Advanced Information Security Risk Management

Gary Gaskell

(CISSP, CISM, CISA, CCSP, FACS, CP-Cyber Security (ACS), GAICD
M App Sc, B Eng, B IT)
E: gary.gaskell@infosecservices.com.au
W: www.infosecservices.com.au
M: 0438 603 307

With thanks to Mark Ames, CISA, CISM, CRISC

Infosec Services Pty Ltd

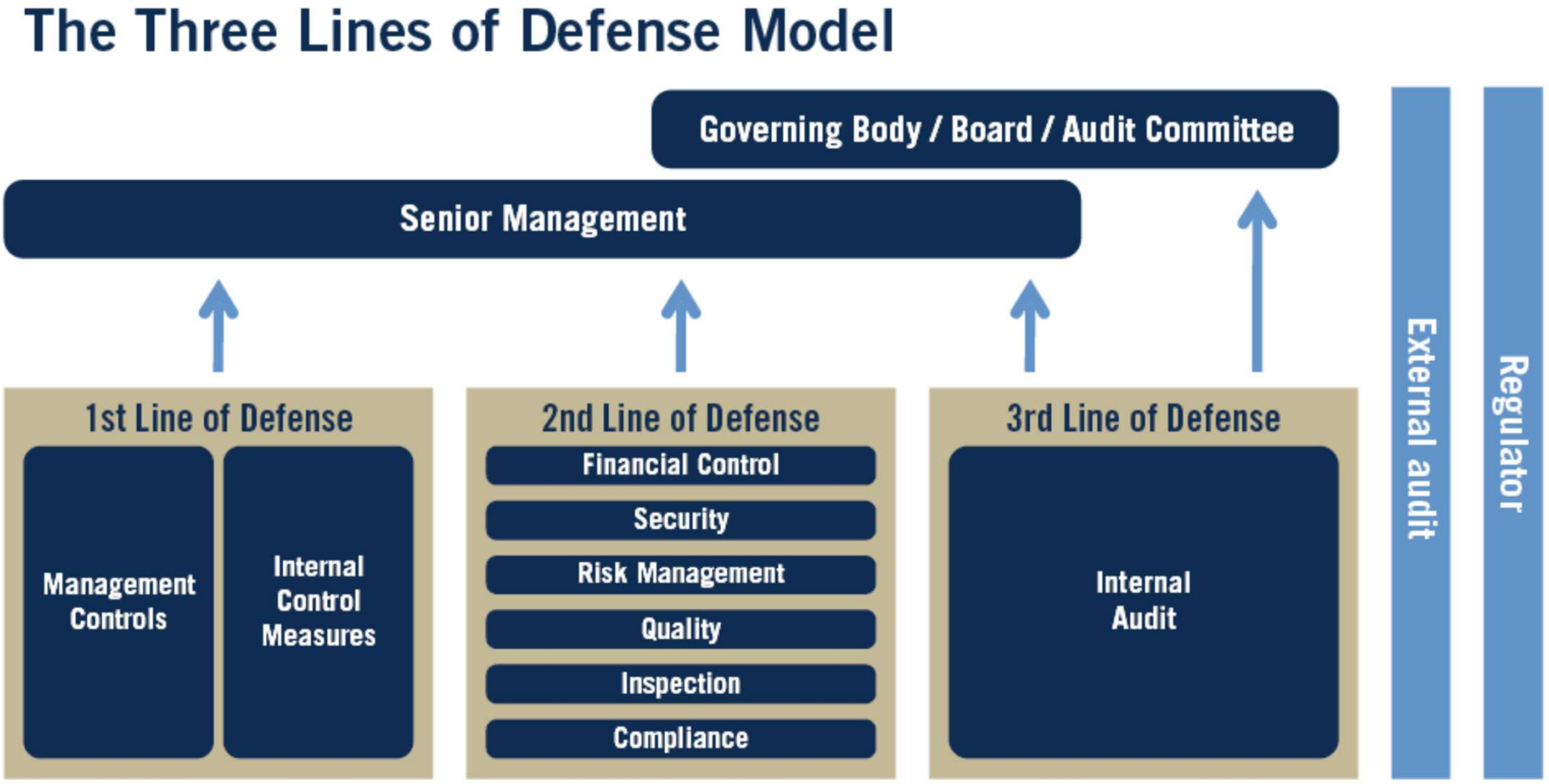
Objectives

- Moving on from the simple view
  - Adapting to achieve your goals
  - Avoiding pitfalls
- Confident RM application
  - Hypothetical risk assessment
  - Sharing experiences and insight

Agenda

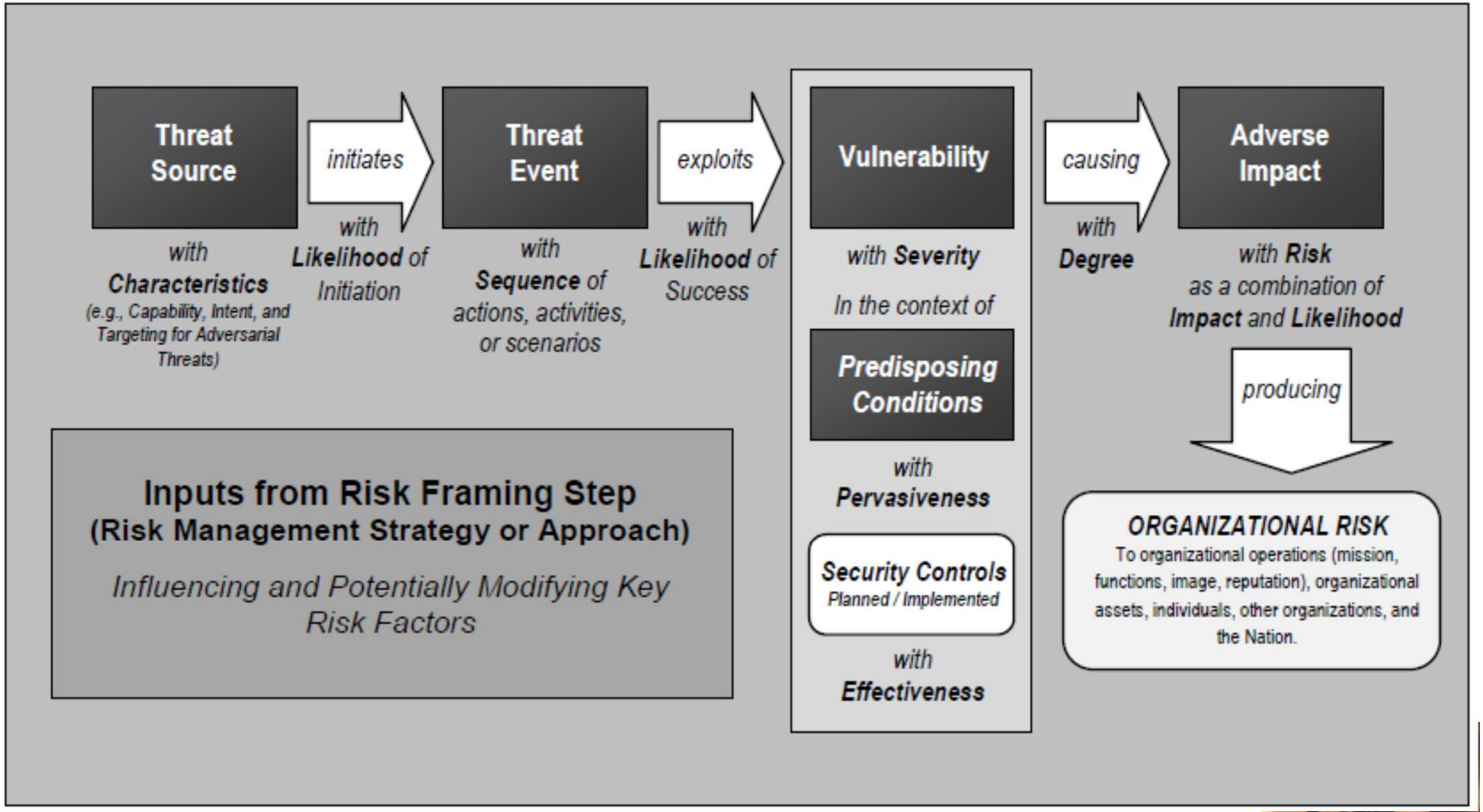
- Your experiences
  - What worked
  - What didn't
- Deep dive – Risk assessments
- Traps for young players
- Practice Run

