Masterclass: Information/Cyber 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
Risk Management Objectives?

- Risk reduction
- Fix risks in the best order
- Translate the information into a business context
- Determine work priorities
- Credibility with senior management
- Your objectives?
Two Key Objectives

- Reporting up
  - E.g. risk to the board or executive

- Security Management
  - Designing a security program
Agenda

- Share experiences
  - Get better at our day jobs
- Basic risk management process
- Application to security risks
- Techniques for
  - identification
  - analysis
  - evaluation
  - Reporting
- Decisions and Judgements
- Workshop – put it into practice 😊
Today’s Rules

Get involved!
All contributions are valuable.
If you don’t understand something – stop us and ask!
We are here to learn and have a laugh as well.
Why are we here?

<table>
<thead>
<tr>
<th>Company</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sony</td>
<td>$2 billion</td>
</tr>
<tr>
<td>Heartland payments</td>
<td>Business failure</td>
</tr>
<tr>
<td>Digi notar</td>
<td>Business failure</td>
</tr>
<tr>
<td>RSA</td>
<td>Significant loss of good will and status, $$$ replacement tokens, liability</td>
</tr>
<tr>
<td>Payrolls – QH</td>
<td>$$, Loss of confidence in a Government</td>
</tr>
<tr>
<td>PCEHR</td>
<td>4 months delay in detection penetration</td>
</tr>
<tr>
<td>US Govt leakage to wikileaks</td>
<td>TBA</td>
</tr>
<tr>
<td>US nuclear superiority</td>
<td>TBA</td>
</tr>
<tr>
<td>Banks – incorrect interest calculations</td>
<td>Inversely proportional cost of rectification</td>
</tr>
<tr>
<td>Yahoo</td>
<td>3 billion accounts - $350 million price drop for Verizon acquisition (ouch!)</td>
</tr>
<tr>
<td>PageUP</td>
<td>TBA</td>
</tr>
<tr>
<td>Equifax</td>
<td>CISO fired, CEO testify to congress, shares ↓ 14%</td>
</tr>
<tr>
<td>Target USA</td>
<td>Loss of CEO (34 years), CIO, $162 million, shares ↓</td>
</tr>
</tbody>
</table>
Why are we Again?

- Demonstrate we made a sound plan!
What’s Changed

Interdependence
Complexity
Interconnection

1960s-1970s
Mainframes
Data on Tapes
Mainframes

1980s
Mainframes, Mini Computers
Data on Tapes, Direct Comms
Mainframes, Mini Computers

1990s
Clients, Servers
Direct data connections, Internet email, FTP
Servers

2000s
Clients, Servers
Ubiquitous Internet
Servers

Digital Enterprise

Inherent Risk

Time

29 May 2019
Copyright © Infosec Services Pty Ltd 2019
The Controls Just Moved

[Diagram showing the movement of controls from Organisational Controls to Organisational Controls with further sub-divisions into Vendor management controls and Cloud Service Provider Controls]
Is this Your Workplace?

Seaforth Baptist website
Getting Management’s Attention

- Loud
- Logic
- Power structure
- Regulator
- Credibility
Decisions

- Decision is a bet
  - Bayes theorem

- Decision process quality
  - AKA Risk management as a tool

- “Improve your Luck”
Deliverables?

- Decision Support
- List of critical functions and assets
- Catalogue of major risks
  - Rate risk level
- Identify control gaps
  - Where risk level is high or extreme
  - Action plan
Security Planning Options

Know the Threat

Assess risks

Plan Security

Baseline controls

Interim Security Plan
Masterclass Overview

- Formal risk management standards
- Some theory & definitions
- Techniques
- Communicating better
ISO 31000

Establish the Scope

Determine Review Method

Identify Participants and Stakeholders

Analyze Risks

Determine Existing Controls

Estimate Likelihood

Estimate Impact

Risk Impact

Accept Risk?

Yes

Evaluate Risks

No

Treat Risks

IT Risk Management Policy & Risk Profile
Standards and Guides

- ISO 31000 and 31010
- ISO 27005
  - ISO 31000 interpreted for security
  - More than ISMS Risk
- NIST - FREE !!
  - SP800-30 Guide for conducting risk assessments
  - SP800-37 – Manage Information Security Risk
  - SP800-161 – Supply chain risk
More standards

- ISO Guide 73
  - Risk Management Vocabulary
- Bank for International Settlements (Basel III)
  - Sound Practices for the Management and Supervision of Operational Risk
- Regulators
  - APRA - Prudential Standards and guides
  - AEMO – Cyber security framework
THEORY AND DEFINITIONS
Theory and Definitions

- **Hazards**
  - A source of potential harm

- **Threats**
  - Potential cause of an unwanted incident, which may result in harm to a system or organisation

- **Vulnerabilities**
  - Weakness of an asset or control that can be exploited by one or more threats

- **Risk**
  - “Effect of uncertainty on objectives”
  - A combination of consequences and likelihood
More Terminology

📍 Uncertainty

- is the state ... of deficiency of information related to, understanding or knowledge of, an event, its consequence or likelihood

📍 Risk owner, Senior Responsible Officer

- person or entity with the accountability and authority to manage a risk
Temporal Aspects of Risk

- Inherent
- Current risk
- Target risk
- Residual risk
Get the Timing Right!

