

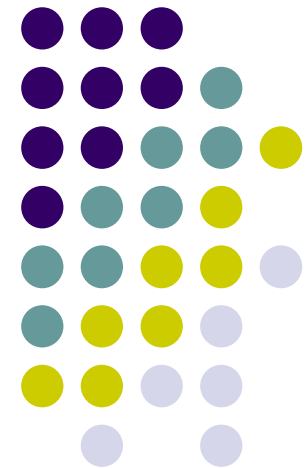
# Information Security Strategy and Governance

## Round Table Meeting



11 June 2008

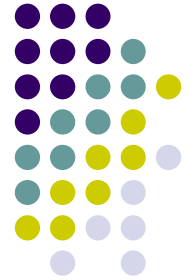
JL Allard, CISM, CISA



**ICT Control**

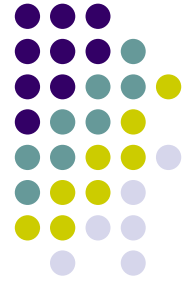


- Origin
- Information Security ?
- Strategy ?
- Governance ?
- Information Security Roles
- Conclusion



# Origin

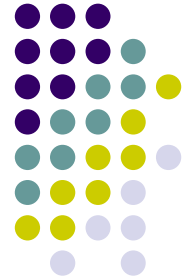
- Research for the French Government
  - DCSSI ([www.ssi.gouv.fr](http://www.ssi.gouv.fr) – owner of EBIOS)
- Multinational European team
- Aim:
  - Guide for Information Security Governance
- Analysis:
  - 5 domains where governance is formalized
  - State, Economy, Enterprises, Projects, IT



