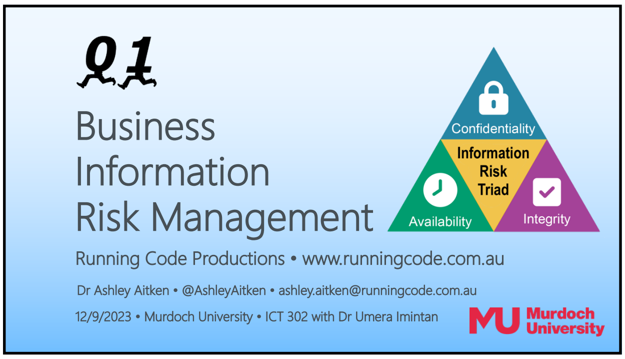


Business Information Risk Management

Confidentiality
Information Risk Triad
Availability
Integrity

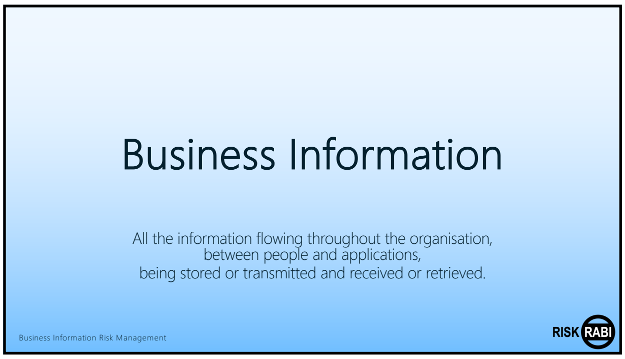
Running Code Productions • www.runningcode.com.au

Dr Ashley Aitken • @AshleyAitken • ashley.aitken@runningcode.com.au

12/9/2023 • Murdoch University • ICT 302 with Dr Umera Imintan

Murdoch University

1



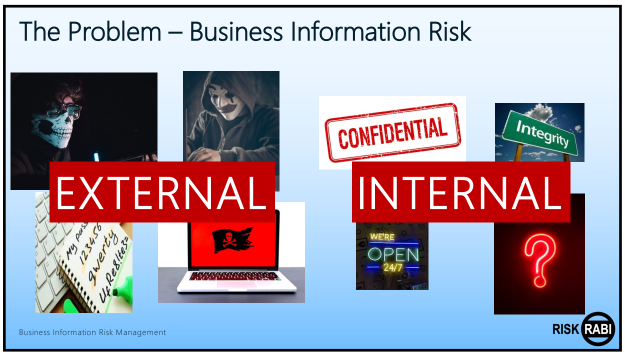
Business Information

All the information flowing throughout the organisation,
between people and applications,
being stored or transmitted and received or retrieved.

Business Information Risk Management

RISK RABI

2



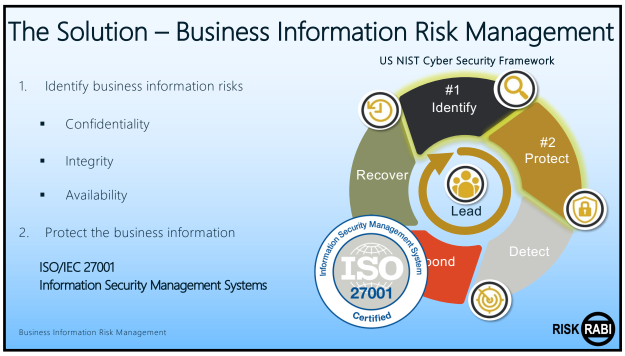
The Problem – Business Information Risk

EXTERNAL
INTERNAL
CONFIDENTIAL
Integrity
WE'RE OPEN 24/7

Business Information Risk Management

RISK RABI

3



The Solution – Business Information Risk Management

1. Identify business information risks
   - Confidentiality
   - Integrity
   - Availability
2. Protect the business information

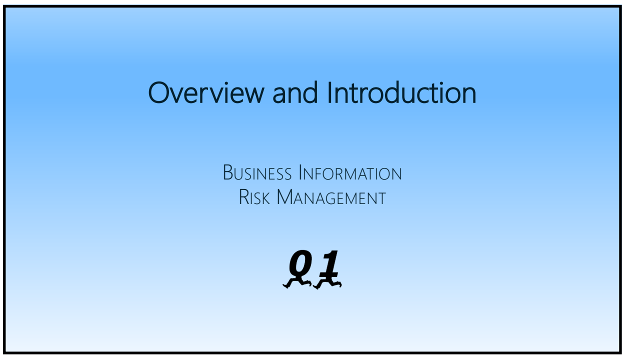
ISO/IEC 27001
Information Security Management Systems