No Controls → Inherent Risk → Current Risk → Target Risk → Residual Risk

Existing Controls → Planned Treatments → Implemented
Controls & Countermeasures

- Preventive
- Detective
- Corrective
Understanding Controls

- Classification
  - General Controls
  - Application Controls

- Classification
  - Preventative
  - Detective
  - Corrective

- Classification
  - Governance controls
  - Management controls
  - Technical controls
## Uncertainty

<table>
<thead>
<tr>
<th>KNOWLEDGE ABOUT LIKELIHOODS</th>
<th>KNOWLEDGE ABOUT OUTCOMES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Well-defined outcomes</td>
<td>Poorly defined outcomes</td>
</tr>
<tr>
<td>Some basis for probabilities</td>
<td>risk</td>
</tr>
<tr>
<td>No basis for probabilities</td>
<td>“INCERTITUDE”</td>
</tr>
<tr>
<td></td>
<td>ambiguity</td>
</tr>
<tr>
<td></td>
<td>uncertainty</td>
</tr>
<tr>
<td></td>
<td>ignorance</td>
</tr>
</tbody>
</table>

Control Cost/Benefit Analysis
- It usually comes down to $$

<table>
<thead>
<tr>
<th>Level of Risk</th>
<th>Cost of Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>$$$$$</td>
</tr>
<tr>
<td>Insignificant</td>
<td>$</td>
</tr>
</tbody>
</table>

- No Brainer
- Open for debate!
- Forget it!
Enterprise Risk Management

Diagram:
- Executive
  - Advice
  - Risk Register
- Audit & Risk Committee
  - Risk Register
- Business Units
  - Risk Register
- Service Providers
  - Risk Register

Governance - Risk Direction, Acceptance
Risk Summaries
A LITTLE MORE THEORY
Threats, Vulnerabilities and Risks

**Threats** → \textit{exploit} → **Vulnerabilities** → \textit{expose} → **Value**

**Assets** (including Business Processes)
Complex Cyber Risk View

**Likelihood**
- High
- Medium
- Low

**Impact**
- High
- Medium
- Low

**Risk**
- High
- Medium
- Low

**Threats**
- Human, Natural
- Technical, Physical
- Environmental, Operational

**Information classified for Value & Importance**
- Confidentiality
  - High
  - Medium
  - Low
- Integrity
  - High
  - Medium
  - Low
- Availability
  - High
  - Medium
  - Low

**Controlled**
- Administrative
- Technical
- Physical

**Mitigated with**
- Insurance
- Contracted Out

**Accepted by Executive**

**Vulnerabilities**
- Reduced after Controls implemented

**Targets**
- People
- Places
- Processes
- Systems

**Attack Surface**
- Reduced after Controls implemented

**Attack Surface**

**Low**

**Medium**

**High**

**Reducing**

**Reduced after Risk Transfer and/or Controls implemented**

**Mitigated**

**Transferred to External**
- Insurance
- Contracted Out

**Must cost less than possible Impact**

**Reducing**

**Reduced after**

**CAUTION**
MISNOMERS AND VARIANTS -

LET’S BE CLEAR WHAT WE SAY . . .
Risk Assessment Variants

Variant 1 – Security Engineering
Variant 2 – “Risk Assessment”
Vulnerability Assessment

Absent controls

Weak controls

List of vulnerabilities

Risk Assessment
Risk Assessment Approaches

❖ High level
  ▪ Identify major risks to achieving objectives
  ▪ Identify significant threats and vulnerabilities
  ▪ Focus on consequences to operational objectives and processes

❖ Low level
  ▪ Detailed inventory of assets,
  ▪ Catalogue all threats and vulnerabilities
  ▪ Focus on consequences to individual assets
Risk Assessment Methods

- **Qualitative – Relative ratings of risk**
  - Facilitated workshops
  - Educated best estimates from operational staff and managers

- **Semi-Quantitative - Puts $$ to relative ratings**
  - According to organisational criteria
  - Software tools (CRAMM, Phoenix)

- **Quantitative - $$ Ratings of risk**
  - Specialist consultancy, actuarial
  - Annual Loss Expectancy, etc
  - Detailed formal analysis & reviews
  - Tends to be very costly
Risk Management Frameworks