Institute of Internal Auditors



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

NIST SP800-30 (USA)



NIST SP800-30 (USA)

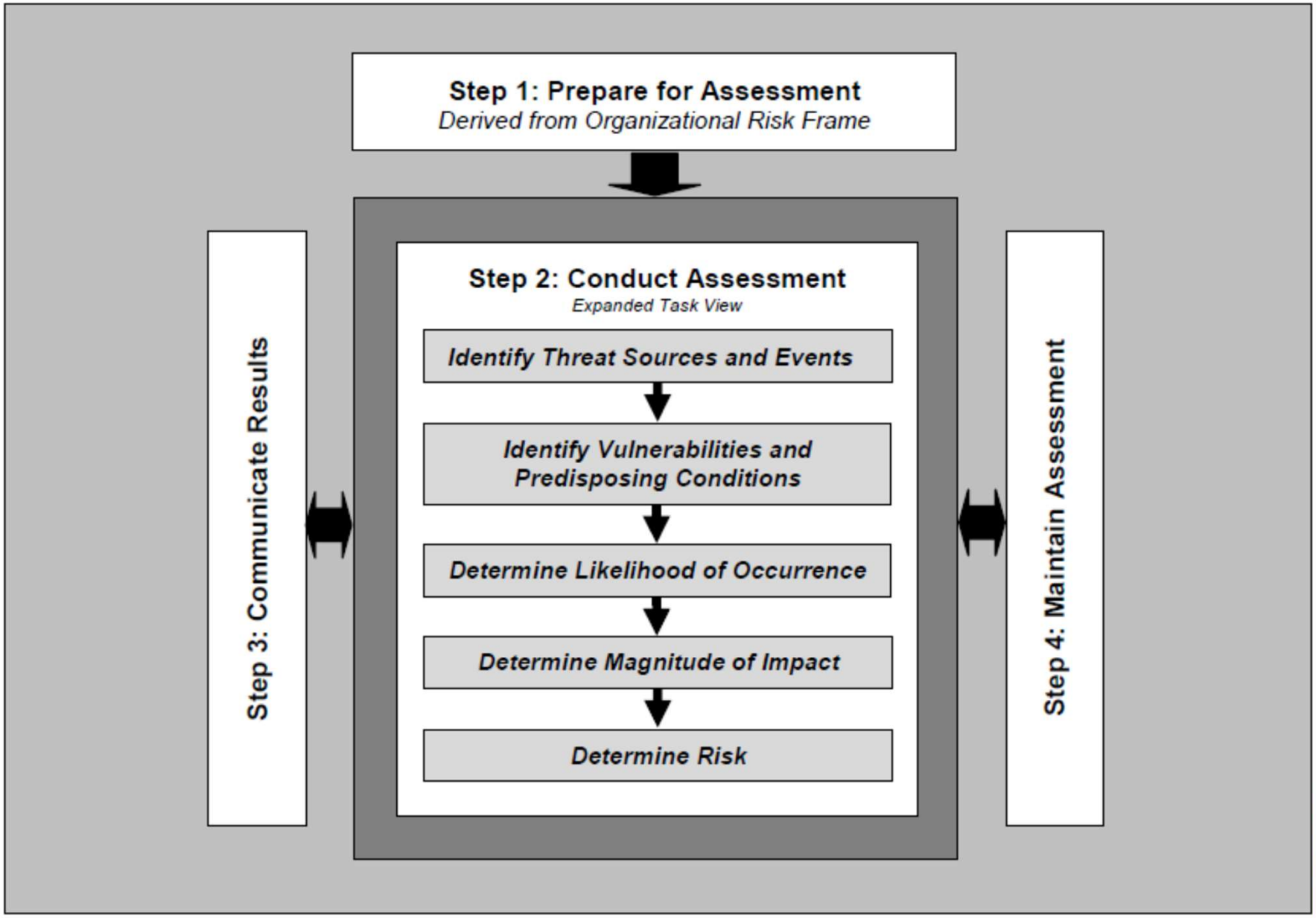
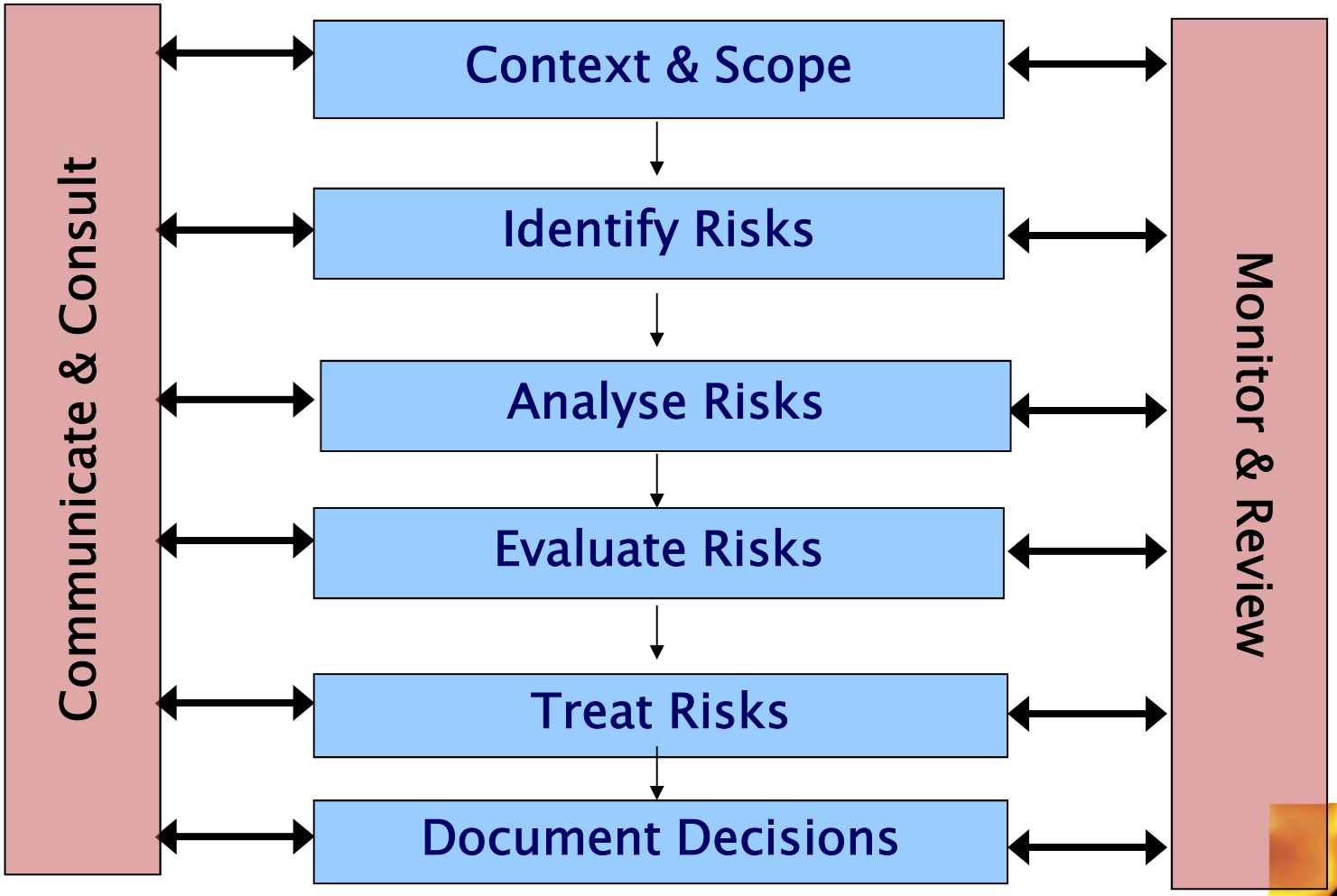