US NIST Cyber Security Framework
#1 Identify
#2 Protect
Detect
pond
Recover
Lead
Information Security Management System
ISO 27001
Certified

Business Information Risk Management

RISK RABI

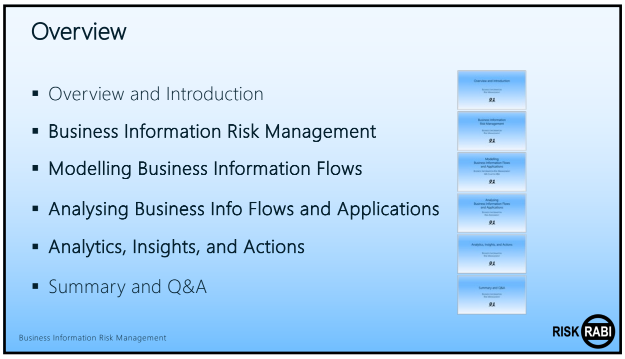
5



Overview and Introduction

Business Information
Risk Management

7



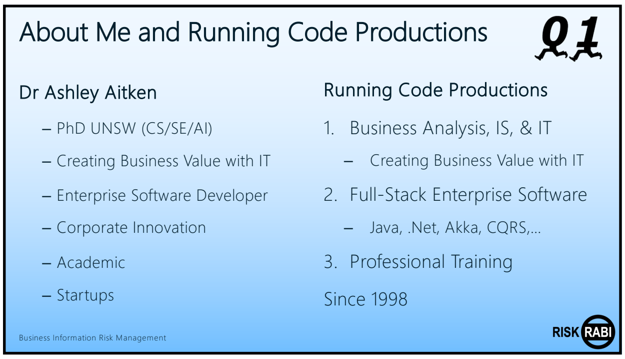
Overview

- Overview and Introduction
- Business Information Risk Management
- Modelling Business Information Flows
- Analysing Business Info Flows and Applications
- Analytics, Insights, and Actions
- Summary and Q&A

Business Information Risk Management

RISK RABI

8



About Me and Running Code Productions

Dr Ashley Aitken

- PhD UNSW (CS/SE/AI)
- Creating Business Value with IT
- Enterprise Software Developer
- Corporate Innovation
- Academic
- Startups

Running Code Productions

1. Business Analysis, IS, & IT
   - Creating Business Value with IT
2. Full-Stack Enterprise Software
   - Java, .Net, Akka, CQRS,…
3. Professional Training

Since 1998

Business Information Risk Management

RISK RABI

9

Thank You to Murdoch University

Murdoch
UNIVERSITY

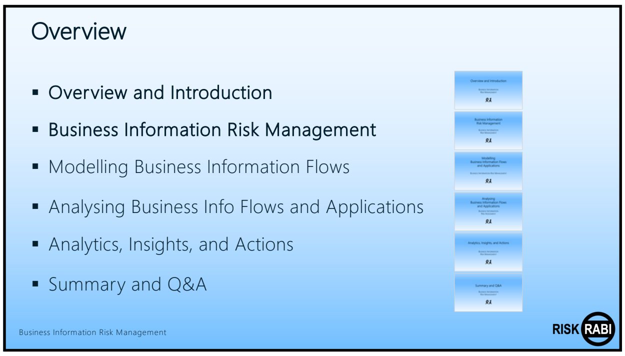
Business Information Risk Management

RISK RABI

10

Any Questions?

11



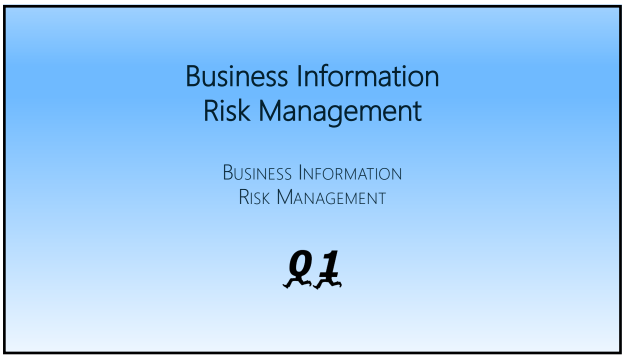
Overview

- Overview and Introduction
- Business Information Risk Management
- Modelling Business Information Flows
- Analysing Business Info Flows and Applications
- Analytics, Insights, and Actions
- Summary and Q&A