- ISO/IEC/AS/NZS 27001
  - Code of practice & specification for information security management systems (ISMS)

- ISO/IEC TR 13335-3
  - Guidelines for the Management of IT Security – This is getting old

- ISO 31000
  - Risk Management
  - Generic & Independent
  - Good framework


- Your CFO/ finance division
Mandate and Commitment (4.2)

Design of framework (4.3)

Implementing risk Management (4.4)

Continual improvement of the Framework (4.6)

Monitoring and review of the Framework (4.5)

Establishing the context (5.3)

Risk assessment (5.4)

Risk identification (5.4.2)

Risk analysis (5.4.3)

Risk evaluation (5.4.4)

Risk treatment (5.5)

Monitoring & review (5.6)

Communication & consultations (5.2)

Principles (Clause 3)

Framework (Clause 4)

Process (Clause 5)

a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization

ISO 31000 - Relationship between the principles, framework and process
5.3 ESTABLISHING THE CONTEXT
- 5.3.2 External Context
- 5.3.3 Internal Context
- 5.3.4 Risk Management Process Context
- 5.3.5 Developing Risk Criteria

5.4 RISK ASSESSMENT

5.4.2 RISK IDENTIFICATION
- What can happen, when, where, how & why

5.4.3 RISK ANALYSIS
- Determine existing controls
- Determine Likelihood
- Determine Consequences
- Estimate Level of Risk

5.4.4 RISK EVALUATION
- Compare against criteria.
- Identify & assess options.
- Decide on response.
- Establish priorities.

5.5 RISK TREATMENT
- 5.5.2 Selection of risk treatment options
- 5.5.3 Preparing and implementing risk treatment plans

Monitor & Review

Communication & Consultation
## Risk Analysis

### 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

### Treatment Decisions
- Context & Scope
- Risk Management Method
- Analyse Risks
- Evaluate Risks
- Communicate & Consult
- Monitor & Review

### Risk Management Method

#### Identify Risks
- **Almost Certain**
  - Insignificant: Medium
  - Minor: High
  - Moderate: High
  - Major: Extreme
  - Catastrophic: Extreme

#### Analyse Risks
- **Likely**
  - Insignificant: Medium
  - Minor: Medium
  - Moderate: High
  - Major: High
  - Catastrophic: Extreme

- **Possible**
  - Insignificant: Low
  - Minor: Medium
  - Moderate: Medium
  - Major: High
  - Catastrophic: High

- **Unlikely**
  - Insignificant: Low
  - Minor: Low
  - Moderate: Medium
  - Major: Medium
  - Catastrophic: High

- **Rare**
  - Insignificant: Low
  - Minor: Low
  - Moderate: Low
  - Major: Medium
  - Catastrophic: Medium

---

**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

**Use your organisation’s matrix**

---

29 May 2019
Context & Scope

• What’s the environment and what are we analysing?
• How will we approach it
• How deep will we go?
Define the Context

Context

- Why is the review taking place?
- Who are the consumers?
- What are the expectations and deliverables?
- Is there an existing framework?
- Are results of previous reviews available?
Operational risk management

Security risk management

Financial risk management including fraud risk

Personnel risk review elements incorporating:
- agency requirements
- program requirements
- sub-program requirements
- key individual requirements

Physical risk review elements incorporating:
- agency requirements
- site requirements
- area requirements

Information risk review elements incorporating:
- agency requirements
- site requirements
- compartmental requirements

Agency business plan

Operational plan

Security plan

Business continuity plan

Financial plan including fraud control plan

Personnel security policy and procedures elements:
- eligibility policy
- employment conditions (fit and proper person) checks policy
- DSAP and security clearance policy
- aftercare policy

Physical security policy and plan elements including:
- site security plans
- personal safety and security measures
- physical asset protection measures
- information protection measures

ICT and information security policy and plan elements including:
- ICT plan
- information classification policy
- access and availability policies

Security and fraud governance policies and procedures elements including:
- contractor security/fraud management policy
- security/fraud awareness training, investigations and review policy
- audit and reporting policy

International obligations
Risk Management Context

❖ How are other risks managed?
❖ Senior management risk management experience.
❖ Does the organisation plan or react?
❖ Who are risks reported to, accepted by?
❖ How do risk criteria fit the culture and practices?
❖ Are there specific business criteria?
How Mature is the Organisation?