FIGURE 5: RISK ASSESSMENT PROCESS

Risk Management Process



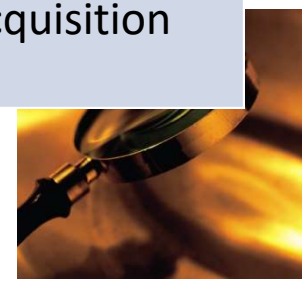
WHAT WORKED

Hmmm

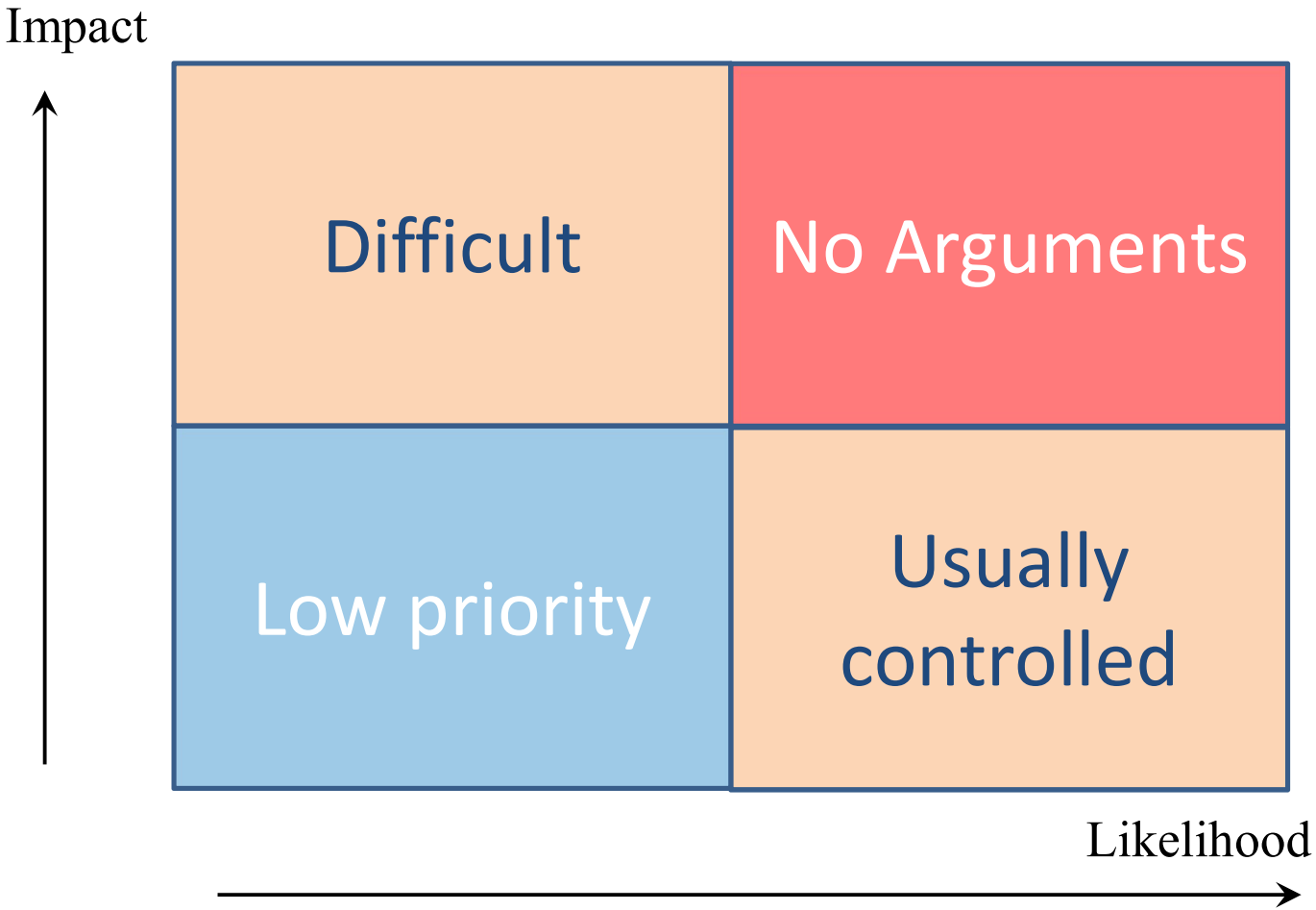
Sony	$2 billion
Heartland payments	Business failure
Digi notar	Business failure
RSA	Significant loss of good will and place on the pedestal $$ for replacement of tokens $$ liability for consequential breakins
Payrolls – QH	$$, Loss of confidence in a Government
PCEHR	4 months delay in detection penetration
US Govt leakage to wikileaks	TBA
US nuclear superiority	TBA
Banks – incorrect interest calculations	Inversely proportional cost of rectification

Hmmm

Sony	**$2 billion**
Heartland payments	Business failure
Digi notar	Business failure
RSA	Significant loss of good will and place on the pedestal $$ for replacement of tokens $$ liability for consequential breakins
Payrolls – QH	$$, Loss of confidence in a Government
PCEHR	4 months delay in detection penetration
US Govt leakage to wikileaks	TBA
US nuclear superiority	TBA
Banks – incorrect interest calculations	Inversely proportional cost of rectification
Yahoo	3 billion accounts $350 million price drop for Verizon acquisition (ouch!)



Support for Security



Traps & Pitfalls

Don’t Expect Perfection

- Not all threats may be identified before hand
  - Remember September 11
- Likelihood is an educated guess
  - Imperfect information
  - Predicting the future
  - Betting with the odds
- Vulnerability is variable
  - Human perception
  - Changing circumstances
- Consequences are often hypothetical
  - What if?
  - Worst case or likely case impacts?

Traps for New Players

- Ideology
- Ignorance
- Politics
- Security is only confidentiality
- Auditing detailed controls
- All risks are high
- Quantitative
- Too much detail

Security is not just Secrets

- Security is:
  - Confidentiality
  - Integrity
  - Availability

Auditing

- It is not necessary to audit controls to prepare a risk assessment
- Detailed risk assessments analyse control effectiveness
  - High level risk assessments focus on major control gaps

Details, details, . . .

- Don’t get too detailed
  - “breadth first” rather than “depth first”
  - Group similar assets
- Quantitative assessments
  - Many information security issues don’t suit an analysis based on $$
  - Aim for qualitative assessments

Getting Management's Attention

- Loud
- Logic
- Power structure
- Regulator
- Credibility

Practical Realities

An Imperfect Process

- Not all threats may be identified
  - Remember September 11
- Likelihood is an educated guess
  - Imperfect information
  - Predicting the future
  - Betting with the odds
- Vulnerability is variable
  - Human perception
  - Changing circumstances
- Consequences are often hypothetical
  - What if?