Business Information Risk Management

RISK RABI

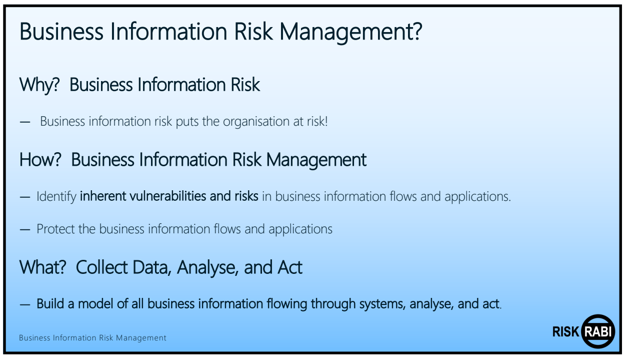
12



Business Information Risk Management

Business Information
Risk Management

13



Business Information Risk Management?

Why? Business Information Risk

- Business information risk puts the organisation at risk!

How? Business Information Risk Management

- Identify **inherent vulnerabilities and risks** in business information flows and applications.
- Protect the business information flows and applications

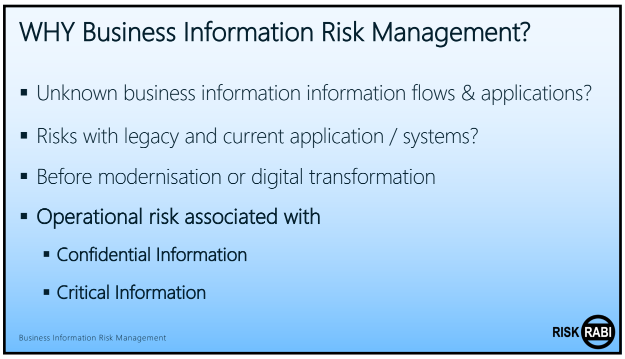
What? Collect Data, Analyse, and Act

- Build a model of all business information flowing through systems, analyse, and act.

Business Information Risk Management

RISK RABI

14



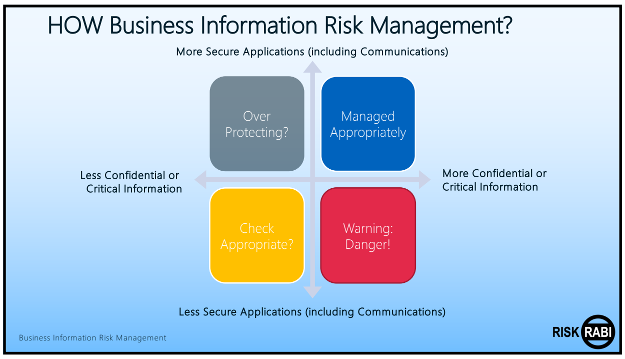
WHY Business Information Risk Management?

- Unknown business information information flows & applications?
- Risks with legacy and current application / systems?
- Before modernisation or digital transformation
- Operational risk associated with
  - Confidential Information
  - Critical Information

Business Information Risk Management

RISK RABI

15



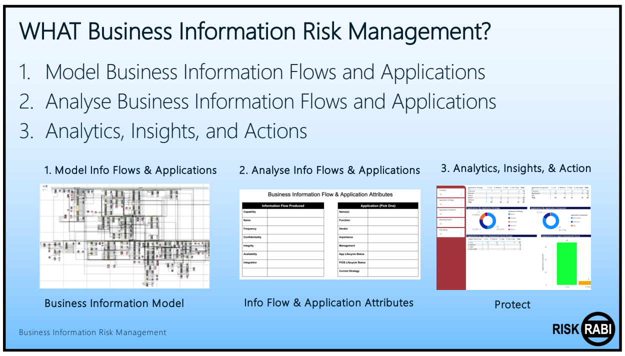
HOW Business Information Risk Management?

More Secure Applications (including Communications)
Over Protecting?
Managed Appropriately
Less Confidential or Critical Information
More Confidential or Critical Information
Check Appropriate?
Warning: Danger!
Less Secure Applications (including Communications)

Business Information Risk Management

RISK RABI

16



WHAT Business Information Risk Management?