Capability Maturity Model

<table>
<thead>
<tr>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimised</td>
</tr>
<tr>
<td>Managed</td>
</tr>
<tr>
<td>Defined</td>
</tr>
<tr>
<td>Repeatable</td>
</tr>
<tr>
<td>Initial/Adhoc</td>
</tr>
</tbody>
</table>
Scope the Review

Scope

- What exactly is being reviewed?
- Are there specific focus areas within the scope?
  - Hot buttons
- How far will the review go?
  - Level of detail
- Who is affected within the agency?
Typical Scope Options

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

- Identify
  - Internal policies
  - Business processes & goals
  - Legislation/regulations

- Operational context
  - Administrative processes
  - Team/division/section objectives
Planning

- Agree objectives with management & sponsors
- Identify key resources
- Set out a project plan
  - Tasks
  - Resources
  - Stakeholder scheduling
  - Timetable
First know what’s important

- Identify major operational processes
  - What’s your organisation’s purpose in life?
  - What’s your most important product?
- Identify Stakeholders
  - Who are your customers?
  - Who benefits from your activities?
Preparation - Outcomes

- Context & Scope Defined
- Management & Stakeholders on side
- Metrics and methods agreed
- Do-able Plan
Risk Identification

- List what could go wrong
5.3 ESTABLISHING THE CONTEXT
5.3.2 External Context
5.3.3 Internal Context
5.3.4 Risk Management Process Context
5.3.5 Developing Risk Criteria

5.4 RISK IDENTIFICATION
What can happen, when, where, how & why

5.4.2 RISK IDENTIFICATION
What can happen, when, where, how & why

5.4.3 RISK ANALYSIS
Determine existing controls
Determine Likelihood
Determine Consequences
Estimate Level of Risk

5.4.4 RISK EVALUATION
Compare against criteria.
Identify & assess options.
Decide on response.
Establish priorities.

5.5 RISK TREATMENT
5.5.2 Selection of risk treatment options
5.5.3 Preparing and implementing risk treatment plans
Identification

- What?
- When? (as in triggers)
- Where? What?
- How?
- Why?
Activities

- Identify critical assets
- Identify known and perceived threats
- Plot the threats in the Threat Matrix
  - Integrity
  - Confidentiality
  - Availability
Examples of Key Assets

- Reputation
- Payroll Process
  - supporting systems
- General Ledger
  - Access control, integrity checks
- Client list
  - Privacy and accuracy
- Intellectual Property
  - Timeliness and accuracy
- Sales & cash flow
  - And cancelled ones!
Major Areas of Risk

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

- Errors and omissions
- Malicious activity
  - internal
  - external
- Environmental threats
  - Fire, Flood
  - Power loss
  - natural disasters
Breadth First Search

<table>
<thead>
<tr>
<th>Accidental Events</th>
<th>Integrity</th>
<th>Confidentiality</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

Malicious Events

- Errors & Omissions
- Fraud, Hacking
Examples of Risks

- **Integrity**
  - Modified data in forms or databases
  - Unauthorised transactions

- **Confidentiality**
  - Sensitive personal information available on web
  - Disclosure of sensitive documents to a competitor

- **Availability**
  - Inadequate operational performance of IT systems
  - IT outage due to hardware failure
  - Customers cannot use online services due to denial of service attacks

<table>
<thead>
<tr>
<th></th>
<th>Integrity</th>
<th>Confidentiality</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accidental Events</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Malicious Events</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
</tbody>
</table>

Errors & Omissions
Fraud, Hacking
Risks and Threats

- **Confidentiality**
  - Hacker puts **customer file** on the Web
  - Email **orders** are read by competitors

- **Integrity**
  - Disgruntled employee modifies data in manufacturing database – produce faulty goods
  - MIS files modified by operators
  - Wrong pathology results lead to death

- **Availability**
  - Technician trips over cable
  - Power supply blows up
  - Denial of service attacks
  - No backups
  - Ransomware and extortion
Vulnerabilities - examples

- Operational complexity
- Lack of skills and competence
- Inadequate documentation
- No fall-back or recovery plans
- Poor access controls
- Software flaws
- Software Misconfiguration
How to List the Risks

- Workshop
- Brainstorm
  - Don’t debate
  - Value all input
- Record the risks
- Vulnerabilities
  - Gap Analysis
  - Vulnerability Scanner
  - Pen test
Risk Analysis

- Estimate the Likelihood and Consequences
- Identified Risks
5.3 ESTABLISHING THE CONTEXT
5.3.2 External Context
5.3.3 Internal Context
5.3.4 Risk Management Process Context
5.3.5 Developing Risk Criteria

5.4 RISK IDENTIFICATION
What can happen, when, where, how & why

5.4.2 RISK IDENTIFICATION
What can happen, when, where, how & why

5.4.3 RISK ANALYSIS
Determine existing controls
- Determine Likelihood
- Determine Consequences
- Estimate Level of Risk

5.4.4 RISK EVALUATION
Compare against criteria.
Identify & assess options.
Decide on response.
Establish priorities.

5.5 RISK TREATMENT
5.5.2 Selection of risk treatment options
5.5.3 Preparing and implementing risk treatment plans

ISO 31000 Risk management process in detail
Risk Analysis

- Determine likelihood
- Usually assume current controls
- Identify and scope consequences
- Determine levels of risk
- Identify
  - Medium/High/Extreme risk levels
## Risk Analysis

