Risk Definition

Risk is anything that may affect the ability of organisation to achieve its objectives.

Covering

- Hazard - Bad things are happening
- Uncertainty – Things are not occurring as expected
- Opportunity – Good things are not happening

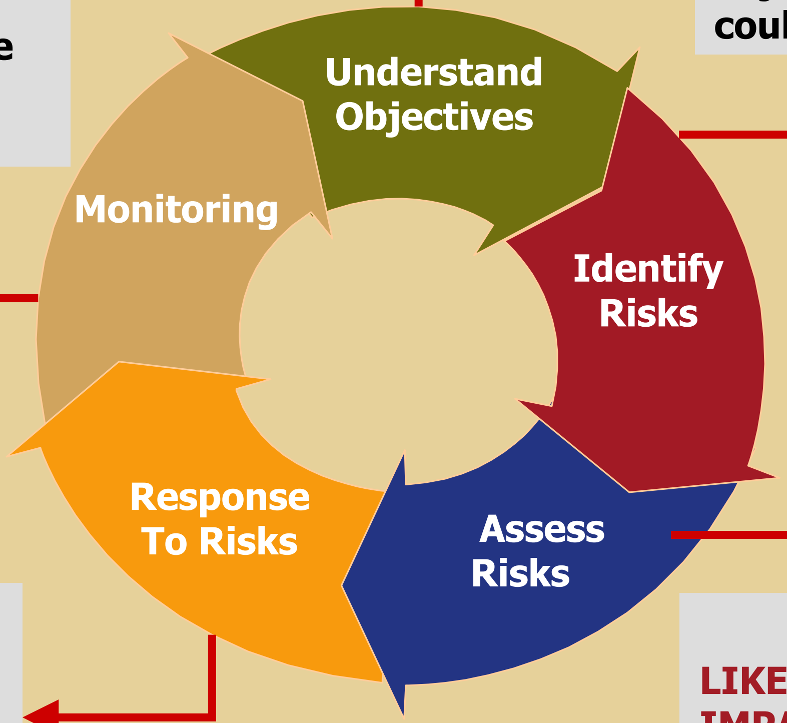
Risk Definition (continue)

Inherent Risk

Residual Risk

Acceptable Risk

Risk Management Process



Understand Objectives

Identify Risks

Assess Risks

Response To Risks

Monitoring

IT objectives should be define in such a way that inline with business objectives. 7 IT objectives could be used as a basis.

Anything that can affect ability to achieve above objectives.

People, Process and Technology

LIKELIHOOD of occurrence and **IMPACT** to objective would be assess at both **INHERENT** and **RESIDUAL** level.

If **RESIDUAL** risk is still exceed **ACCEPTABLE** risk, additional risk response should be implemented.

All steps would be monitored to ensure that risk and response are align at all time

IT Objectives

CobiT's Information Criteria can be used as a basis to define IT objectives

7 Criteria are

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

IT Risk Assessment

2. Risk Identification

People, Process & Technology

Internal & External

Hazard, Uncertainty & Opportunity

Effectiveness & Efficiency

- Poor management (planning & policy)
- System (H/W & Technology
- Skills of IT and non-IT
- Processing management (design & executions)

Confidentiality

- Security management (policy & procedure)
- System (H/W & Technology & network)
- User awareness
- Hackers, Viruses

Availability

- System & network design
- Hardware fails
- External sabotage
- Viruses & Attack
- No BCP, backup & recovery

Reliability & Integrity

- System design (input, process & output)
- Hackers & Unauthorised access
- Poor authority granting procedures

Compliance

- Unaware or not understand rules and regulations
- No monitoring

IT Risk Assessment

3. Assessment : (Business Impacts & Likelihood)

Business Impacts

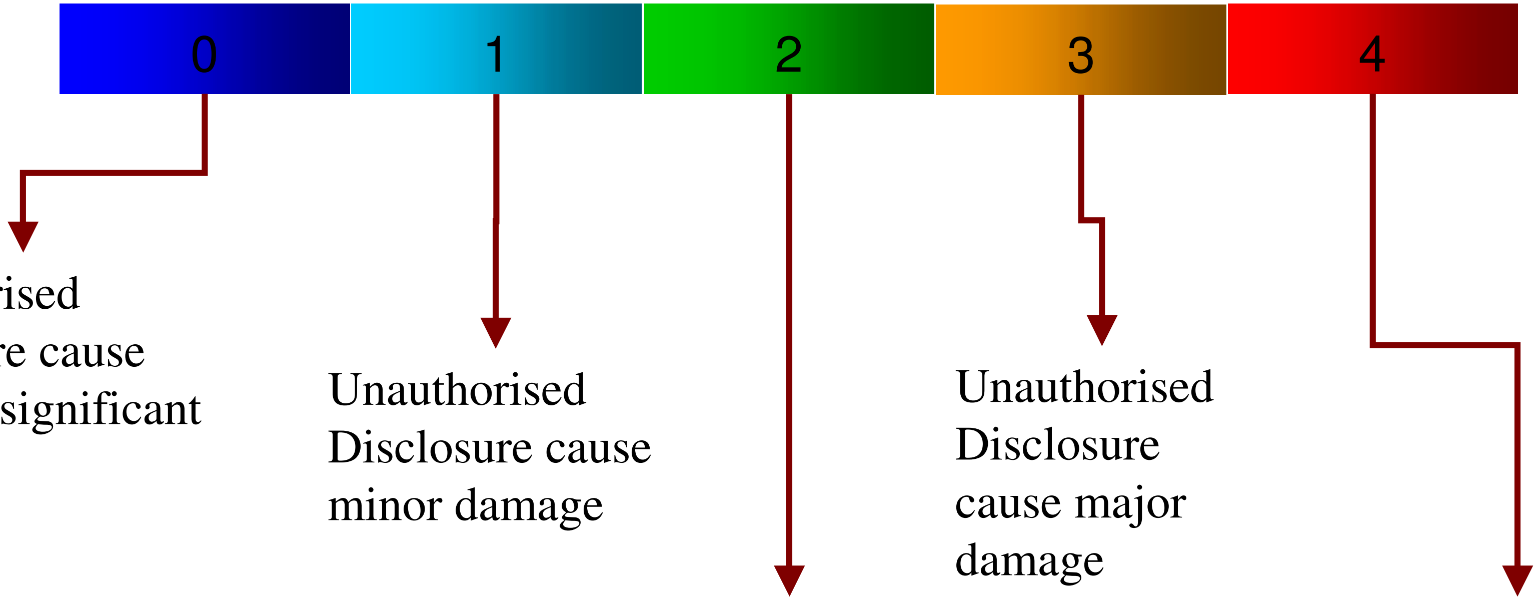
- Financial Impacts
- Damage to Reputations, due to unsecured systems
- Interruption to business operations
- Loss of valuable assets (system and data)
- Delay in decision making process

Likelihood

- Nature of business (industry)
- Organisation structure & culture
- Nature of the system (open & close, new & outdate technology)
- Existing Controls
- Etc.