# 1. Information Security

Our definitions & concepts

**ICT Control**

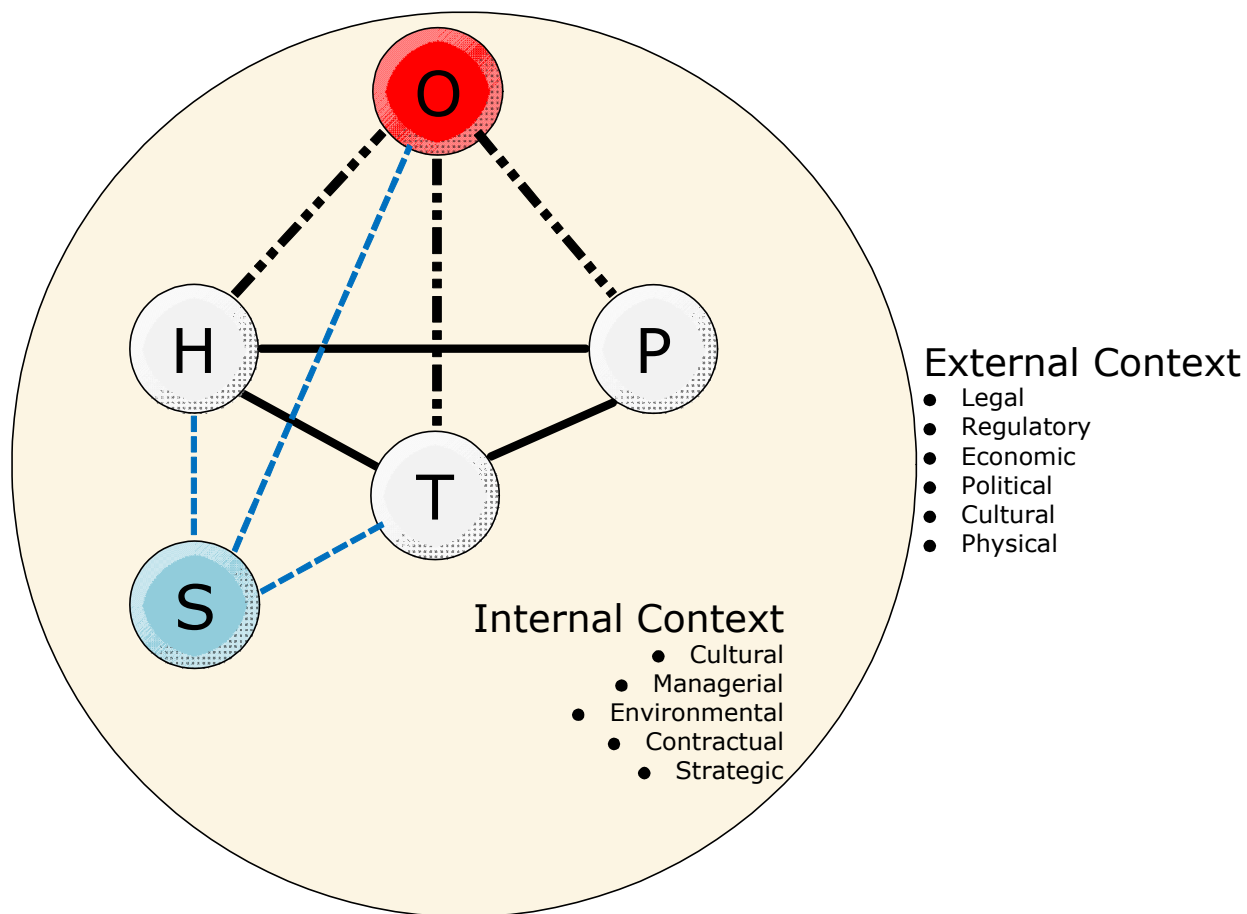


# Information Security

- **Information**
  - Data with signification, value
- **Process**
  - Set of coordinated actions to achieve a goal
- **Information process**
  - Process to 'handle' information through its full lifecycle
- **System**
  - Set of coordinated elements, organized to achieve a goal.
  - Combines the 'actors', the 'means and resources' and the processes
- **Information system**
  - A system to process information and achieve business goals
- **Security**
  - The reasonable assurance to be safe from unacceptable risks.



# Information Security 'SCOPE'



## 2. Information Security Strategy



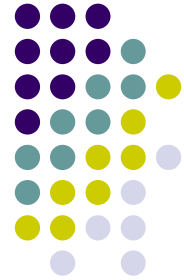
My definitions & concepts

**ICT Control**



# Strategy

- Strategy
  - A way to achieve objectives
- Selecting
  - The best resources
  - The best moment in time/timeframe
  - The best path
  - The best actions ('tactics')
- $W_5HC$
- No move can be an option... if the others get weaker by the time.



# Security Strategy

- Security Strategy
  - A way to go from a given (weak) position to another (better) position through a moving context.
- (some) Security Objectives
  - Less risky position
  - Better recognition to enhance image/position
  - Compliance to legal, regulatory, contractual requirements
- SMART Objectives

# Information Security Strategy



- Several paths
  - The fastest
  - The safest
  - The shortest
  - The cheapest
  - Etc...
- Specificity
  - Same place/resources/business objectives
  - Potentially variable context
  - Mainly in the 4th dimension (time)



# Security SWOT

<h2>Strengths</h2> <ul style="list-style-type: none"><li>•A combination of factors able to firmly sustain the achievement of security objectives.</li><li>•An actual achievement (mastery of the PDCA cycle) of a security objective.</li><li>•Strengths are generally internal and must be preserved to allow obtaining a long term success.</li></ul>	<h2>Weaknesses</h2> <ul style="list-style-type: none"><li>•A factor for nuisance, a lack of protection susceptible to prevent achieving a security objective.</li><li>•Is generally internal and must be resolved to obtain a long term success.</li><li>•Weaknesses are generally internal or caused by constraints.</li></ul>
<h2>Opportunities</h2> <ul style="list-style-type: none"><li>•A factor or tendency that can contribute to achieve a security objective.</li><li>•May resolve or correct a weakness, multiply tenfold the strengths and (if successfully exploited) lead to achieve a security objective.</li><li>•Opportunities are both internal and external.</li></ul>	<h2>Threats</h2> <ul style="list-style-type: none"><li>•A factor or a tendency that presents a potential obstacle, and opening the risk that opportunities can't be exploited or security objectives can't be achieved.</li><li>•May augment the weaknesses and reduce the forces.</li><li>•Threats are both internal and external.</li></ul>



# Information Security Strategy

- SWOT
  - Strength = what is possible/achieved
  - Weaknesses = vulnerabilities...
  - Opportunities = what could if...
  - Threats = what prevents to...
- Helps defining strategic alternatives
  - S-O: using S to take profit of O
  - S-T: using S to counter T
  - W-O: use O to cover W
  - W-T: cover W and counter T
- “Precaution Principle”  
=> W-T, then W-O, then S-T or S-O

Future workshops!