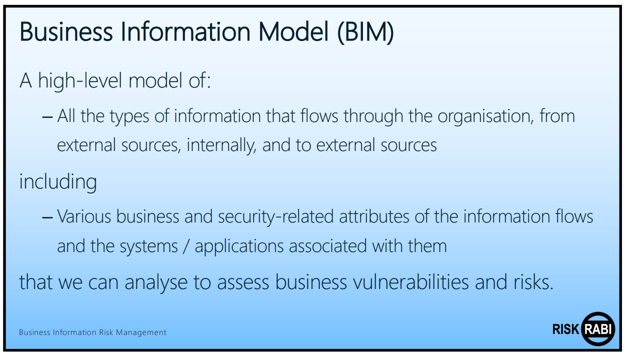
1. Model Business Information Flows and Applications
2. Analyse Business Information Flows and Applications
3. Analytics, Insights, and Actions

1. Model Info Flows & Applications
2. Analyse Info Flows & Applications
3. Analytics, Insights, & Action
Business Information Flow & Application Attributes
Business Information Model
Info Flow & Application Attributes
Protect

Business Information Risk Management

RISK RABI

17



Business Information Model (BIM)

A high-level model of:

– All the types of information that flows through the organisation, from external sources, internally, and to external sources

including

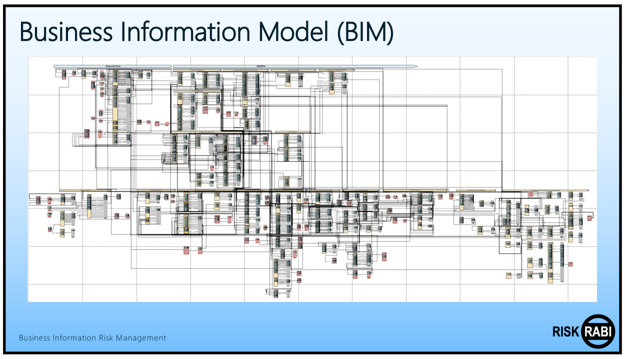
– Various business and security-related attributes of the information flows and the systems / applications associated with them

that we can analyse to assess business vulnerabilities and risks.

Business Information Model

RISK RABI

18

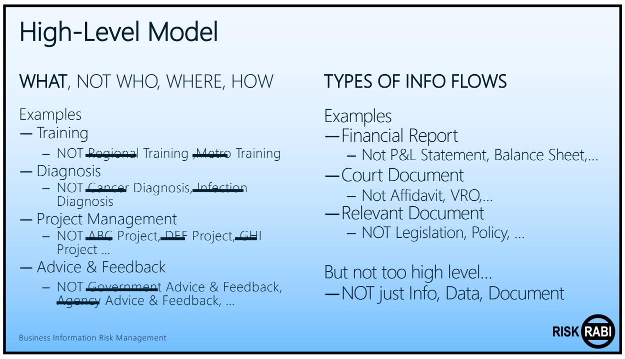


Business Information Model (BIM)

Business Information Risk Management

RISK RABI

19



High-Level Model

WHAT, NOT WHO, WHERE, HOW

Examples
- Training
  - NOT ~~Regional~~ Training ~~, Metro~~ Training
- Diagnosis
  - NOT ~~Cancer~~ Diagnosis~~, Infection~~ Diagnosis
- Project Management
  - NOT ~~ABC~~ Project~~, DEF~~ Project~~, GHI~~ Project ...
- Advice & Feedback
  - NOT ~~Government~~ Advice & Feedback, ~~Agency~~ Advice & Feedback, ...

TYPES OF INFO FLOWS

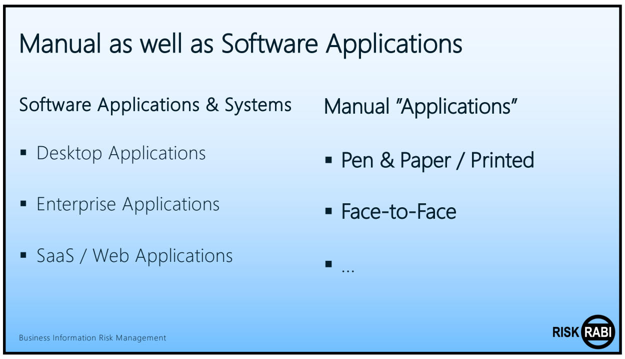
Examples
- Financial Report
  - Not P&L Statement, Balance Sheet,...
- Court Document
  - Not Affidavit, VRO,...
- Relevant Document
  - NOT Legislation, Policy, ...