Risk Assessment - Impacts

Assessing the Business Impacts – (e.g. Confidentiality)



Unauthorised Disclosure cause almost insignificant damage

Unauthorised Disclosure cause minor damage

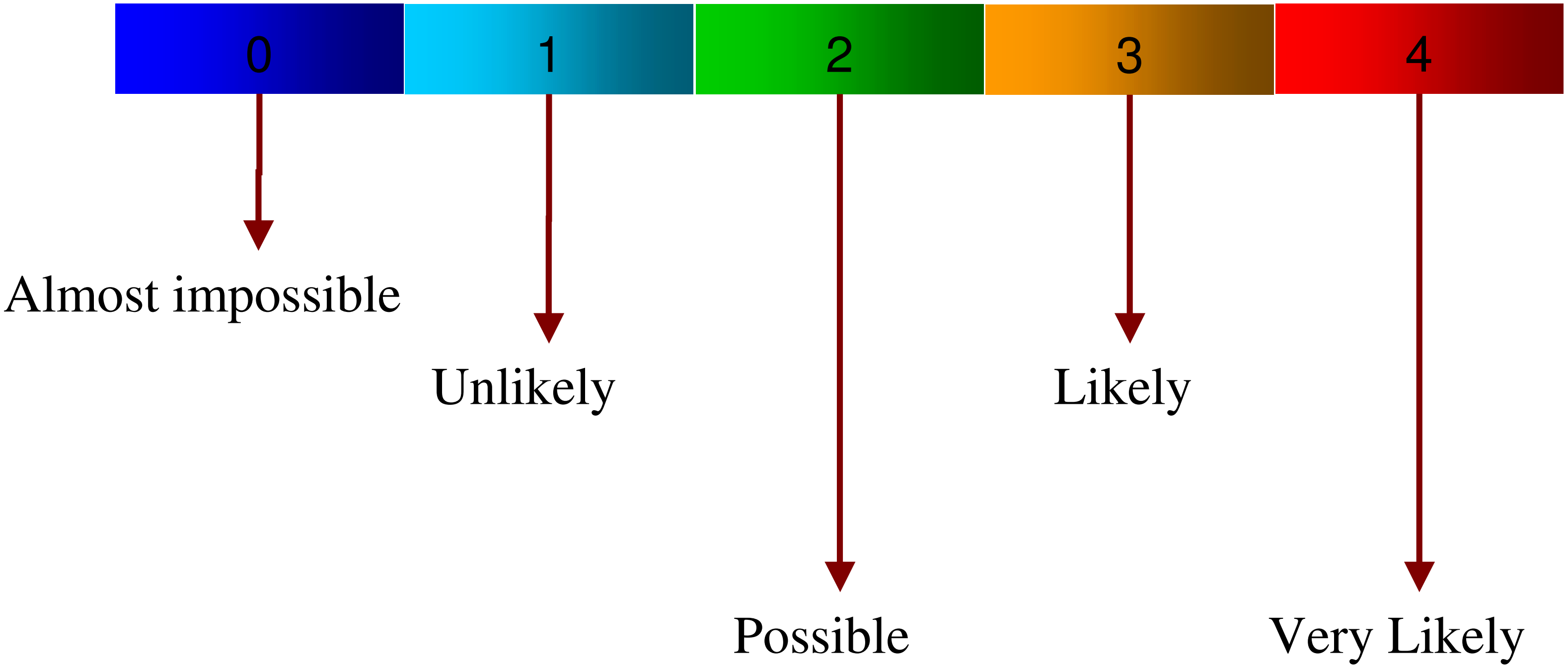
Unauthorised Disclosure cause significant but tolerable.

Unauthorised Disclosure cause major damage

Unauthorised Disclosure could threaten business survival.