# Information Security Objectives

- Confidence in survival to disasters (BCM)
- Resilience to security incidents
- Effectiveness/efficiency of controls to achieve (business) objectives
  - Benchmarking & reconnaissance
- Higher quality in business processes
- Adequacy of security controls
  - Self-Esteem
- Information security governance
  - Self Actualization

# Information Security Strategy



- Short and long term
  - Select a step-wise approach
  - Clearly define the first step
  - ‘imagine’ how you would be when the objective is reached
    - How you’ll feel
    - What you’ll do
  - Needs FLEXIBILITY in means/resources/actions

# Information Security Strategy



**Why not using  
BSCs  
to formalize  
and  
'govern'  
the strategy  
?**

**Future workshops!**

**ICT Control**



# 3. Information Security Governance

The results of our research

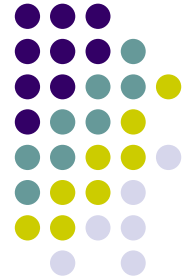
1

# Governance



“IT governance is the term used to describe how those persons entrusted with governance of an entity will consider IT in their supervision, monitoring, control and direction of the entity. How IT is applied within the entity will have an immense impact on whether the entity will attain its vision, mission or strategic goals.”

— ROBERT S. ROUSSEY, CPA, PROFESSOR,  
UNIVERSITY OF SOUTHERN CALIFORNIA



# Governance

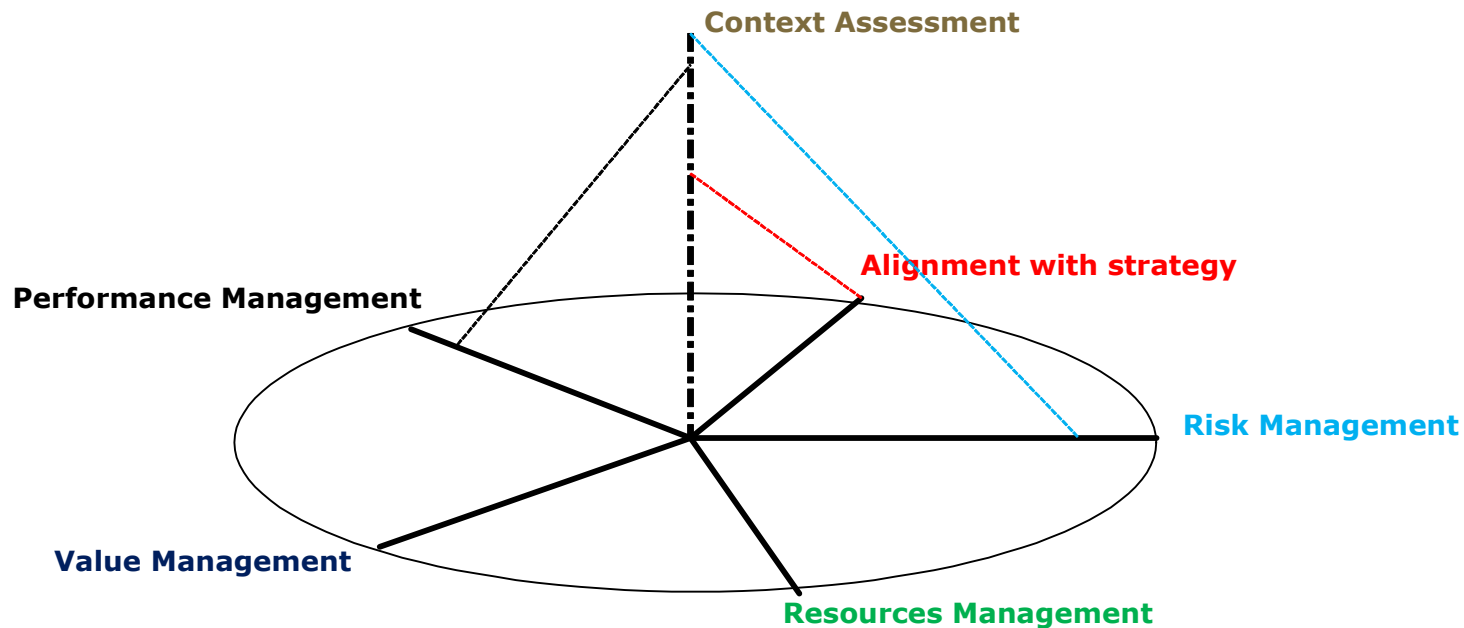
- Definition
  - The way of directing, supervising, monitoring and controlling activities
- Study in 5 domains
  - State governance
  - Economics
  - Enterprises
  - Projects
  - IT
- Same directions (streams, focus areas)
  - Strategic alignment
  - Risk management
  - Value management
  - Resources management
  - Performance management