Managing Risk

- Not all risks can be eliminated
  - Doing business is taking a risk!
- Not all risks can be anticipated
  - SARS, September 11
- Management makes investment decisions
  - Cost of controls vs cost of potential consequences
- Risk analysis is only the beginning
- An ongoing program is essential

Fact: Commitment Varies

- Management perception of threats
  - Ignorance is bliss?
  - Credibility of the risk management process
  - Priorities from Board or Cabinet
- Risk appetite
  - Willingness to accept potential losses and disruptions
- Context of existing “culture”
  - Not invented here
  - Head in the sand
  - Full speed ahead
  - CYA

Constraints

- Skilled resources
  - Training and experience
- Funding
  - Budget and finance processes may be inadequate
- Internal competition for priority
  - My risk is bigger than yours
- Impact on operational staff
  - Additional human resources may be required
  - Or fear of this
- Effort
  - RM effort must be balanced against other activities

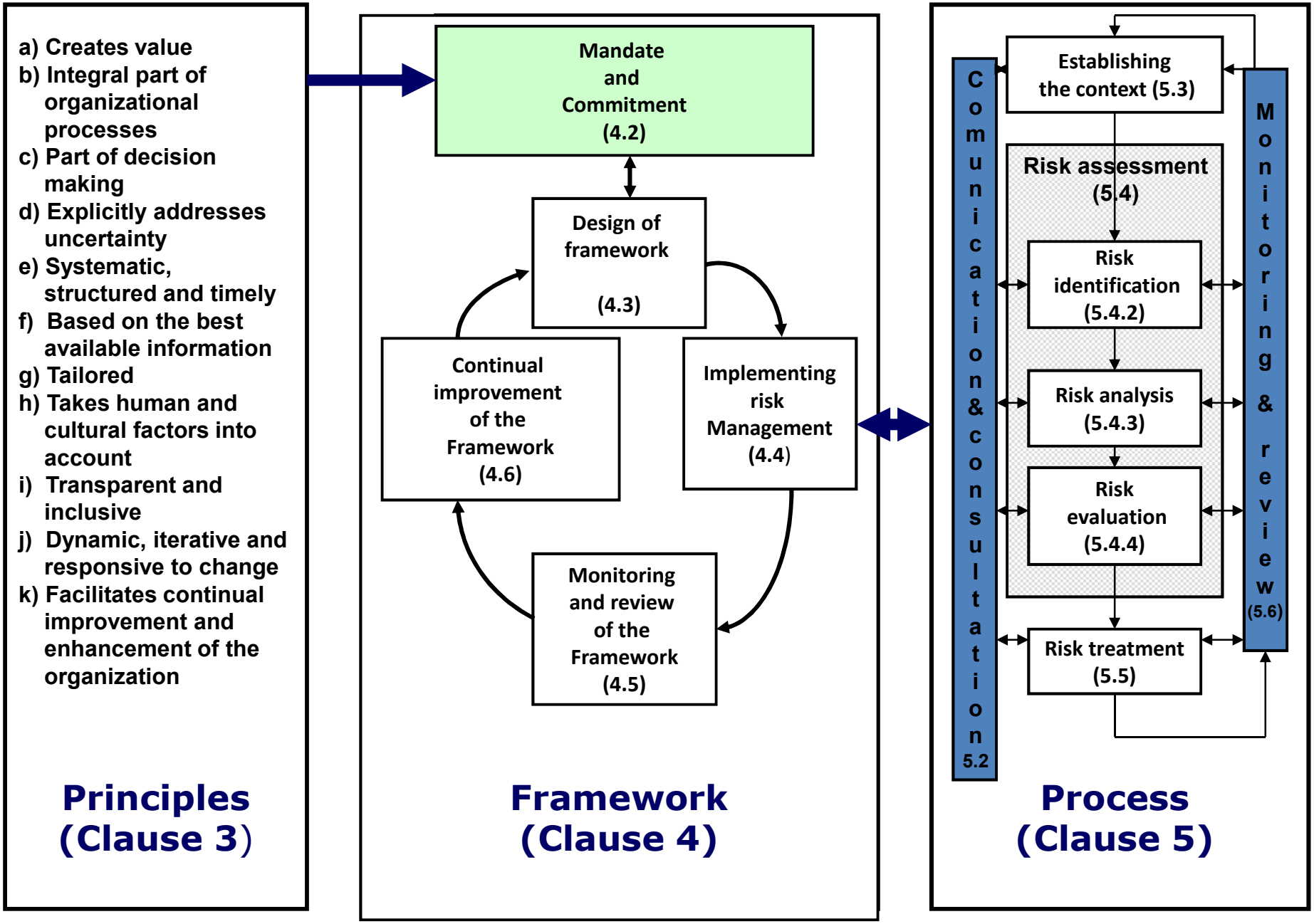
Time and Money

- Lead times for risk treatment
  - The longer you wait, the more it costs
  - Today's major risk could be irrelevant next year
  - New and urgent critical risks can intervene
  - The worst could happen *before* you're prepared
- Costs
  - Design and development
  - Implementation
  - Management and maintenance
  - Operational overheads
  - Impact on system reliability or availability

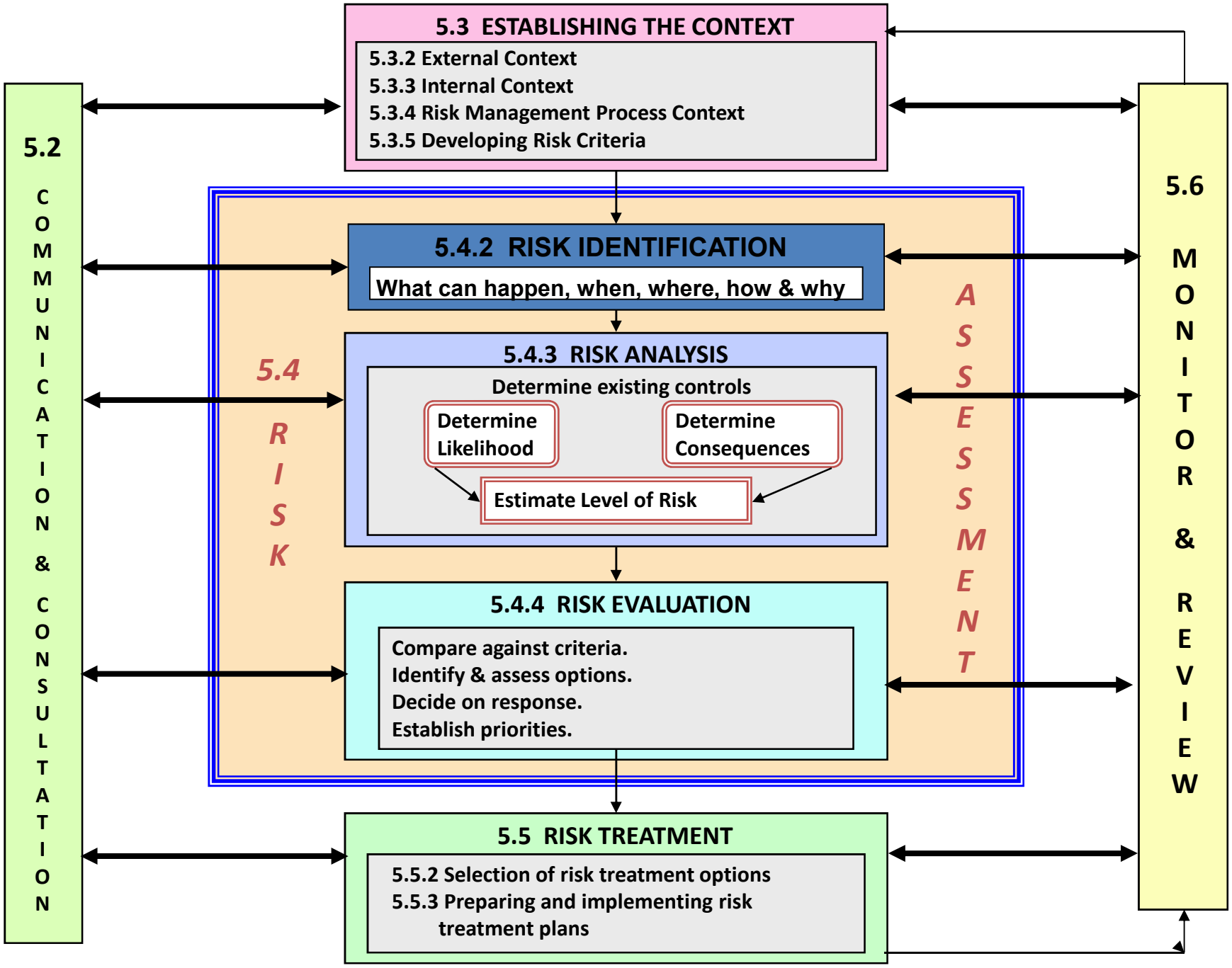
Details, Details . . . .