Risk Assessment - Likelihood

Assessing the Likelihood - **(e.g. confidentiality)**



0

1

2

3

4

Almost impossible

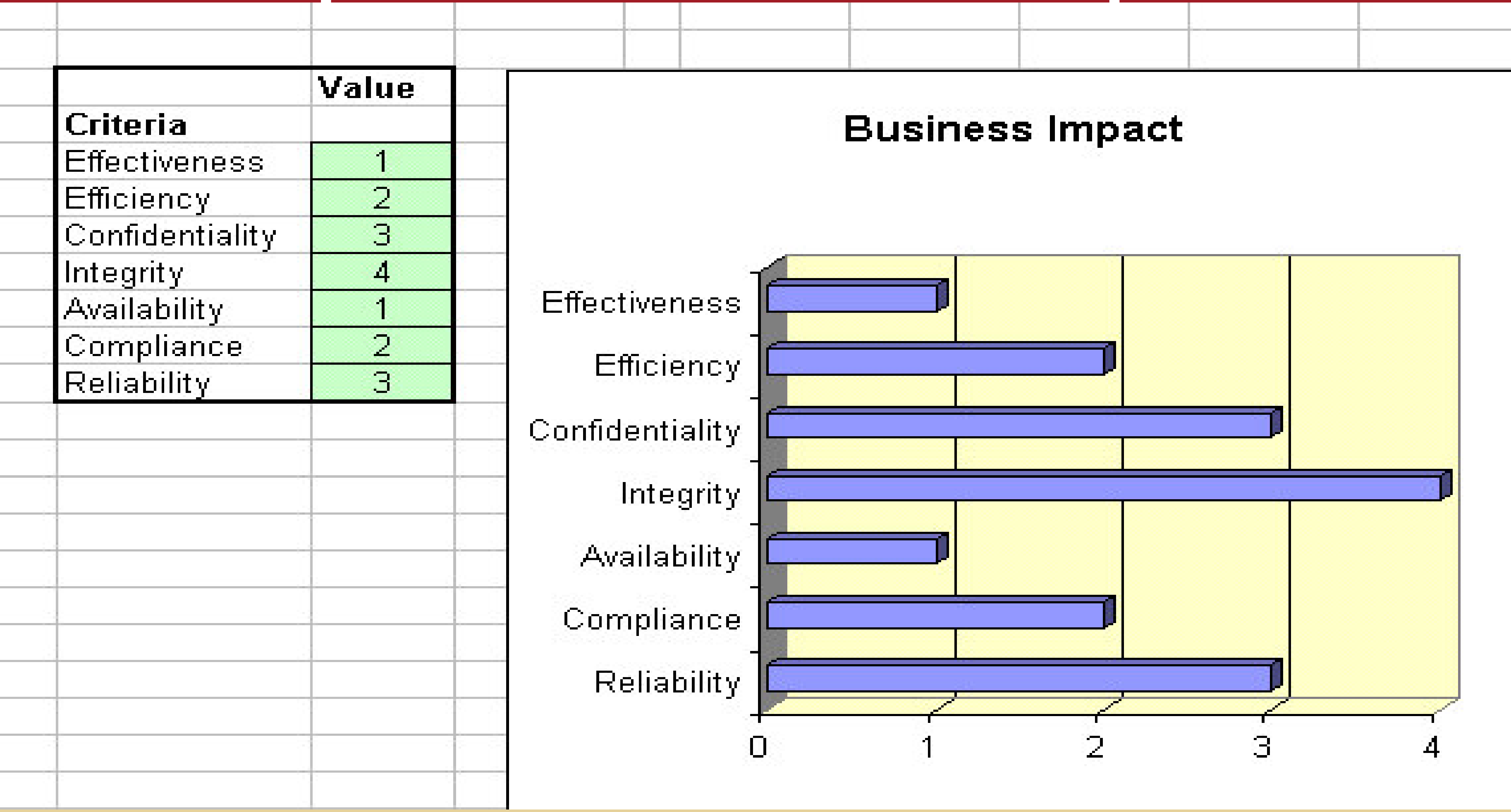
Unlikely

Possible

Likely

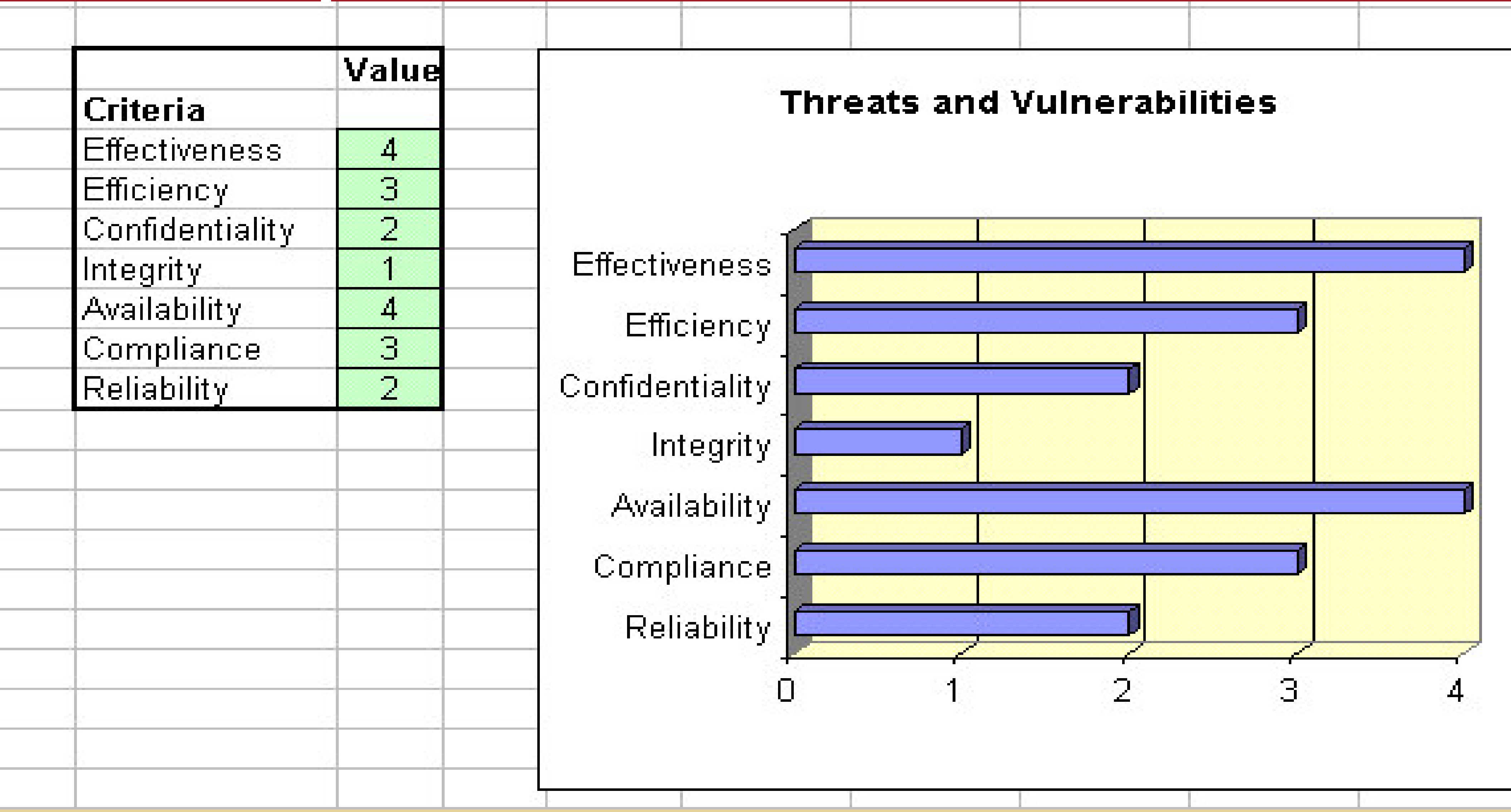
Very Likely

Example – Overall Business Impacts



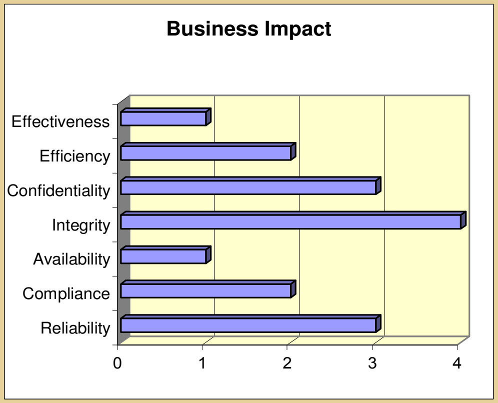
	Value
Criteria	
Effectiveness	1
Efficiency	2
Confidentiality	3
Integrity	4
Availability	1
Compliance	2
Reliability	3