### Likelihood

<table>
<thead>
<tr>
<th>Measure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Is expected to occur in most conditions (1 or more times per year).</td>
</tr>
<tr>
<td>Medium</td>
<td>The event will probably happen in most conditions (2 years).</td>
</tr>
<tr>
<td>Low</td>
<td>The event should happen at some time (5 years).</td>
</tr>
<tr>
<td>Unlikely</td>
<td>The event could happen at some time (10 years).</td>
</tr>
</tbody>
</table>

*Customise for your organisation*
Likelihood of Specific Threats

❖ Information sources
  ▪ Operational history
  ▪ General experience
  ▪ Intelligence
  ▪ Industry information sharing

❖ Likelihood ratings
  ▪ High, medium or low
## Risk Analysis

### Impact

<table>
<thead>
<tr>
<th>Measure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Major</strong></td>
<td><strong>Major</strong> problems would occur and threaten the operation of important processes resulting in <strong>significant financial loss</strong>.</td>
</tr>
<tr>
<td><strong>Moderate</strong></td>
<td>Business would continue, but would be <strong>severely limited</strong>, resulting in some <strong>financial or opportunity loss</strong>.</td>
</tr>
<tr>
<td><strong>Minor</strong></td>
<td>Effectiveness of business operations would be <strong>threatened but dealt with</strong>.</td>
</tr>
<tr>
<td><strong>Insignificant</strong></td>
<td>Dealt with as a part of <strong>routine</strong> operations.</td>
</tr>
</tbody>
</table>

---

**Customise for your organisation**
## Impact Categories

<table>
<thead>
<tr>
<th></th>
<th>Safety</th>
<th>Financial</th>
<th>Reputation</th>
<th>Legal</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Many deaths</td>
<td>bankrupt</td>
<td>Lost govt customer confidence, global</td>
<td>Govt takeover, CEO jailed</td>
<td>Long term huge impact</td>
</tr>
<tr>
<td>Major</td>
<td>One death</td>
<td>Major loss</td>
<td>Nation wide adverse coverage, board spill</td>
<td>Govt intervention, major fines, board sacked</td>
<td>Severe impact</td>
</tr>
<tr>
<td>Moderate</td>
<td>Disabled</td>
<td>Lost profit</td>
<td>Adverse news</td>
<td>Fines, extra audit</td>
<td>Impact, major response</td>
</tr>
<tr>
<td>Minor</td>
<td>Hurt</td>
<td>&lt; $100 K</td>
<td>Local issue</td>
<td>Low fines</td>
<td>Special response</td>
</tr>
<tr>
<td>Insignificant</td>
<td>Timeoff</td>
<td>Petty cash</td>
<td>No one care</td>
<td>Noted</td>
<td>Normal response</td>
</tr>
</tbody>
</table>
Direct Consequences/Costs

- Work around costs
- Recovery costs
- Staff overtime
- Equipment replacement
- Data re-entry
- Reputation recovery
Consequential Loss - Examples

- Operational impairments
- Loss of capability and function
- “Courier Mail” factor
- Recovery, restoration, and penalty costs
- Damage or impact to other areas of operations
- Financial
- Opportunity lost
- Political
- Reputation & Confidence
- Liability – damages or criminal
Current Mitigations

- Assess likelihood and consequences levels according to existing controls
- Controls include any mitigating circumstances
  - Fire alarms, evacuation plans
  - Insurance
  - Access Controls & IT controls
  - Management Supervision, business processes
  - BCP, DRP, etc
Risk Analysis

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

Use your organisation’s matrix
Analysis Progress

- Identified assets at risk
- Identified threats
- Identify threat likelihood
- Estimate Consequences
- Rate Consequence
- Risks ranked
Risk Evaluation
Decisions Decisions . . .

image courtesy of www.novodiem-bv.com
5.3 ESTABLISHING THE CONTEXT
- 5.3.2 External Context
- 5.3.3 Internal Context
- 5.3.4 Risk Management Process Context
- 5.3.5 Developing Risk Criteria

5.4 RISK IDENTIFICATION
- Risk Assessment
  - What can happen, when, where, how & why

5.4.2 RISK IDENTIFICATION
- Determine existing controls
  - Determine Likelihood
  - Determine Consequences
  - Estimate Level of Risk

5.4.3 RISK ANALYSIS
- Compare against criteria.
- Identify & assess options.
- Decide on response.
- Establish priorities.