- Don’t get too detailed
  - “breadth first” rather than “depth first”
  - Grouping or abstraction strategy
    - similar assets
    - similar vulnerabilities, similar threats
- Quantitative assessments
  - Many information security issues don’t suit an analysis based on $$
  - Aim for qualitative assessments

RISK THEORY REVISITED



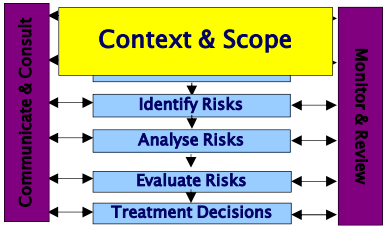
ISO 31000:2009 Figure 1 – Relationship between the principles, framework and process



ISO 31000:2009 Risk management process in detail

CONTEXT – DETAILED DISCUSSION

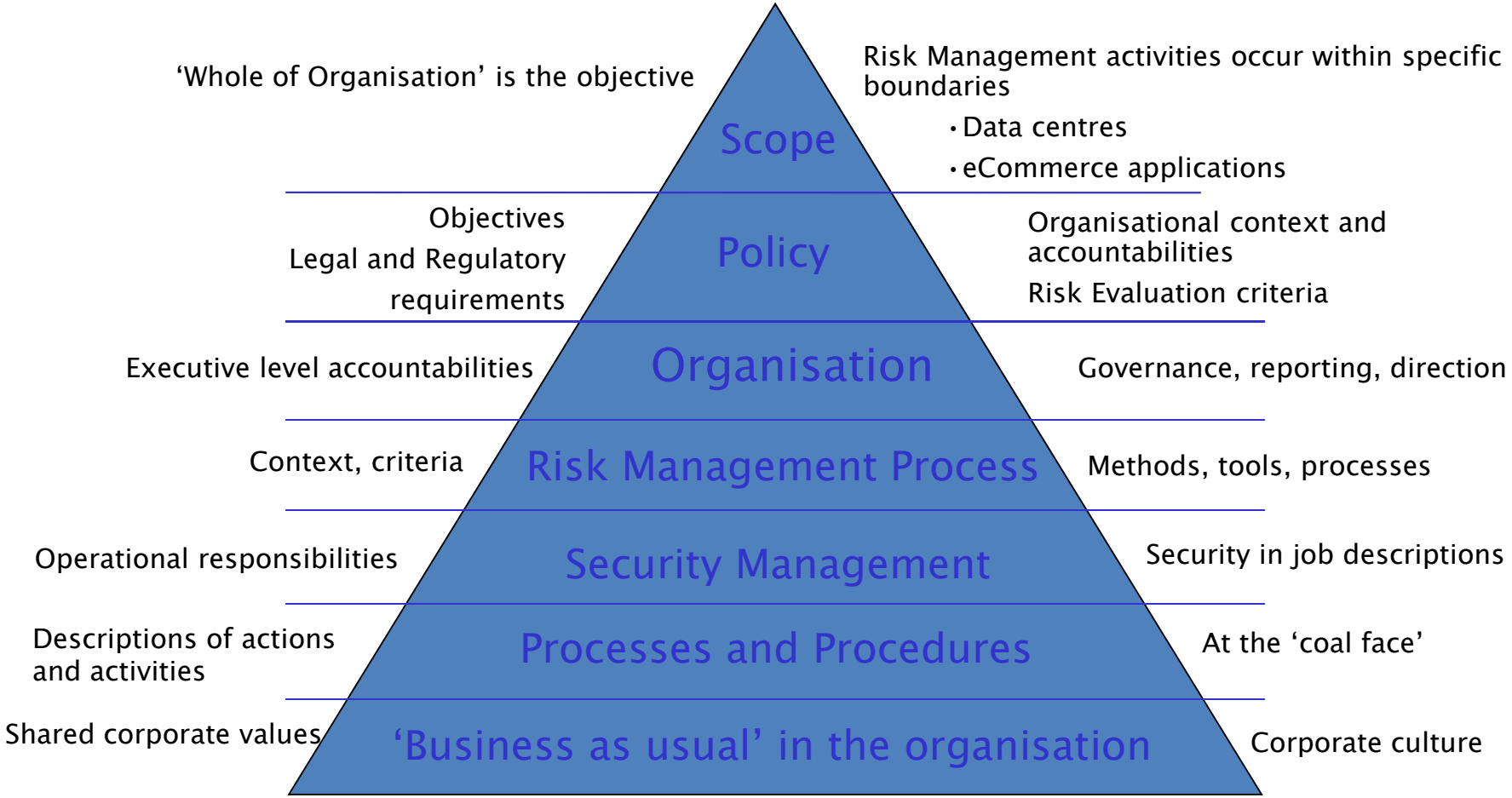
Context



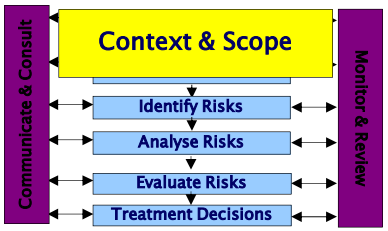
- Strategic Context
  - Objectives
    - Organisational
    - Key players
  - Operational Environment
  - Strengths & Weaknesses
- Organisational Context
  - Policy
  - Governance structure
  - Management structure
  - Capabilities
  - Culture

- Risk Management Context
  - Attitudes towards Risk
  - Skills and experience
- Evaluation Criteria
  - How is organisational performance measured?
  - How will risk be measured?
  - Is accountability welcomed?

The Risk Management Context



Risk in the Organisational Context



Media

Utilities

Banking & Finance

Construction

Retail

Health Care

Less Vulnerable

More Vulnerable

Agriculture

Communications

Transportation

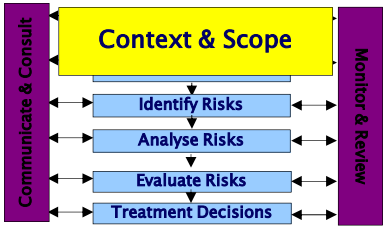
Education

Manufacturing

Government

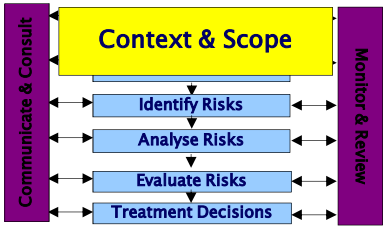
Source IDC 2000

Identify the assets in scope



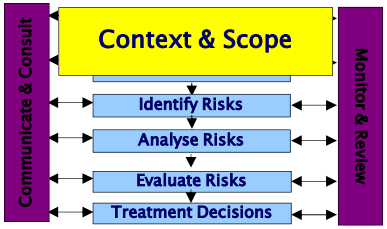
- Business Processes
- Critical data and information
- Technical Infrastructure
- Physical infrastructure
- Business units
- Legal drivers

Scope of Risk Assessments

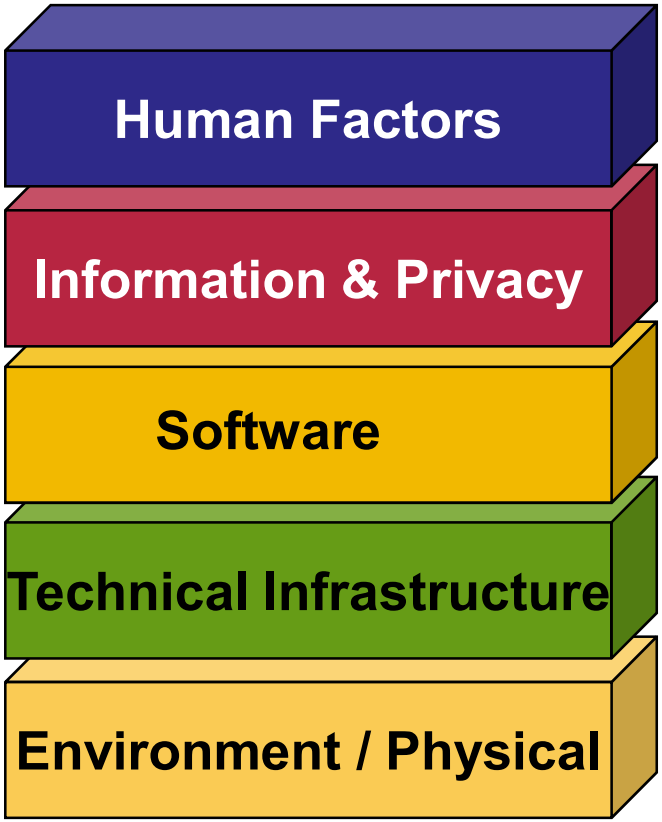


- Organisation wide
  - systems and operational processes
- Specific information systems
- Projects
- Technical analysis of software and configurations
- Operations, Infrastructure