**One 'principle':  
taking account of the contexts**

# Information Security Governance



- One new direction (*focus area*)
  - Assessment of external and internal contexts
  - Orthogonal



# 5 governing processes (1 for each direction)



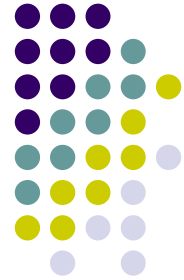
- Strategic Alignment
  - *Manage ISec Strategy*
- Risk Management
  - *Manage Information Risks*
- Value Management
  - *Manage ISec Rules*
- Resources Management
  - *Organize ISec*
- Performance Management
  - *Manage an ISec Supervision Environment*

*Within the full ISec Scope*



# Manage ISec Strategy

- *Analyse contexts; Determine strategy; Align strategy*
- Make sure that ISec strategy is
  - Aligned
    - With Business strategy and objectives
    - Takes into account ALL the contexts
  - Approved
  - Communicated
  - Updated when needed
- See CobiT
  - PO1, PO2, PO3, PO5, PO6



# Manage Information Risks

- *Analyse risk contexts; Assess Risks; Treat Risks*
- Make sure
  - The risk management approach and methodology is appropriate and correctly used
  - The risk assessment is done
    - With detailed knowledge of the internal and external contexts
    - in close co-operation with interested parties and results are validated
  - The risk treatment is done in close relation with the owner of the assets and the actors of the actions
  - The risk management tools, mechanisms, references, decisions are maintained, still valid and approved
- See CobiT
  - PO9 extended beyond IT on the full (information) process/system



# Manage ISec Rules (& Actions)

- *Analyse contexts; Establish rules; establish actions*
- Make sure the expectations (requirements) of the risk management are
  - Translated in
    - SMART objectives
    - W<sub>5</sub>HC activities
  - Taking care of the internal context
    - Capability and maturity
    - Management mode(s)
    - Organisational culture
  - Documented and communicated as appropriate
  - Correctly implemented
  - Updated when needed
- Provide Education, Training and Awareness programmes
- See Cobit: PO4, PO8, PO10, A1x and DSx



# Organise ISec

- *Analyse existing organization (capacity); Determine ISec competencies; Determine Structure*
- Identify, implement and manage
  - Necessary skills and knowledge to achieve objectives and perform activities
  - Appropriate roles and responsibilities
  - Appropriate structure
  - Appropriate communication channels
- Provide
  - Education and training programmes
- Ensure
  - Flexibility to enable crisis management
  - Monitoring and review of the organisation
  - Adequation to internal and external contexts

- See CobiT: PO7, AI4, DS7

# Manage an ISec Supervision Environment



- *Conceive supervision solutions; Run supervision solutions; Run continuous improvement*
- Determine and implement
  - Indicators, metrics and dashboards
  - Communication channels
    - Emergency
    - Feedback and measurement
  - Verification, audit, reporting standards and procedures
  - Recommendations processes and procedures
- See CobiT ME<sub>x</sub>, feedback from AI<sub>x</sub> and DS<sub>x</sub>



# Isec Operational Processes

Governance is good !

But what do we have to govern?

Operations !

More than ISO 27002

More than CISM domains 3 to 5

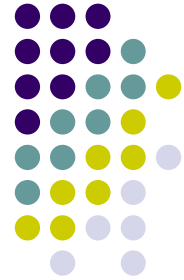


# Isec Operational processes

## 3 fields

- Preparation
  - To be ruled by Project Management
- Functional
  - The 'real' operations
- Supportive
  - To create the 'culture'

All provide feedback to the Control Environment.