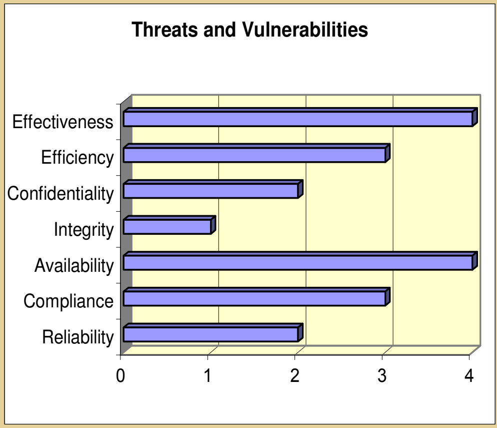
Example – Overall Likelihood



Criteria	Value
Effectiveness	4
Efficiency	3
Confidentiality	2
Integrity	1
Availability	4
Compliance	3
Reliability	2

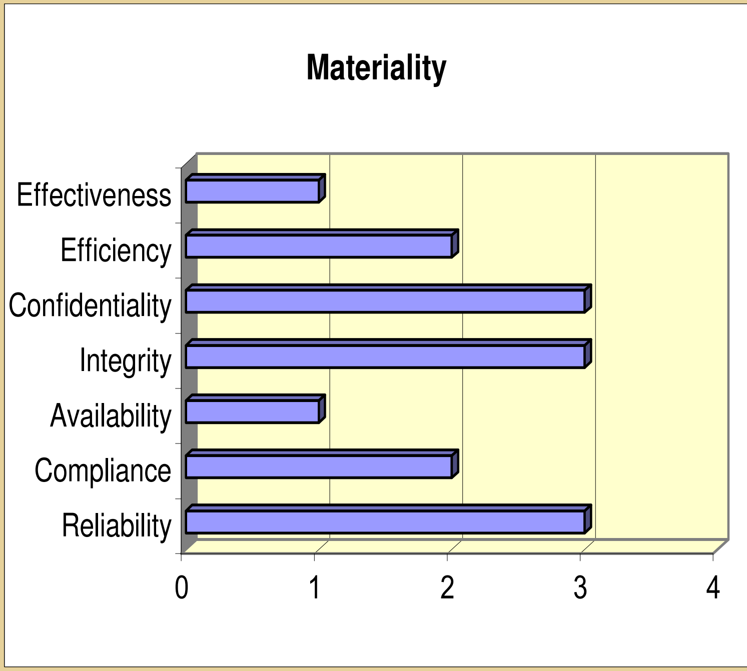
Combine Impacts & Likelihood





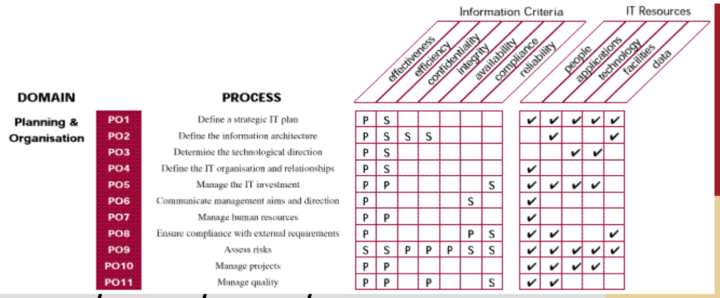
Risk Aversion Table

	BIF				
T&V	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	0	1	2	3
2	0	1	2	3	4
3	0	1	2	3	4
4	0	1	2	4	4



Inherent Risk

From assessment of Impacts & Likelihood



	DOMAIN	PROCESS	effectiveness	efficiency	confidentiality	integrity	availability	compliance	reliability	people	applications	technology	facilities	data
			Information Criteria							IT Resources				
Planning & Organisation	PO1	Define a strategic IT plan	P	S						✔	✔	✔	✔	✔
	PO2	Define the information architecture	P	S	S	S					✔			✔
	PO3	Determine the technological direction	P	S								✔	✔	
	PO4	Define the IT organisation and relationships	P	S						✔				
	PO5	Manage the IT investment	P	P					S	✔	✔	✔	✔	
	PO6	Communicate management aims and direction	P					S		✔				
	PO7	Manage human resources	P	P						✔				
	PO8	Ensure compliance with external requirements	P					P	S	✔	✔			✔
	PO9	Assess risks	S	S	P	P	P	S	S	✔	✔	✔	✔	✔
	PO10	Manage projects	P	P						✔	✔	✔	✔	
	PO11	Manage quality	P	P		P			S	✔	✔			

F5	Inherent Risk	Effectiveness	Efficiency	Confidentialit y	Integrity	Availibility	Compliance	Reliability
	Materiality	**1**	**2**	**3**	**3**	**1**	**2**	**3**
Planning and organisation								
PO 1	Define a strategic IT plan	H	C					
PO 2	Define the information architecture	H	C	C	C			
PO 3	Determine the technological direction	H	C					
PO 4	Define organisation and relationships	H	C					
PO 5	Manage the investment	H	C					C
PO 6	Communicate management aims and direction	H					C	
PO 7	Manage human resources	H	C					
PO 8	Ensure compliance with external requirements	H					C	C
PO 9	Assess risk	H	C	E	E	H	C	C
PO 10	Manage projects	H	C					
PO 11	Manage quality	H	C		E			C
Acquisition and implementation								
AI 1	Identify automated solutions	H	C					
AI 2	Acquire and maintain application software	H	C		C		C	C
AI 3	Acquire and maintain technology architecture	H	C		C			
AI 4	Develop and maintain procedures	H	C		C		C	C
AI 5	Install and accredit systems	H			C	H		
AI 6	Managing changes	H	C		E	H		C