Major Areas of Risk



- Human factors
  - Errors, fraud, unauthorised activity.
- Information & Privacy
  - Appropriate management of sensitive and personal Information
- Disruptive software (Malware)
  - Viruses, worms, programming errors
- Technical Configuration & Change Management
  - Hackers, operational errors, inappropriate access
- Physical and Environmental
  - Theft, disruption, flood, fire



Accurate Analysis

- Correct Context
  - Audiences
    - Decisions & funding
    - Implementation of Recommendations
  - Crucial for the communication
  - Setting the criteria for acceptance, treatment . .
  - Know who and why you're doing the risk assessment
  - Know the management's drivers

RISK IDENTIFICATION

Agree on the Threats

- A major source of disengagement
- Tools
  - Case studies
  - Regulations, industry experience
  - Threat assessment process (formal)
    - Standards Australia Handbook 167
      - Security Risk Assessment
        - » (this is a physical security document)

Scope of Threats

- errors and omissions
- fraud and theft
- employee sabotage
- loss of physical and infrastructure support
- malicious hacking
- malicious code
- industrial espionage

Australian Government TISN – Defence in Depth

Threat Assessment

Source	Motivation	Intent	Capability	Threat Level	Evaluation & Comments

Workshops

List risks:

Brainstorming, Structured discussion

RISK ANALYSIS

Analysing Risk

- Identify known and perceived Threats
- Consider the Likelihood
- Evaluate the Impact
  - Consider your *existing* security regime
- Determine Level of Risk

Risk Likelihood

Vulnerability Level

Threat Level	Low	Medium	High
High	Moderate	Likely	Almost Certain
Medium	Unlikely	Moderate	Likely
Low	Rare	Unlikely	Moderate

Analysis – Key Aspects

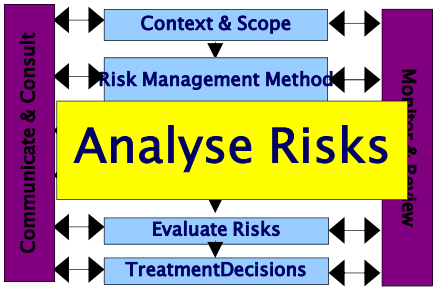
Aligned to ‘Enterprise risk’

Analyse Consequences

Consequence	Financial	WHS	Legal	Reputation	Environment
Catastrophic	Profit x 10	Multiple	Loss of licence	Long term negative brand	Long term severe damage
Severe	Profit x 1	Death, severe injury	Restricted licence,	Media campaign	Short term severe damage
Major	10% of profit	Serious injury	Fines, damages	Adverse media	Major damage
Minor	1% profit	Minor injury	Technicality	Minor exposure	Repairable
Insignificant	> $ 5000	Loss of time	Mediation	Limited awareness	Negligible

Risk Analysis

Risk Evaluation - **Level of Risk**



Level of Risk

Impact

Likelihood

	Insignificant	Minor	Moderate	Major
High	M	H	E	E
Medium	M	M	H	E
Low	L	M	M	H
Unlikely	L	L	M	M

Legend
E: extreme risk; immediate action required
H: high risk; senior management attention needed
M: moderate risk; management responsibility must be specified
L: low risk; manage by routine procedures

Customise for your Organisation

RM Process – Analysis Pitfalls

- Traps :
  - Wrong audience
  - Inaccurate consequence
  - Ignoring compensating controls

Compensating Factors

- Search for other controls that limit the risk
  - Business process level
  - Financial separation of duties
  - Detective controls, eg.

Set Priorities

Risk register

Risk Description	Risk Assessment		Existing controls	Impact Rating	Likelihood Rating	Level of Risk	Risk priority
	Threat	Probability					
Router Compromise	Intrusion, Disruption	Many times per year	Password Only	**MODERATE**	**HIGH**	**HIGH**	**?**
Physical Destruction of Data Centre	Operations Disrupted for one month	Once in 25 Years	None (Not addressed in BCP)	**MAJOR**	**LOW**	**HIGH**	**?**

NIST SP800-30 (USA)

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

Risk Treatment

- Avoid the risk
  - Just DON'T do it
- Transfer or share the risk
  - Shift liability by contract
- Apply Controls
  - Processes and Technology
- Insurance

Examples of Controls

- Integrity
  - Design Controls (Validation, etc)
  - Access controls
  - Logging
  - Change Management Processes
- Confidentiality
  - Authentication
  - Encryption
  - Non-disclosure agreement
- Availability
  - Capacity and resource planning
  - Business Continuity Plan
  - Architecture and Design (redundancy)