But not too high level...
- NOT just Info, Data, Document

Business Information Risk Management

RISK RABI

20



Manual as well as Software Applications

Software Applications & Systems

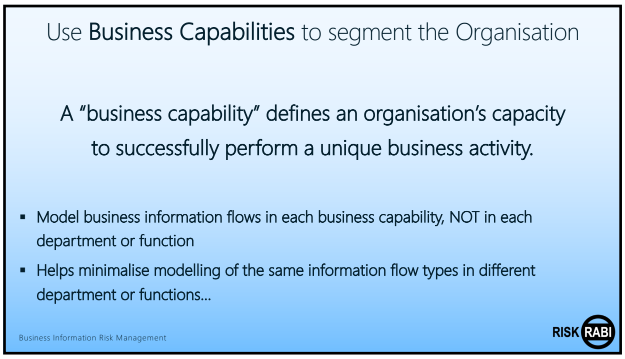
- Desktop Applications
- Enterprise Applications
- SaaS / Web Applications

Manual "Applications"

- Pen & Paper / Printed
- Face-to-Face
- …

Business Information Risk Management

21



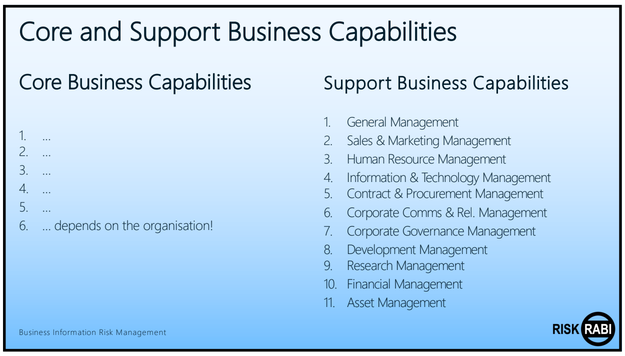
Use **Business Capabilities** to segment the Organisation

A "business capability" defines an organisation's capacity to successfully perform a unique business activity.

- Model business information flows in each business capability, NOT in each department or function
- Helps minimalise modelling of the same information flow types in different department or functions…

Business Information Risk Management

23



Core and Support Business Capabilities

Core Business Capabilities

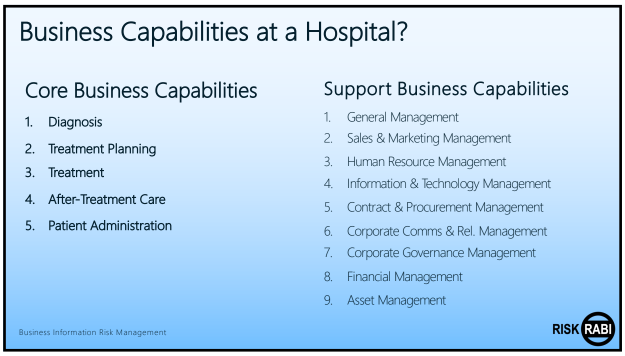
1. …
2. …
3. …
4. …
5. …
6. … depends on the organisation!

Support Business Capabilities

1. General Management
2. Sales & Marketing Management
3. Human Resource Management
4. Information & Technology Management
5. Contract & Procurement Management
6. Corporate Comms & Rel. Management
7. Corporate Governance Management
8. Development Management
9. Research Management
10. Financial Management
11. Asset Management

Business Information Risk Management

24



Business Capabilities at a Hospital?

Core Business Capabilities

1. Diagnosis
2. Treatment Planning
3. Treatment
4. After-Treatment Care
5. Patient Administration

Support Business Capabilities

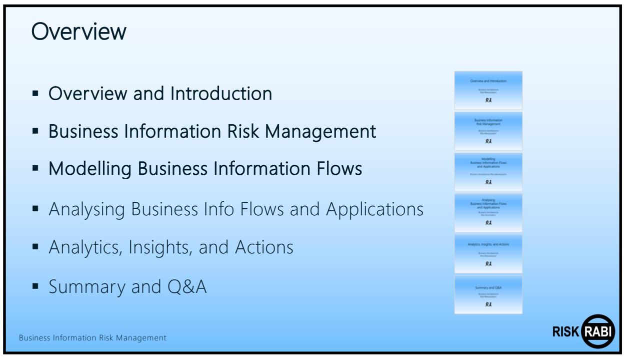
1. General Management
2. Sales & Marketing Management
3. Human Resource Management
4. Information & Technology Management
5. Contract & Procurement Management
6. Corporate Comms & Rel. Management
7. Corporate Governance Management
8. Financial Management
9. Asset Management

Business Information Risk Management

25

Any Questions?