5.4.4 RISK EVALUATION
- Selection of risk treatment options
- Preparing and implementing risk treatment plans

5.5 RISK TREATMENT
- Monitor & Review

ISO 31000 Risk management process in detail

29 May 2019
Risk Evaluation

Risk Level

Risk Appetite

Risk 1

Risk 2

Risk 3

Risk 4
Evaluation

- Compare to criteria from the *context* phase
- Identify and assess options
- Decide on the response
  - Accept
  - Treat
  - Avoid
  - Transfer
- Establish priorities
## Risk Evaluation - Document

<table>
<thead>
<tr>
<th>Identification</th>
<th>Analysis</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payroll delayed due to EFT file corrupted</td>
<td>Existing Controls</td>
<td>Likelihood</td>
</tr>
<tr>
<td></td>
<td>CRC checks</td>
<td>Possible</td>
</tr>
<tr>
<td>IT outage - Flooded data centre, loss of sales, backups onsite</td>
<td>Backups</td>
<td>Rare</td>
</tr>
<tr>
<td>. . .</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Risk Treatment & Acceptance

- Determine appropriate actions to manage risk
5.2 COMMUNICATION & CONSULTATION

5.3 ESTABLISHING THE CONTEXT
- 5.3.2 External Context
- 5.3.3 Internal Context
- 5.3.4 Risk Management Process Context
- 5.3.5 Developing Risk Criteria

5.4 RISK

5.4.2 RISK IDENTIFICATION
- What can happen, when, where, how & why

5.4.3 RISK ANALYSIS
- Determine existing controls
- Determine Likelihood
- Determine Consequences
- Estimate Level of Risk

5.4.4 RISK EVALUATION
- Compare against criteria.
- Identify & assess options.
- Decide on response.
- Establish priorities.

5.5 RISK TREATMENT
- 5.5.2 Selection of risk treatment options
- 5.5.3 Preparing and implementing risk treatment plans

5.6 MONITOR & REVIEW

ISO 31000 Risk management process in detail

Copyright © Infosec Services Pty Ltd 2019
## Risk Evaluation

### Risk register

<table>
<thead>
<tr>
<th>Risk Description</th>
<th>Consequences of the Event</th>
<th>Existing controls</th>
<th>Consequence rating</th>
<th>Likelihood rating</th>
<th>Level of risk</th>
<th>Action priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure of payroll file transfer</td>
<td>4 Days Delay Paying employees</td>
<td>Courier backup</td>
<td>MODERATE</td>
<td>HIGH</td>
<td>HIGH</td>
<td>?</td>
</tr>
<tr>
<td>Flooded data centre</td>
<td>IT Outage, No sales</td>
<td>DR Plan</td>
<td>MAJOR</td>
<td>POSSIBLE</td>
<td>HIGH</td>
<td>?</td>
</tr>
</tbody>
</table>
Risk Management Decisions

Level of Risk

- Catastrophic
- Insignificant

Cost of Treatment

- No Brainer
- Open for debate!
- Forget it!
Set Treatment Priorities

- **Highest level risks first**
  - don’t ignore the hard issue/high risk

- **Schedule the simple and cheap**
  - ‘quick fixes’

- **Must plan to treat high or extreme risks**
  - Often regulated requirements

- **Report other risks**
Set Treatment Priorities

- Risk level does not equal priority!
  - Fixing one risk could reduce other high risks
  - Quick wins = commonsense
- Priorities must be set within risk levels
  - Constraints, timing, ease of implementation
  - Treating certain risks may have greater effect on overall organizational risk
Risk Treatment

- Treatment options
- Treatment decision
- Consider constraints
- Control classes
- Plan
Control Constraints

❖ Culture
❖ System lifecycle
❖ 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
Control Classes

✦ Major/Classic
  - Prevention
  - Detection
  - Correction

✦ Minor
  - Deterrence
  - Limitation
  - Recovery
Treatment Plans

- Senior Management Accountability
- Funding
  - Existing operational budget
  - Additional funding
- Scheduling
Risk Acceptance

- Risk can only be accepted by accountable management or board

- The higher the risk level, the higher the appropriate authority required
Risk Acceptance

- Report residual risk to process owners, senior management

- Accepting the risk is not the end of the process!!
  - Changes to the risk and operating environment require ongoing monitoring
Tools
Tools for Risk Assessments

- **Risk identification**
  - The risk analysis matrix – via a spreadsheet!
- **Documentation for each phase**
  - Emphasis on appropriate level of detail/abstraction
- **More advanced tools**
  - Risk databases
  - Workflow
  - Corpgovrisk.com
  - CRAMM
  - SAAS – e.g. intelligence bank – GRC tools
Identification Tools

- Interviews
- Workshops
- Experienced staff/consultants
- Checklists of risks, standards
- Process flowcharts
- CIA analysis
- Scenario analysis
- Formal tools
Risk Analysis Tools

- **Matrices**
  - Likelihood (Threat/Vulnerability)
  - Risk (Impact/Likelihood)