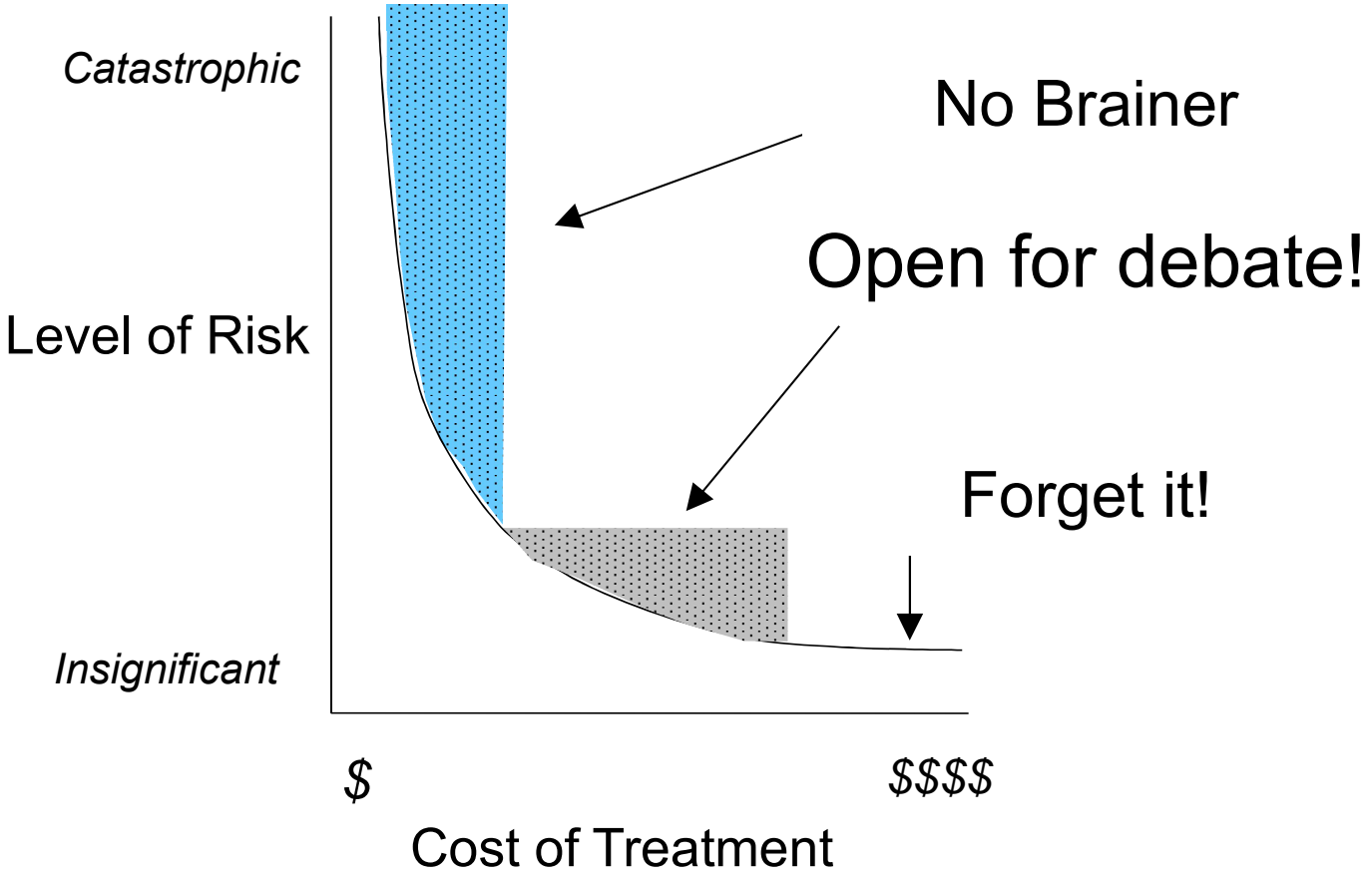
TECHNIQUES - EVALUATION

Decisions Decisions . . .

image courtesy of www.novodiem-bv.com

Control Cost/Benefit Analysis

- It usually comes down to $$



Document Decisions

Risk register

Risk Description	Risk Assessment		Existing controls	Impact Rating	Likelihood Rating	Level of Risk	Risk priority	Treatment Plan
	Threat	Probability						
Router Compromise	Intrusion, Disruption	Many times per year	Password Only	**MODERATE**	**HIGH**	**HIGH**	**2**	Project Y03
Physical Destruction of Data Centre	Operations Disrupted for one month	Once in 25 Years	None (Not addressed in BCP)	**MAJOR**	**LOW**	**HIGH**	**1**	Project Z21

Effective Risk Management Framework

- Align
  - policies and operational objecti
- Integrate
  - manageme
- Com

s throughout the organisation

anagement program

Information risk management process

Priority – Effective Communication!!

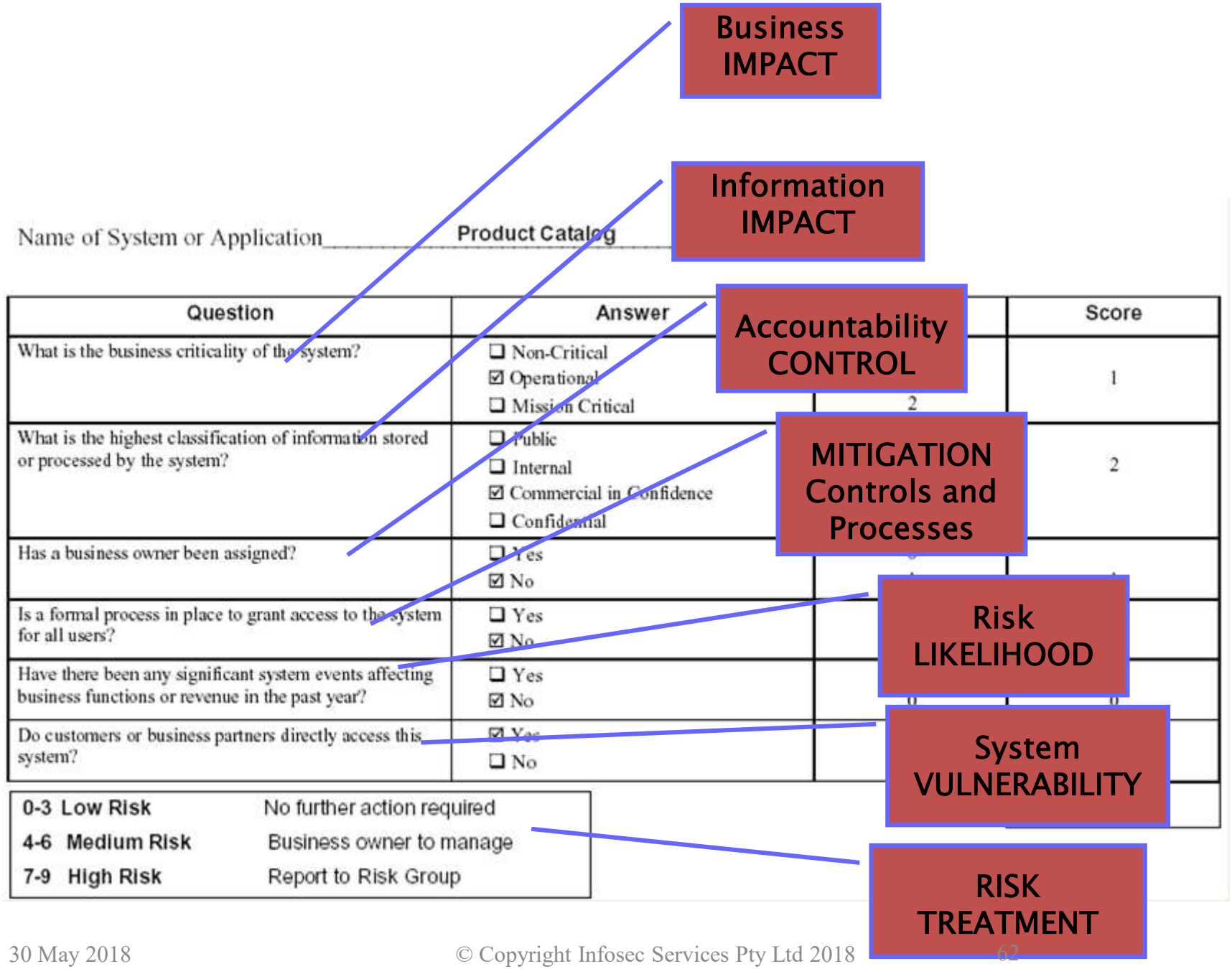
TECHNIQUES – PROGRESS REPORTS

Scorecards & Self Assessment

- Effective shortcuts and metrics
- Customised to organisation
- Integrated with performance reporting and project methodologies

Risk Self Assessment

- Simple questionnaires and checklists
- Tailored to organisation
  - Policy
  - Risk methodology
  - Risk profile
- Can be integrated with other monitoring and compliance tools



Balanced Scorecards

- Defines objectives and metrics
  - Linked to corporate governance/strategy
- Sets targets and initiatives
  - Linked to performance management
- Provides regular reports
  - Assessment and comparison
- Established corporate management and performance monitoring tool

Balanced Scorecards Projects

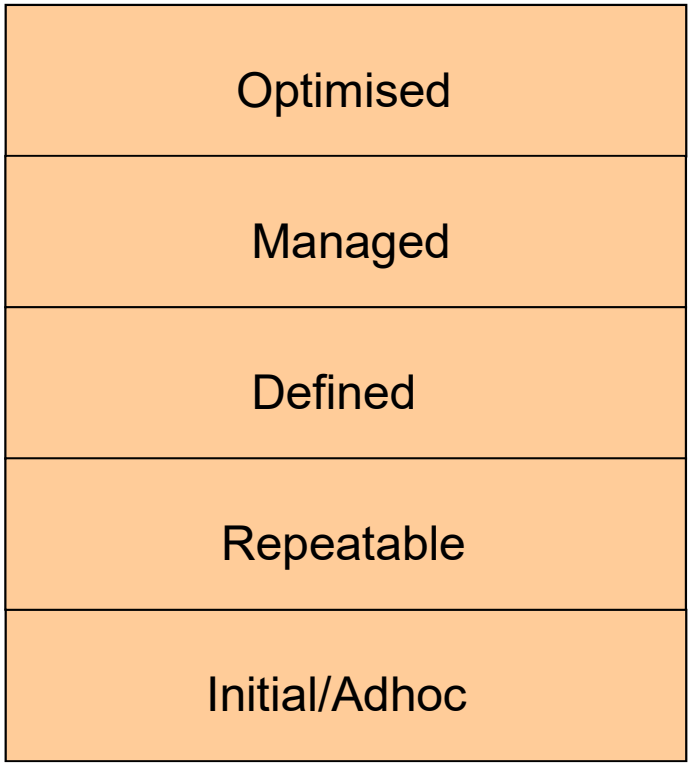
- Objective
  - Identify and manage IT security risks for new projects
- Measures
  - Completed self assessments
  - Completed security plans
  - Security plans on schedule
  - Trained project managers
- Targets
  - 85% of projects by requirements phase.
- Initiatives
  - Self assessment training or project managers