27

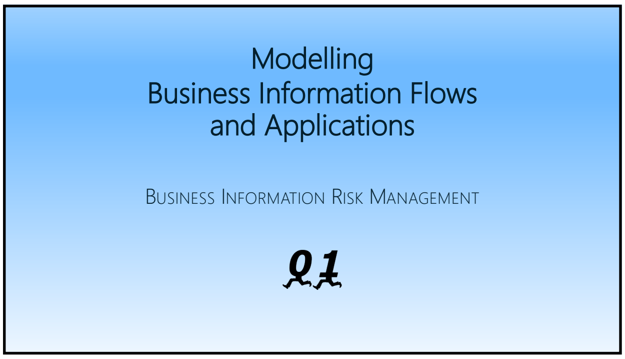


Overview

- Overview and Introduction
- Business Information Risk Management
- Modelling Business Information Flows
- Analysing Business Info Flows and Applications
- Analytics, Insights, and Actions
- Summary and Q&A

Business Information Risk Management

28

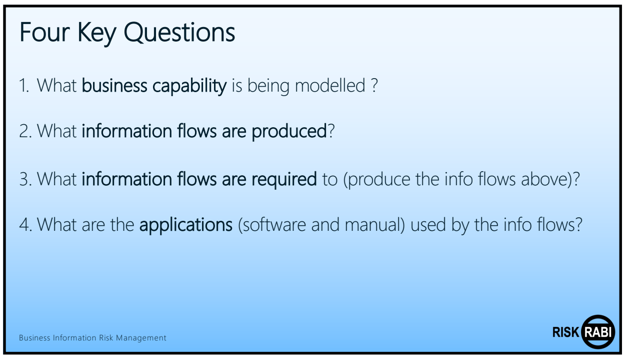


Modelling
Business Information Flows
and Applications

BUSINESS INFORMATION RISK MANAGEMENT

Q1

29



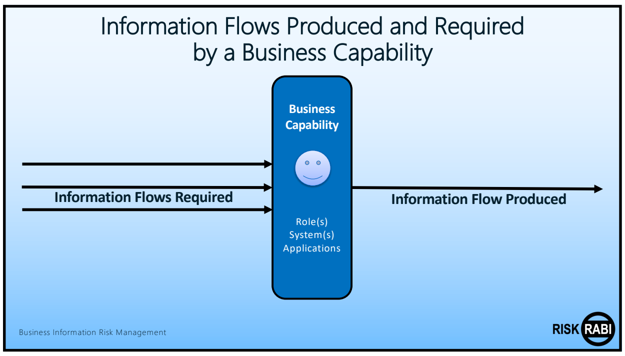
Four Key Questions

1. What **business capability** is being modelled ?
2. What **information flows are produced**?
3. What **information flows are required** to (produce the info flows above)?
4. What are the **applications** (software and manual) used by the info flows?