- **Spreadsheets**
## Sample RM Table

<table>
<thead>
<tr>
<th>Risk Assessment</th>
<th>Analysis</th>
<th>Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>Likelihood</td>
<td>Impact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Gap Analysis Table

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Current controls</th>
<th>Compliance Level</th>
<th>Residual Risk</th>
<th>Recommendation</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classify assets</td>
<td>Policy Training</td>
<td>Partial</td>
<td>High</td>
<td>Reduce risk Train staff</td>
<td>Security Manager</td>
</tr>
<tr>
<td>Business Continuity Management</td>
<td>No BCP</td>
<td>Nil</td>
<td>Extreme</td>
<td>Reduce risk Develop BCP</td>
<td>CIO</td>
</tr>
</tbody>
</table>
Gap Analysis Inputs

❖ Standards
  ▪ ISO/AS 27002
  ▪ PCIDSS
  ▪ Aust Govt – ISM, Top Mitigations list

❖ Sector Guides
  ▪ APRA
  ▪ TISN – Critical Infrastructure

❖ Vendor Guides
  ▪ IT Infrastructure
Documentation

- Risk identification
  - List of threats and vulnerabilities

- Risk analysis
  - List of risks including probability and the likely impact

- Risk evaluation
  - List of prioritised risks

- Risk acceptance
  - Management acknowledgement of current risks

- Risk treatment
  - Plans for risk mitigation
Techniques

Find the ‘best fit’ approach
Levels of Rigour

- **Informal judgement** *(for high level RA)*
  - Rely on local skills and experience
  - Operational history
  - Expert review and assistance

- **Semi formal** *(appropriate for subsequent detailed RA)*
  - Workshopping, scenario walkthroughs
  - Delphi technique

- **Formal**
  - Actuary
  - Fault tree analysis

- **CRAMM, RAMP and other (expensive) software**
Techniques – Context & Scope
Context & Scope Techniques

❖ Sponsor

❖ Legal drivers
  ▪ General Counsel
Techniques – Risk Identification
Identification Techniques

❖ **Brainstorming**
   - Interviews
   - Workshops

❖ **Standards & guidelines**

❖ **Project, IT documentation**

❖ **Industry experience**
   - Verizon Data Breach Investigations Report
   - Industry information sharing networks
     - Formal and informal!
   - AusCERT, CERT Australia
Techniques – Risk Analysis
Analysis Techniques

❖ Likelihood
  ▪ Collecting opinions
  ▪ Industry averages

❖ Impacts
  ▪ Corporate documentation
  ▪ Interview C suite

❖ Risk level
  ▪ Use/extend enterprise risk framework
Techniques - Evaluation
Evaluation Techniques

❖ Compare against criteria
❖ Assess options
  ▪ Accept
  ▪ Treat
  ▪ Avoid
  ▪ Transfer
❖ Executive discussions
❖ Record recommendations and decisions
Techniques – Treatment Plans
Treatment Techniques

- Treatment plans, security plans, programs
- Prioritise actions
- Treatment planning
  - Identify control options
  - Costs v’s benefits
    - Financial costs
    - Operational costs
    - Opportunity costs
Treatment Costing

- Business as usual
- Operation funding
  - Management level approvals?
- Capital expenditure funding
- Timeframes
- Benefits
  - Is the treatment worth the effort?
Advanced Risk Management
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

The Three Lines of Defense Model

Governed by:
- Governing Body / Board / Audit Committee

1st Line of Defense:
- Management Controls
- Internal Control Measures

2nd Line of Defense:
- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance

3rd Line of Defense:
- Internal Audit

Adapted from ECIICIA/FRMA Guidance on the 8th EU Company Law Directive, article 41
NIST SP800-30 (USA)
Step 1: Prepare for Assessment
Derived from Organizational Risk Frame

Step 2: Conduct Assessment
Expanded Task View
- Identify Threat Sources and Events
- Identify Vulnerabilities and Predisposing Conditions
- Determine Likelihood of Occurrence
- Determine Magnitude of Impact
- Determine Risk

Step 3: Communicate Results

Step 4: Maintain Assessment

FIGURE 5: RISK ASSESSMENT PROCESS
Support for Security

Impact

Likelihood

Difficult

No Arguments

Low priority

Usually controlled

Copyright © Infosec Services Pty Ltd 2019
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
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
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
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
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
Threat Assessment

<table>
<thead>
<tr>
<th>Source</th>
<th>Motivation</th>
<th>Intent</th>
<th>Capability</th>
<th>Threat Level</th>
<th>Evaluation &amp; Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