Legends

🟥 Exposure
🟧 Concern
🟩 Housekeeping
🟩 OK

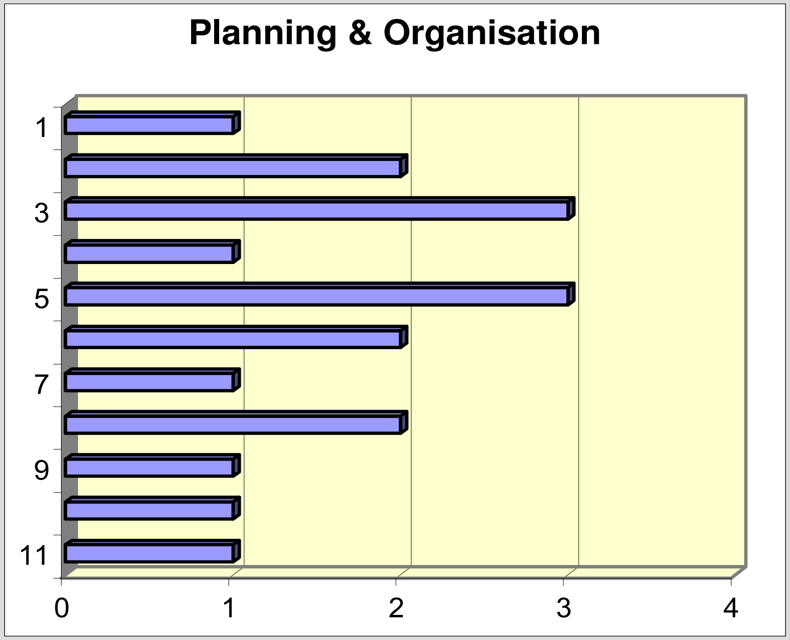
Evaluate Controls

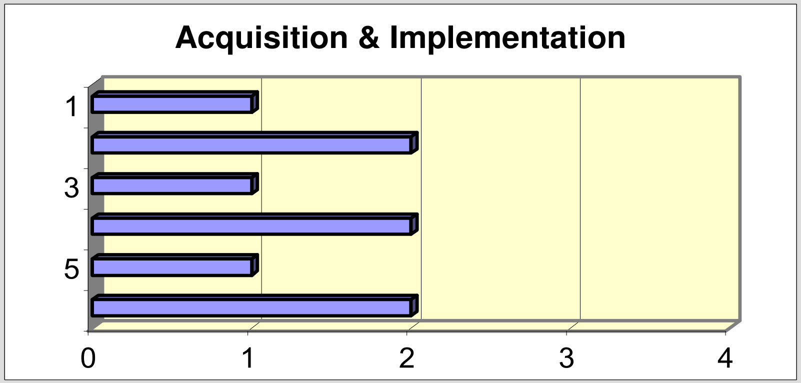
Planning and organisation

PO 1	Define a strategic IT plan	1
PO 2	Define the information architecture	2
PO 3	Determine the technological direction	3
PO 4	Define organisation and relationships	1
PO 5	Manage the investment	3
PO 6	Communicate management aims and direction	2
PO 7	Manage human resources	1
PO 8	Ensure compliance with external requirements	2
PO 9	Assess risk	1
PO 10	Manage projects	1
PO 11	Manage quality	1

Acquisition and implementation

AI 1	Identify automated solutions	1
AI 2	Acquire and maintain application software	2
AI 3	Acquire and maintain technology architecture	1
AI 4	Develop and maintain procedures	2
AI 5	Install and accredit systems	1
AI 6	Managing changes	2





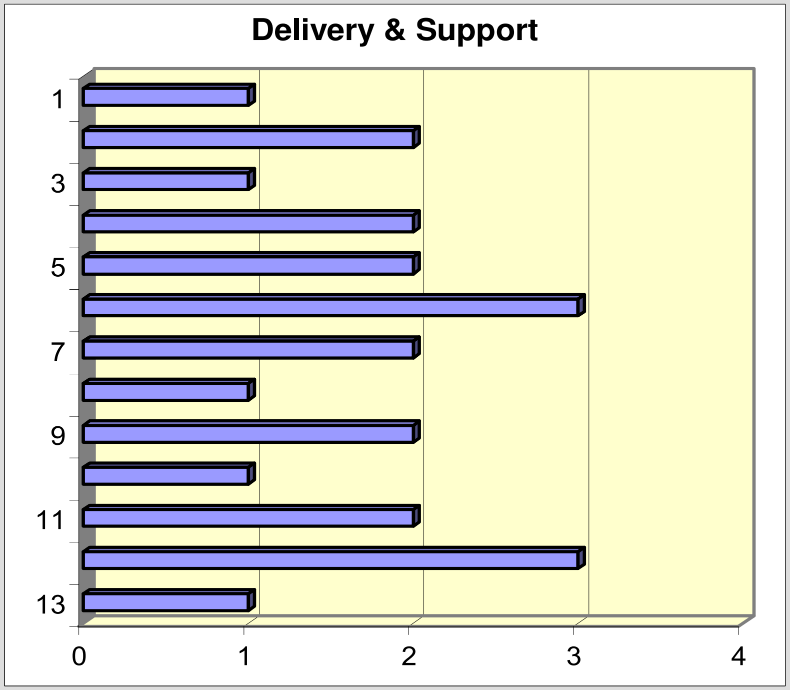
Evaluate Controls

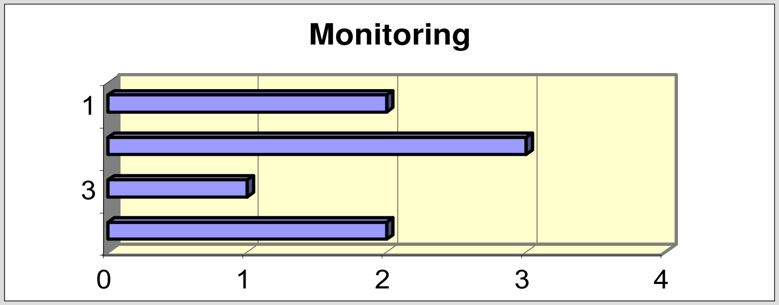
Delivery and support

DS 1	Define service levels	1
DS 2	Manage third-party services	2
DS 3	Manage performance and capacity	1
DS 4	Ensure continuous service	2
DS 5	Ensure systems security	2
DS 6	Identify and allocate costs	3
DS 7	Educate and train users	2
DS 8	Assist and advice customers	1
DS 9	Manage the configuration	2
DS 10	Manage problems and incidents	1
DS 11	Manage data	2
DS 12	Manage facilities	3
DS 13	Manage operations	1

Monitoring

M 1	Monitor the processes	2
M 2	Assess internal control adequacy	3
M 3	Obtain Independent Assurance	1
M 4	Provide for independent audit	2


