Forrester Research, May 2011)
- Security of control systems and the integrity of the flow of data is an important part of our license to operate

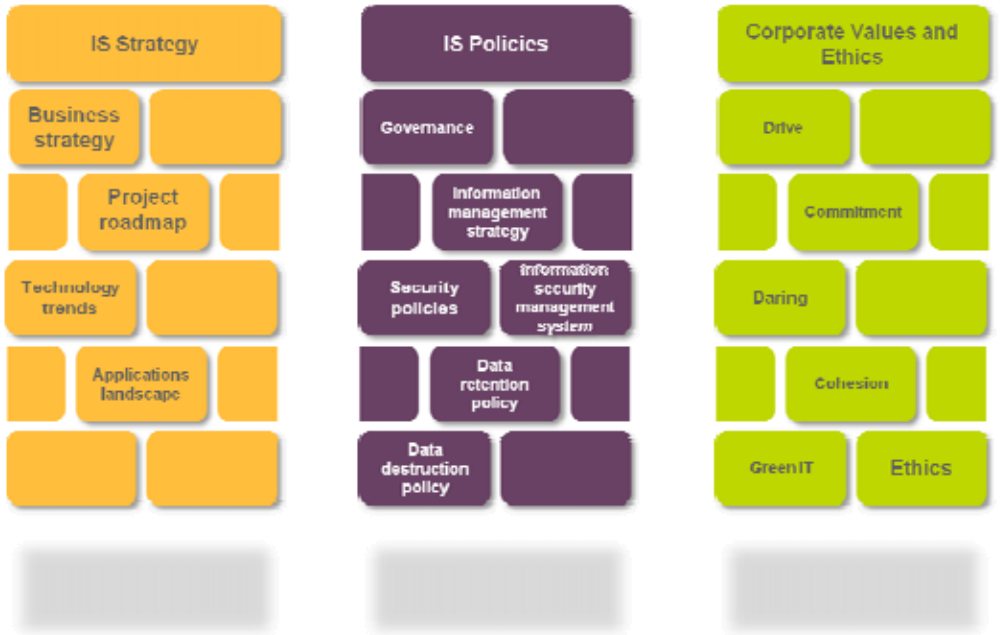


The Corporate Approach

- Global risk analysis and assessment
- Thematic Security Policies based on ISO2700x (TSPs) group-wide
  - Principles, best practices, some directives, opt-out dispensation
- Phased introduction
- Empowerment of local affiliates to respond to local environment
- Rationalisation and integration into the system of Internal Controls

The Local Approach

- ISMS
  - Kick-start the approach and ongoing process
- InfoSec Steering Committee
  - Chaired by MD
  - Meets quarterly to review programme of work
- Binding to global work
  - Thematic Security Policies (TSPs) and integration into System of Internal Controls



- Active engagement
  - ITIL, Partnership Project Management Framework (PPMF) & User Awareness

What Are We Doing?

- Acceptable Use Policy (AUP) and ongoing awareness and education
- Additional AUPs for Administrators acknowledging their elevated privileges and therefore trust within the organisation
- Principle of Least Privilege & Segregation of Duties
- Establishing the Perimeter
  - Physical access and external media
  - Network access
  - Contractual framework
- Governance and Risk Management
- Business Continuity Management

Capital Projects

- Security by Design: security now needs to be built in from the outset.
- Risk Assessment of all the systems and data flows on the platform: what could happen if the various component parts of the system are compromised?
- Remote Access Management: Physical access is controlled by robust IAM processes; Remote Access processes need to be just as robust
- Gjoa SHIELD: implemented by GDF SUEZ E&P's Norwegian affiliate to control access to the Gjoa platform:
  - OLF104 compliant
  - Integration with Work Management System

Self-Assessment and Benchmarking

- **Internal**

  IS risk management process with InfoSec Steering Committee

- **Local Consultancy**

  Bespoke CMMI based rating as part of ITIL

- **Group**

  Rating against ISO27000 and integration into the system of Internal Controls

Strategy is to use multiple methods to generate a rounded view

The Challenges

- User awareness and buy-in
- Balance between usability and security
- Acceptance of changes and managing the perception of “tightening up”/”you don’t trust us anymore”
- Management of risks vs cost
  - Perception of threats and risks
  - Appropriate actions
  - Timeline

www.gdfsuez.com

Engagement and communication.


GDF SUEZ