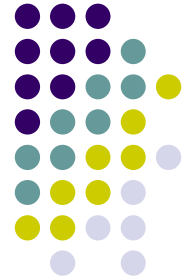


# I Sec Operational Processes

## Preparatory

- **Conceive I Sec control**
  - Provide Precise description of controls
  - *Feasibility; General description; Detailed description*
- **Realize I Sec control**
  - Validate an operational prototype
  - *Develop; Integrate; Test*
- Validate I Sec control
  - Accredit the control in its operational context
  - *Test; Accredit; Prepare deployment*

**Porter's Value Chain**



# I Sec Operational Processes

## Functional

- **Operate I Sec controls**
  - Make the controls effective within the ISMS
  - *Deployment; Operation; Maintenance*
- Ensure I Sec SLA
  - verify operational effectiveness
    - = achievement of expected results
    - = achievement operational quality of control and results
  - *Activate indicators; Measure indicators; Communicate*
- Operate I Sec watch
  - Obtain relevant information on context changes
  - *Activate tasks; Analyze information; Communicate*

**Porter's Value Chain**



# Isec Operational Processes

## Supportive

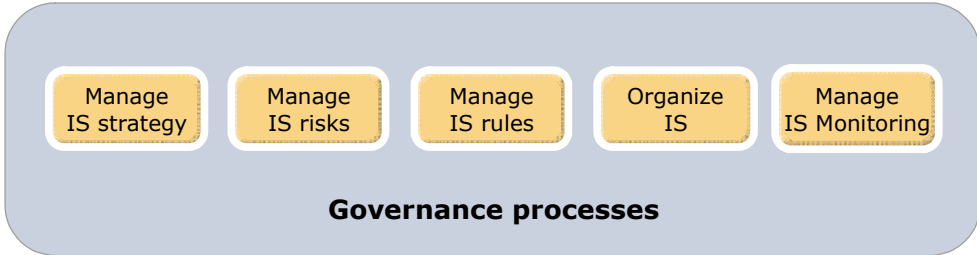
- **Isec Training and Awareness**
  - Ensure knowledge transfer and Isec behaviors
  - *Identify need; Train; Evaluate results*
- **Support to Isec clients**
  - Fulfil user's requests (See ITIL)
  - *Log requests; Handle requests; Communicate*
- Respond to Isec Contingencies
  - Ensure appropriate response and reduce negative consequences (See ISMS, ITIL)
  - *Log contingencies; Resolve; Communicate*

**Porter's Value Chain**

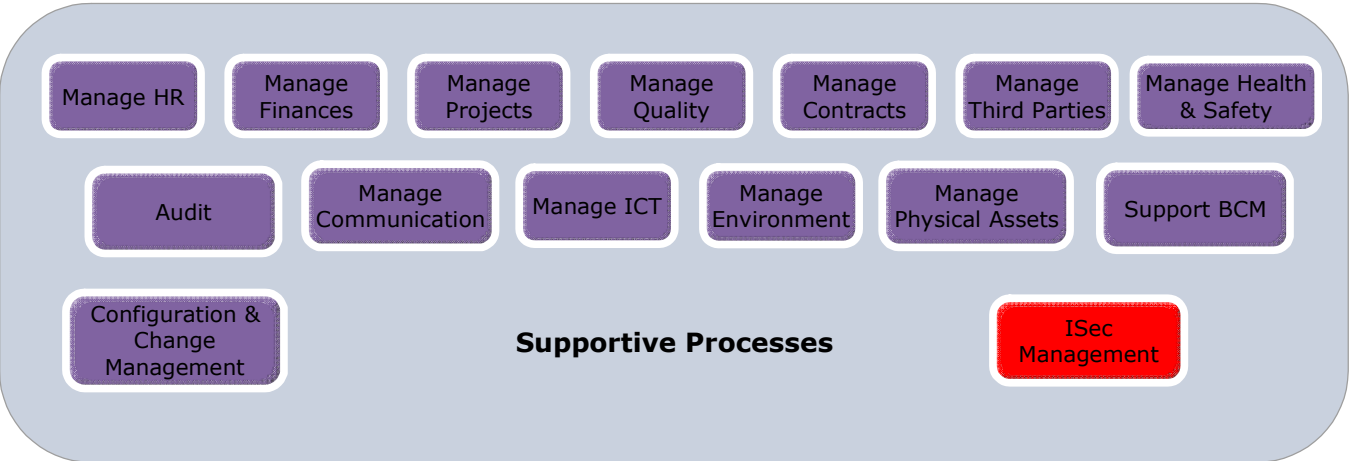
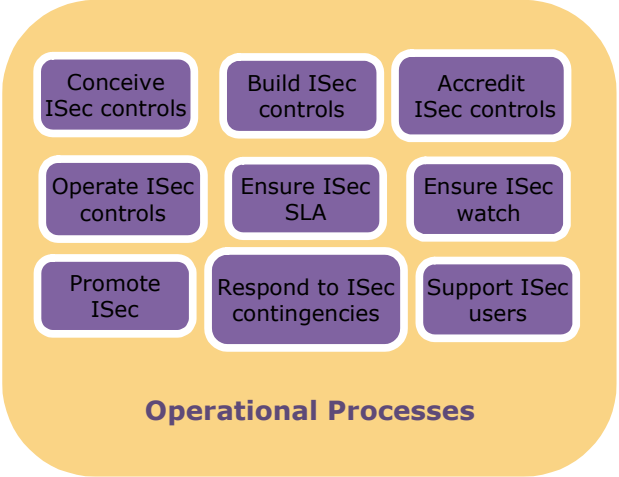