Delivery & Support


Monitoring

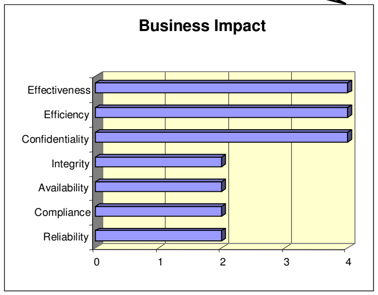
Residual Risks

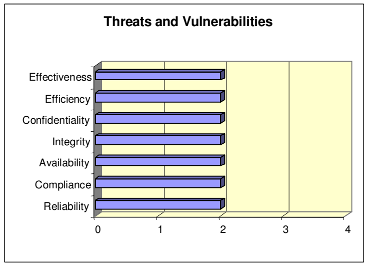
E2	Control Risk	*Control Evaluation*	Effectiveness	Efficiciency	Confidentiality	Integrity	Availibility	Compliance	Reliability
	Materiality		**1**	**2**	**3**	**3**	**1**	**2**	**3**
Planning and organisation									
PO 1	Define a strategic IT plan	**1**	O	H					
PO 2	Define the information architecture	**2**	+	O	H	H			
PO 3	Determine the technological direction	**3**	+	+					
PO 4	Define organisation and relationships	**1**	O	H					
PO 5	Manage the investment	**3**	+	+					O
PO 6	Communicate management aims and direction	**2**	+					O	
PO 7	Manage human resources	**1**	O	H					
PO 8	Ensure compliance with external requirements	**2**	+					O	H
PO 9	Assess risk	**1**	O	H	C	C	O	H	C
PO 10	Manage projects	**1**	O	H					
PO 11	Manage quality	**1**	O	H		C			C
Acquisition and implementation									
AI 1	Identify automated solutions	**1**	O	H					
AI 2	Acquire and maintain application software	**2**	+	O		H		O	H
AI 3	Acquire and maintain technology architecture	**1**	O	H		C			
AI 4	Develop and maintain procedures	**2**	+	O		H		O	H
AI 5	Install and accredit systems	**1**	O			C	O		
AI 6	Managing changes	**2**	+	O		H	+		H

Legends

- 🟥 Exposure
- 🟧 Concern
- 🟩 Housekeeping
- 🟩 OK
- 🟦 Overprotected

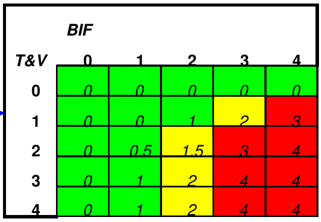
Questionnaires





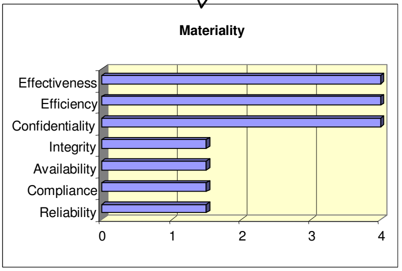
Questionnaires

Risk Aversion Matrix

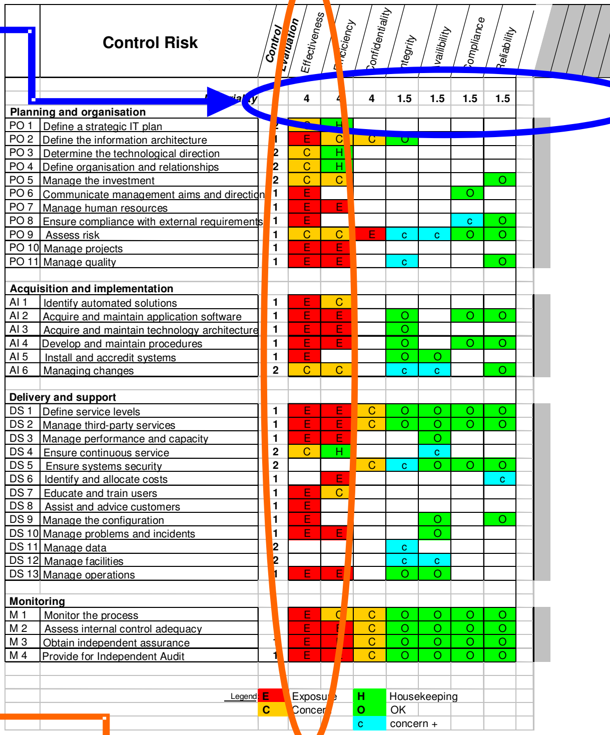


T&V \ BIF	0	1	2	3	4
0	*0*	*0*	*0*	*0*	*0*
1	*0*	*0*	*1*	*2*	*3*
2	*0*	*0.5*	*1.5*	*3*	*4*
3	*0*	*1*	*2*	*4*	*4*
4	*0*	*1*	*2*	*4*	*4*