Balanced Scorecards
Projects

Target	Measure	Score
85% of new projects	Completed Self Assessments	60% / 85% → 7
85% of new projects	Completed Security Plans	50% / 85% → 6
Security plans on schedule	Milestones and deliverables	80% → 8
100% of project managers trained in year	25% of project managers in training this quarter	14% / 25% → 5

Result: 6.5 out of 10

Capability Maturity Model



Accept Residual Risk

- Accept remaining risk
- Report to process owners, senior management

Risk Acceptance

- Don’t surprise management
- Residual risk acceptance
- Continual improvement
  - Monitor & review

Constraints

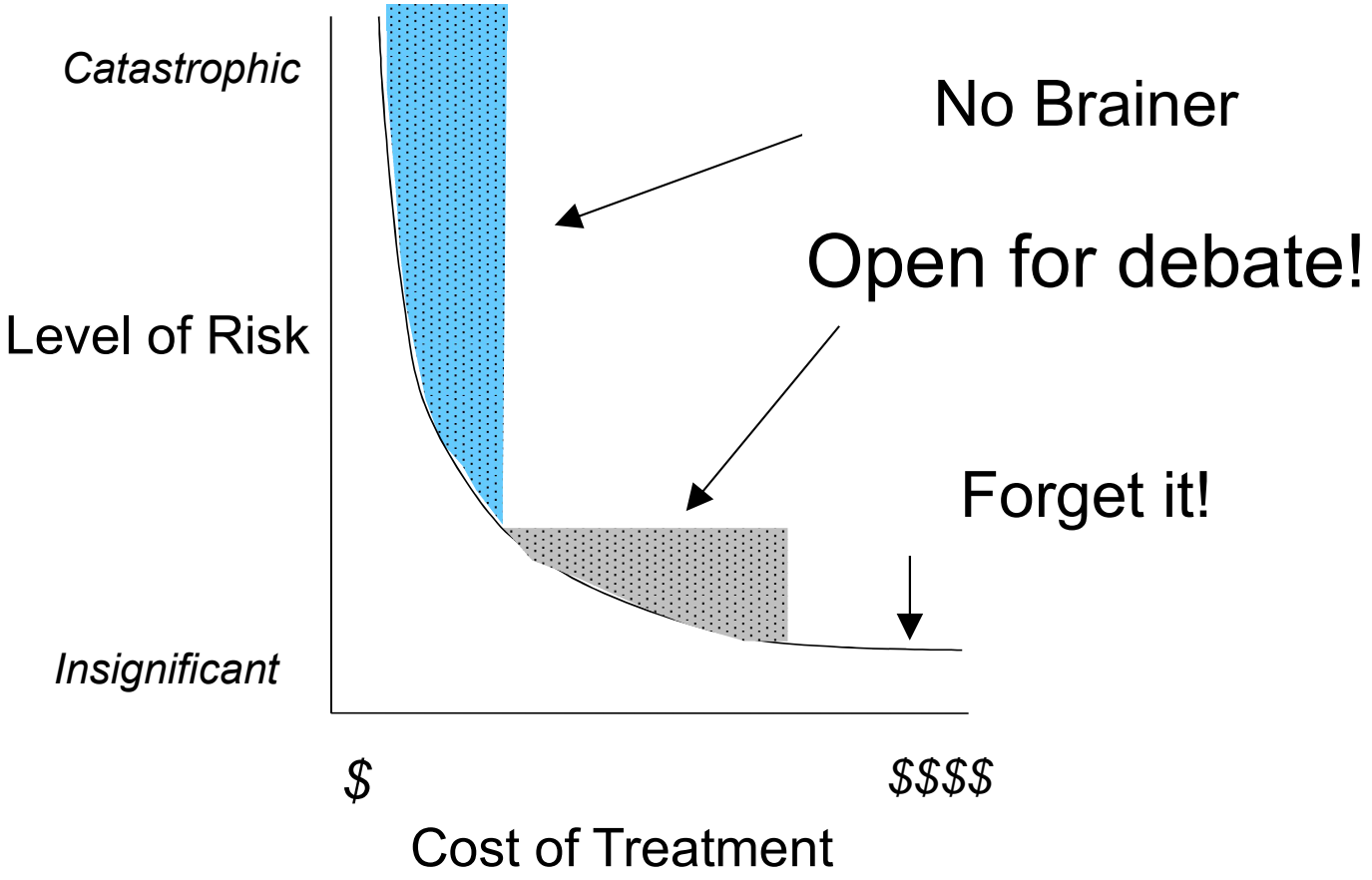
- Skilled resources
  - Training and experience
- Funding
  - Budget and finance processes may be inadequate
- Internal competition for priority
  - My risk is bigger than yours
- Impact on operational staff
  - Additional human resources may be required
- Effort
  - RM effort must be balanced against other activities

Time and Money

- Lead times for risk treatment
  - The longer you wait, the more it costs
  - Today's major risk could be irrelevant next year
  - New and urgently critical risks can intervene
  - The worst could happen *before* you're prepared
- Costs
  - Design and development
  - Implementation
  - Management and maintenance
  - Operational overheads
  - Impact on system reliability or availability

Control Cost/Benefit Analysis

- It usually comes down to $$



Review & Discuss

- Risk Management Activities
- Applications of Risk Management
- Benefits of Risk Management
- Why Different Frameworks and Approaches?
- Special meanings of terms
- What is RISK?

Shortcuts

- Combine threat and vulnerability assessments
- Include existing controls
  - Skip calculating the inherent risk
- Exclude common (non-critical) risks
  - Protected by baseline controls

Critical Success Factors

- Stakeholder involvement
- Regular/appropriate communication with stakeholders
- Manage perceptions
  - perceptions drive decisions
- Balancing effort, risks and opportunity

Critical Success Factors (2)

- Executive support
- Effective communication
  - based on the target audience
- Balancing precision/accuracy and timeframes

Critical Success Factors

- Stakeholder involvement
- Regular/appropriate communication with stakeholders
- Manage perceptions
  - perceptions drive decisions
- Balancing effort, risks and opportunity

Critical Success Factors (2)

- Executive support
- Effective communication
  - based on the target audience
- Balancing precision/accuracy and timeframes

Decisions and Outcomes

Persuasion

- Aristotle - three factors in persuasion:
  - intellectual (logos)
  - psychological (pathos)
  - social or ethical (ethos).

- People rarely change their minds merely on account of objective evidence.
  - People & decisions
    - personal relevance and impact of a claim,
    - Trustworthy source
- Alan Alda
  - Tell a story !

Decision Making

- Risk Assessment goal = decisions
- Psychology of decision making and judgements
  - Kahneman and Tversky
  - Prof Richard Thaler
- Decision theory debate
  - Rational decision theory v's
  - Biased and heuristic decisions

Heuristics

- “Rules of thumb”
- ‘industry good practice’
- ‘major change = major risk’
- . . . . . .

Cognitive Biases

- Deviations from rational judgement
- Availability bias
  - More frequent, recent information = higher weight
- Anchoring bias
  - Tendency to use the first piece of information
- Optimism bias
  - less at risk of experiencing a negative event compared to others
  - I'm a lucky person – always have been !!
- Confirmation bias
  - Due to preconceptions
- Conservatism or regressive bias
  - high values and high likelihoods overestimated
  - low values and low likelihoods are underestimated
- Conflict of Interest
  - Bonuses

Workshop

A practice run!

The End