# Business Support Processes

- Manage HR
- Manage Finance
  - (financial support)
- Manage Accounting
- Manage Third Parties
- Manage customers
- Manage contracts
- Manage IT
- Manage Communication
- Manage Quality
- Manage Projects
- Manage Physical Assets
  - (incl. buildings and facilities)
- Manage Environment
- Audit
- Manage BCM
- Manage Health and Safety
- Manage Configuration and Changes
- **Manage ISec**
- Etc.



The 'full' Picture





# A governance model

Operate	Operate ISec Measures	PDCA <i>Potential</i>
Control	<b>Operate</b> + <i>Conceive</i> + <i>Risk</i> + <i>Rules</i> + <i>Organise</i> <i>(partial?)</i>	PDCA global
<b>Manage</b> (ISO 27001)	<b>Control</b> + Supervise + Promote + Respond to ISec contingencies	PDCA global
<b>Master</b>	<b>Manage</b> + Align + Accredite + Support (Q, P, RH, ICT)	PDCA process + global
<b>Govern</b>	<b>Master</b> + Realise + integrate support processes	PDCA process + global

# Relations



	Pr/SbPr	ISMS	CISM	CobiT
Governing Pr.	5/15	5/10	5/15	5/15
Prepartive Pr.	3/9	1/4	2/6	3/9
Operative Pr.	3/9	1/3	3/7	3/9
Supportive Pr.	3/9	3/9	3/9	3/9

CobiT: + All 'Support Processes



## 4. Information Security Roles

The results of our research  
2



# ISec Roles

- External (to the organization)
  - Regulating bodies
  - Standardization bodies
  - Reflection groups (think tanks)
  - Control bodies
- Internal
  - ISec strategy supervision
  - ISec strategy leader/conductor (Owner – A)
  - ISec ‘animator’ – CISO (manager – R)
  - Local ISec relays
  - Business/process owner/responsible person (custodian – C)
  - User – performer (I)



# 5. Conclusions

...

# I Sec wider than IT Sec



## Conclusion

- I Sec governance does not use new issues
  - IT Governance domains
    - One Governing process per focus area
  - I Sec Operations
    - Value chain (Porter)
    - More complex than ISMS
  - Business support processes
- CobiT and ITIL can both be used if you replace IT by I Sec
  - Only minor changes (focus)
  - Except CobiT DS5 and DS8
- Governance model
  - Step-by-step
  - Continuous improvement
  - CISM tasks – good reference
  - *Integration* of & with other Support Processes is key



**Thank You**

**Time for discussion**

[jlallard@ictcontrol.eu](mailto:jlallard@ictcontrol.eu)

[www.ictcontrol.eu](http://www.ictcontrol.eu)

**ICT Control**