Materiality Intermediate Result



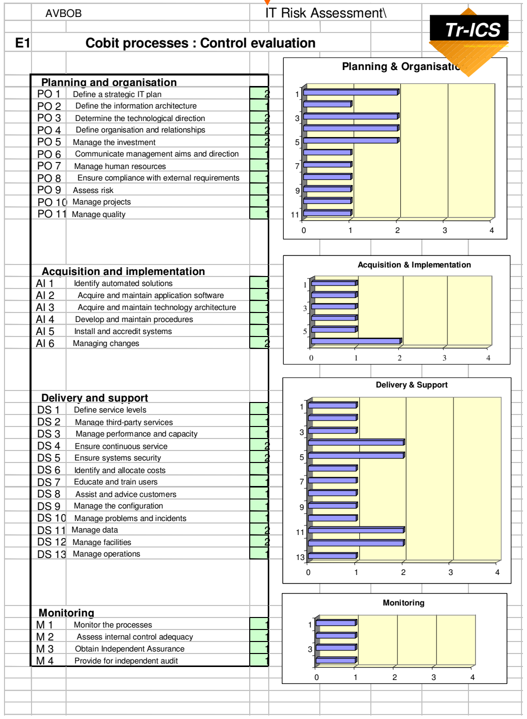
Control Risk Matrix



Control Risk

		Control Evaluation	Effectiveness	Efficiency	Confidentiality	Integrity	Availibility	Compliance	Reliability
	Materiality		4	4	4	1.5	1.5	1.5	1.5
Planning and organisation									
PO 1	Define a strategic IT plan	2	C	H					
PO 2	Define the information architecture	1	E	C	C	O			
PO 3	Determine the technological direction	2	C	H					
PO 4	Define organisation and relationships	2	C	H					
PO 5	Manage the investment	2	C	C					O
PO 6	Communicate management aims and direction	1	E					O	
PO 7	Manage human resources	1	E	E					
PO 8	Ensure compliance with external requirements	1	E					c	O
PO 9	Assess risk	1	C	C	E	c	c	O	O
PO 10	Manage projects	1	E	E					
PO 11	Manage quality	1	E	E		c			O
Acquisition and implementation									
AI 1	Identify automated solutions	1	E	C					
AI 2	Acquire and maintain application software	1	E	E		O		O	O
AI 3	Acquire and maintain technology architecture	1	E	E		O			
AI 4	Develop and maintain procedures	1	E	E		O		O	O
AI 5	Install and accredit systems	1	E			O	O		
AI 6	Managing changes	2	C	C		c	c		O
Delivery and support									
DS 1	Define service levels	1	E	E	C	O	O	O	O
DS 2	Manage third-party services	1	E	E	C	O	O	O	O
DS 3	Manage performance and capacity	1	E	E			O		
DS 4	Ensure continuous service	2	C	H			c		
DS 5	Ensure systems security	2			C	c	O	O	O
DS 6	Identify and allocate costs	1		E					c
DS 7	Educate and train users	1	E	C					
DS 8	Assist and advice customers	1	E						
DS 9	Manage the configuration	1	E				O		O
DS 10	Manage problems and incidents	1	E	E			O		
DS 11	Manage data	2				c			
DS 12	Manage facilities	2				c	c		
DS 13	Manage operations	1	E	E		O	O		
Monitoring									
M 1	Monitor the process		E	C	C	O	O	O	O
M 2	Assess internal control adequacy		E	E	C	O	O	O	O
M 3	Obtain independent assurance	1	E	E	C	O	O	O	O
M 4	Provide for Independent Audit	1	E	E	C	O	O	O	O

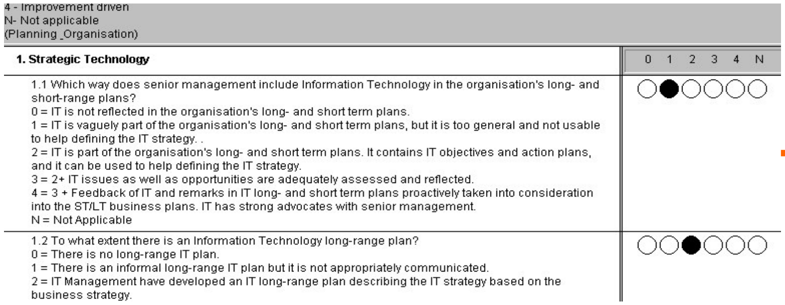
Legend:			
E	Exposure	H	Housekeeping
C	Concern	O	OK
		c	concern +



AVBOB IT Risk Assessment\

E1 **Cobit processes : Control evaluation**

Planning and organisation		
PO 1	Define a strategic IT plan	2
PO 2	Define the information architecture	1
PO 3	Determine the technological direction	2
PO 4	Define organisation and relationships	2
PO 5	Manage the investment	2
PO 6	Communicate management aims and direction	1
PO 7	Manage human resources	1
PO 8	Ensure compliance with external requirements	1
PO 9	Assess risk	1
PO 10	Manage projects	1
PO 11	Manage quality	1
Acquisition and implementation		
AI 1	Identify automated solutions	1
AI 2	Acquire and maintain application software	1
AI 3	Acquire and maintain technology architecture	1
AI 4	Develop and maintain procedures	1
AI 5	Install and accredit systems	1
AI 6	Managing changes	2
Delivery and support		
DS 1	Define service levels	1
DS 2	Manage third-party services	1
DS 3	Manage performance and capacity	1
DS 4	Ensure continuous service	2
DS 5	Ensure systems security	2
DS 6	Identify and allocate costs	1
DS 7	Educate and train users	1
DS 8	Assist and advice customers	1
DS 9	Manage the configuration	1
DS 10	Manage problems and incidents	1
DS 11	Manage data	2
DS 12	Manage facilities	2
DS 13	Manage operations	1
Monitoring		
M 1	Monitor the processes	1
M 2	Assess internal control adequacy	1
M 3	Obtain Independent Assurance	1
M 4	Provide for independent audit	1



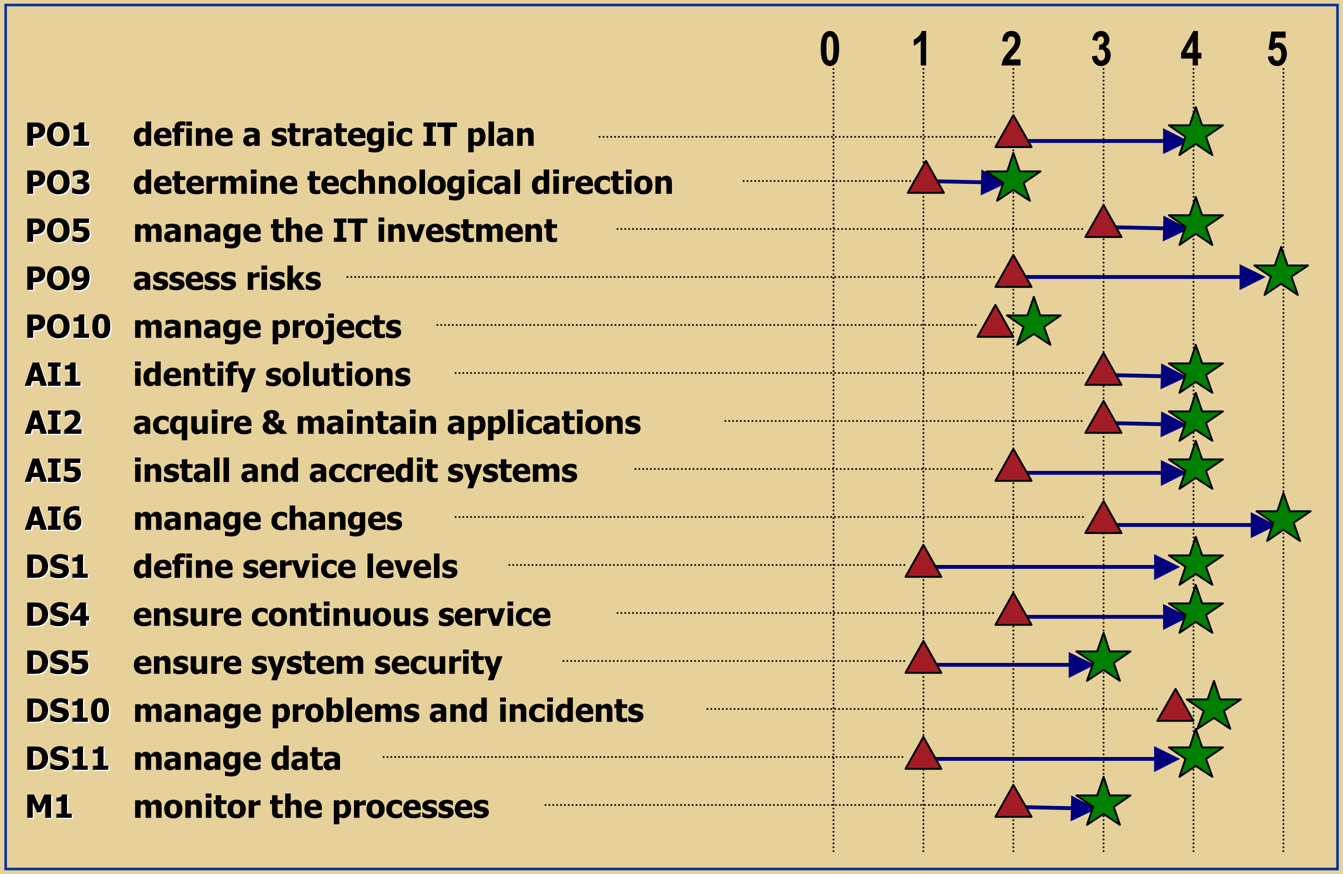
4 - Improvement driven
N- Not applicable
(Planning _Organisation)