29 May 2019
## Threat & Likelihood

<table>
<thead>
<tr>
<th></th>
<th>Low skill threat</th>
<th>Medium skill threat actors, not targeted</th>
<th>Medium skill threat actors, targeted</th>
<th>High skill threat actors, targeted (Capability &amp; Intent)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low maturity controls</td>
<td>Unlikely</td>
<td>Possible</td>
<td>Probable</td>
<td>Almost Certain</td>
</tr>
<tr>
<td>Repeatable controls, no assurance</td>
<td>Unlikely</td>
<td>Possible</td>
<td>Possible</td>
<td>Probable</td>
</tr>
<tr>
<td>Reasonable controls</td>
<td>Rare</td>
<td>Unlikely</td>
<td>Unlikely</td>
<td>Possible</td>
</tr>
<tr>
<td>Strong and verified controls</td>
<td>Rare</td>
<td>Rare</td>
<td>Unlikely</td>
<td>Possible</td>
</tr>
</tbody>
</table>
## Risk Likelihood via Threat Analysis

### Vulnerability Level

<table>
<thead>
<tr>
<th>Threat Level</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Moderate</td>
<td>Likely</td>
<td>Almost Certain</td>
</tr>
<tr>
<td>Medium</td>
<td>Unlikely</td>
<td>Moderate</td>
<td>Likely</td>
</tr>
<tr>
<td>Low</td>
<td>Rare</td>
<td>Unlikely</td>
<td>Moderate</td>
</tr>
</tbody>
</table>
## Analyse Consequences

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Financial</th>
<th>WHS</th>
<th>Legal</th>
<th>Reputation</th>
<th>Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Profit x 10</td>
<td>Multiple</td>
<td>Loss of licence</td>
<td>Long term negative brand</td>
<td>Long term severe damage</td>
</tr>
<tr>
<td>Severe</td>
<td>Profit x 1</td>
<td>Death, severe injury</td>
<td>Restricted licence,</td>
<td>Media campaign</td>
<td>Short term severe damage</td>
</tr>
<tr>
<td>Major</td>
<td>10% of profit</td>
<td>Serious injury</td>
<td>Fines, damages</td>
<td>Adverse media</td>
<td>Major damage</td>
</tr>
<tr>
<td>Minor</td>
<td>1% profit</td>
<td>Minor injury</td>
<td>Technicality</td>
<td>Minor exposure</td>
<td>Repairable</td>
</tr>
<tr>
<td>Insignificant</td>
<td>&gt; $ 5000</td>
<td>Loss of time</td>
<td>Mediation</td>
<td>Limited</td>
<td>Negligible</td>
</tr>
</tbody>
</table>
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.
## Risk register

<table>
<thead>
<tr>
<th>Risk Description</th>
<th>Risk Assessment</th>
<th>Existing controls</th>
<th>Impact Rating</th>
<th>Likelihood Rating</th>
<th>Level of Risk</th>
<th>Risk priority</th>
<th>Treatment Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Compromise</td>
<td>Intrusion, Disruption</td>
<td>Password Only</td>
<td>MODERATE</td>
<td>HIGH</td>
<td>HIGH</td>
<td>2</td>
<td>Project Y03</td>
</tr>
<tr>
<td>Physical Destruction of Data Centre</td>
<td>Operations Disrupted for one month</td>
<td>None (Not addressed in BCP)</td>
<td>MAJOR</td>
<td>LOW</td>
<td>HIGH</td>
<td>1</td>
<td>Project Z21</td>
</tr>
</tbody>
</table>
## TABLE I-5: TEMPLATE – ADVERSARIAL RISK

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

29 May 2019

Copyright © Infosec Services Pty Ltd 2019
TECHNIQUES – PROGRESS REPORTS
Scorecards & Self Assessment

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

<table>
<thead>
<tr>
<th>Target</th>
<th>Measure</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>85% of new projects</td>
<td>Completed Self Assessments</td>
<td>60%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>85%</td>
</tr>
<tr>
<td>85% of new projects</td>
<td>Completed Security Plans</td>
<td>50%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>85%</td>
</tr>
<tr>
<td>Security plans on schedule</td>
<td>Milestones and deliverables</td>
<td>80%</td>
</tr>
<tr>
<td>100% of project managers trained in year</td>
<td>25% of project managers in training this quarter</td>
<td>14%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>25%</td>
</tr>
</tbody>
</table>

Result: 6.5 out of 10
Capability Maturity Model

- Optimised
- Managed
- Defined
- Repeatable
- Initial/Adhoc
Risk Acceptance

- Don’t surprise management
- Residual risk acceptance
- Continual improvement
  - Monitor & review
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
Decisions and Outcomes
Persuasion

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

- Objective evidence rarely changes minds
  - 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
You don’t have to manage risk

Survival is not compulsory!
Best of Luck!

Gary Gaskell
E: gary.gaskell@infosecservices.com.au
W: www.infosecservices.com.au
M: 0438 603 307

Infosec Services Pty Ltd