Business Information Risk Management

RISK RABI

30

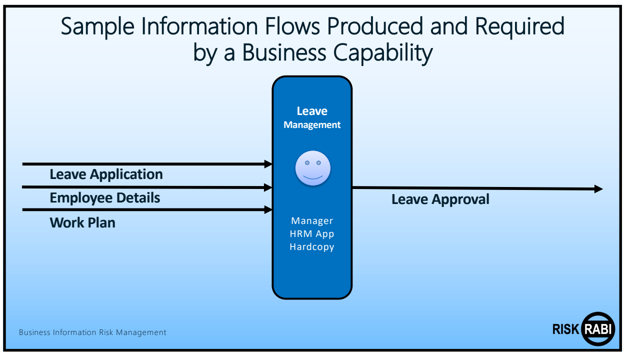


Information Flows Produced and Required
by a Business Capability

Business Information Risk Management

RISK RABI

31

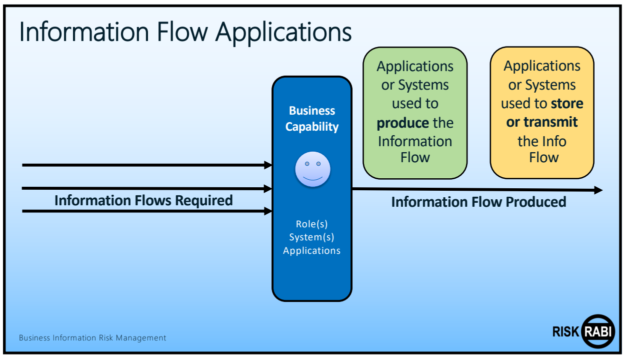


Sample Information Flows Produced and Required
by a Business Capability

Business Information Risk Management

RISK RABI

32



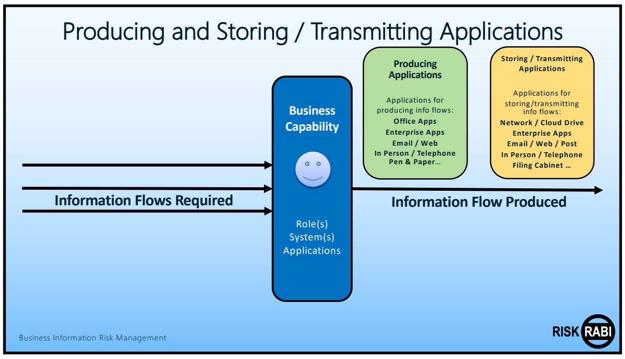
Information Flow Applications

Business Capability
Role(s)
System(s)
Applications
Applications or Systems used to **produce** the Information Flow
Applications or Systems used to **store or transmit** the Info Flow
Information Flows Required
Information Flow Produced

Business Information Risk Management

RISK RABI

33

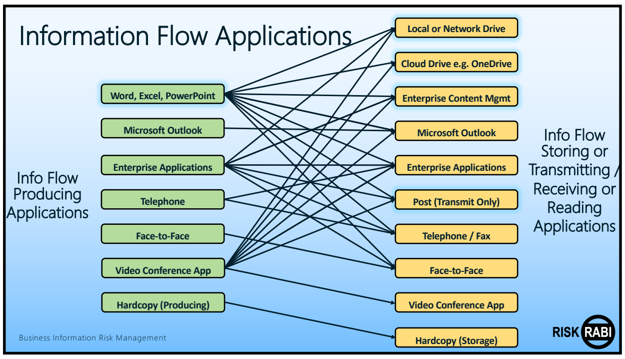


Producing and Storing / Transmitting Applications

Business Information Risk Management

RISK RABI

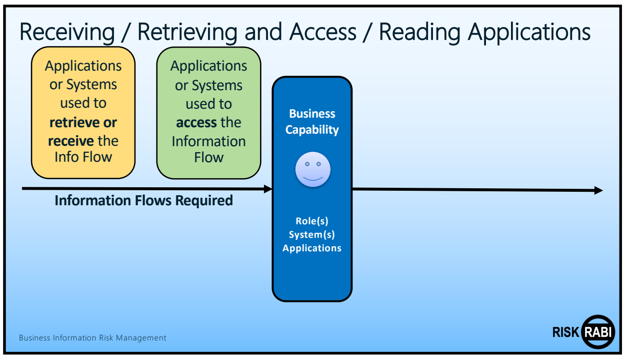
34



Information Flow Applications

Business Information Risk Management

35

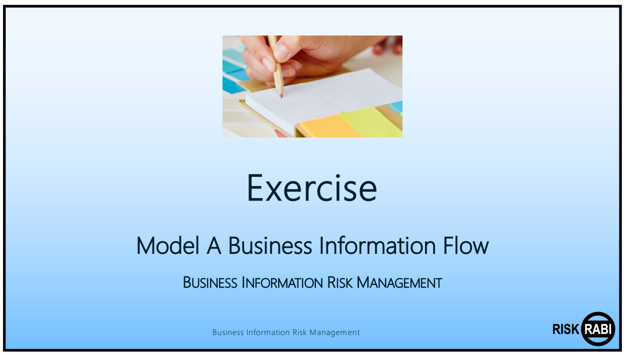


Receiving / Retrieving and Access / Reading Applications

Applications or Systems used to **retrieve or receive** the Info Flow
Applications or Systems used to **access** the Information Flow
Information Flows Required
Business Capability
Role(s)
System(s)
Applications