1. Strategic Technology 0 1 2 3 4 N

1.1 Which way does senior management include Information Technology in the organisation's long- and short-range plans? ○●○○○○
0 = IT is not reflected in the organisation's long- and short term plans.
1 = IT is vaguely part of the organisation's long- and short term plans, but it is too general and not usable to help defining the IT strategy. .
2 = IT is part of the organisation's long- and short term plans. It contains IT objectives and action plans, and it can be used to help defining the IT strategy.
3 = 2+ IT issues as well as opportunities are adequately assessed and reflected.
4 = 3 + Feedback of IT and remarks in IT long- and short term plans proactively taken into consideration into the ST/LT business plans. IT has strong advocates with senior management.
N = Not Applicable

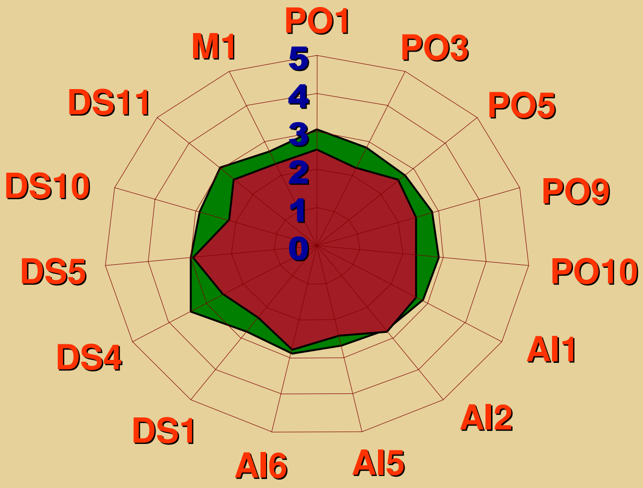
1.2 To what extent there is an Information Technology long-range plan? ○○●○○○
0 = There is no long-range IT plan.
1 = There is an informal long-range IT plan but it is not appropriately communicated.
2 = IT Management have developed an IT long-range plan describing the IT strategy based on the business strategy.

Maturity Gap Analysis

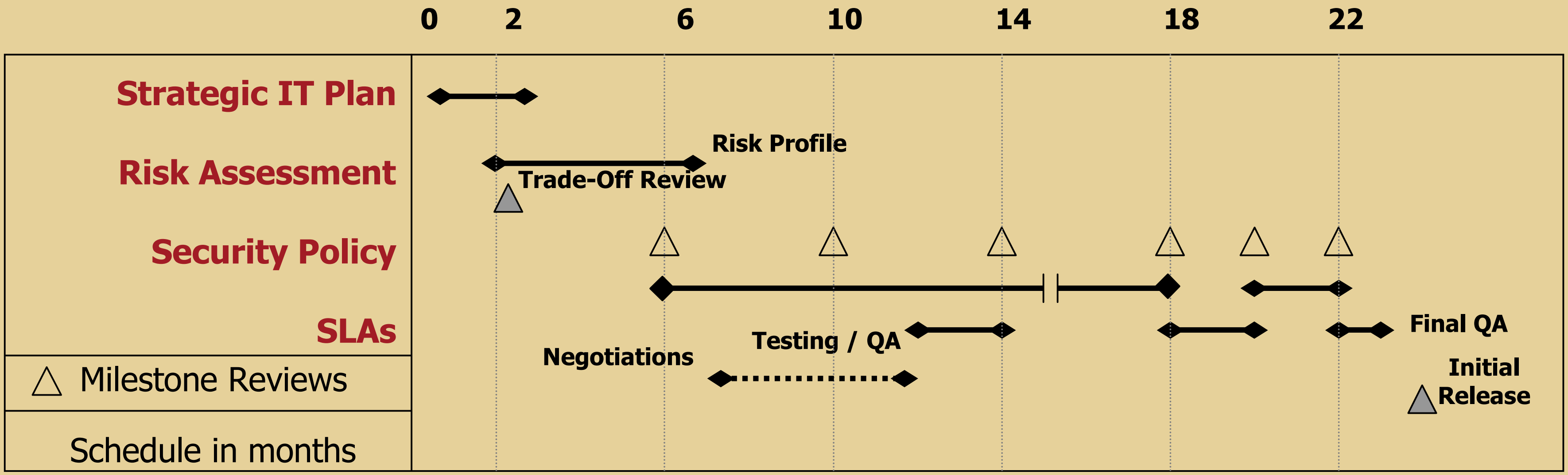


▲ As-Is

★ To-Be



Implementation Master Plan


Strategic IT Plan
Risk Assessment
Security Policy
SLAs
△ Milestone Reviews
Schedule in months
Risk Profile
Trade-Off Review
Negotiations
Testing / QA
Final QA
Initial Release