Business Information Risk Management

36



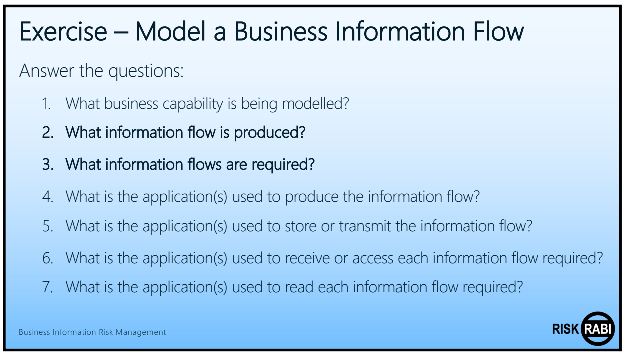
Exercise

Model A Business Information Flow

BUSINESS INFORMATION RISK MANAGEMENT

Business Information Risk Management

37



Exercise – Model a Business Information Flow

Answer the questions:

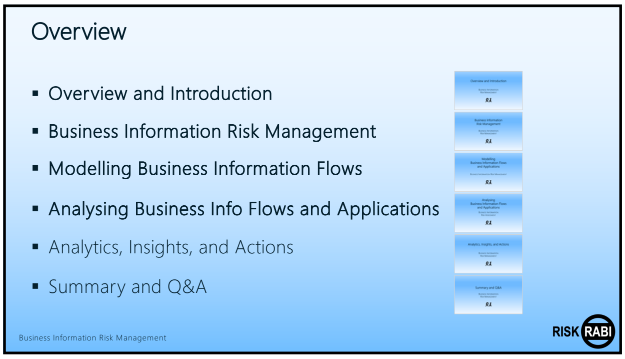
1. What business capability is being modelled?
2. What information flow is produced?
3. What information flows are required?
4. What is the application(s) used to produce the information flow?
5. What is the application(s) used to store or transmit the information flow?
6. What is the application(s) used to receive or access each information flow required?
7. What is the application(s) used to read each information flow required?

Business Information Risk Management

38

Any Questions?

39

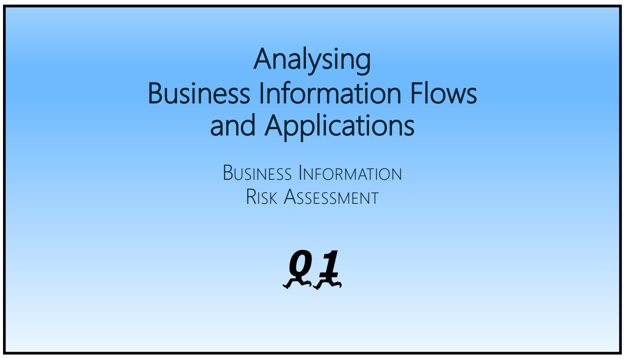


Overview

- Overview and Introduction
- Business Information Risk Management
- Modelling Business Information Flows
- Analysing Business Info Flows and Applications
- Analytics, Insights, and Actions
- Summary and Q&A

Business Information Risk Management

40

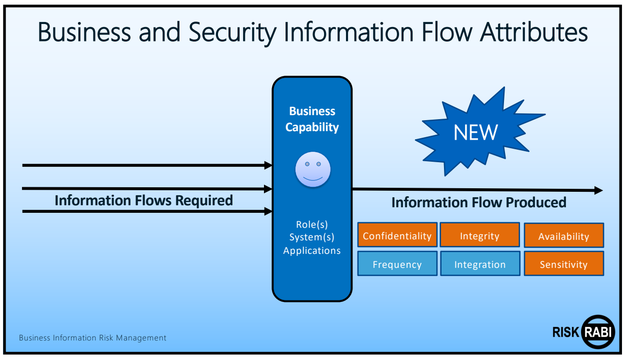


Analysing Business Information Flows and Applications

Business Information Risk Assessment

01

41

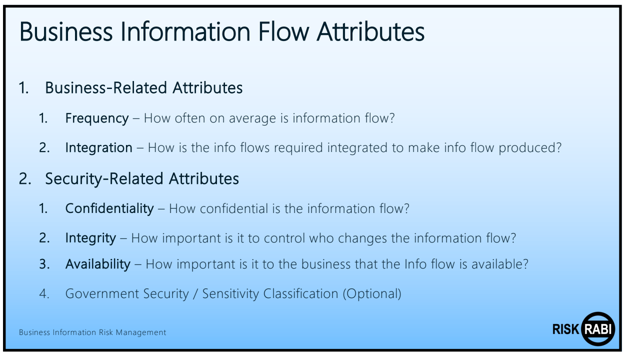


Business and Security Information Flow Attributes

Business Information Risk Management

RISK RABI

42



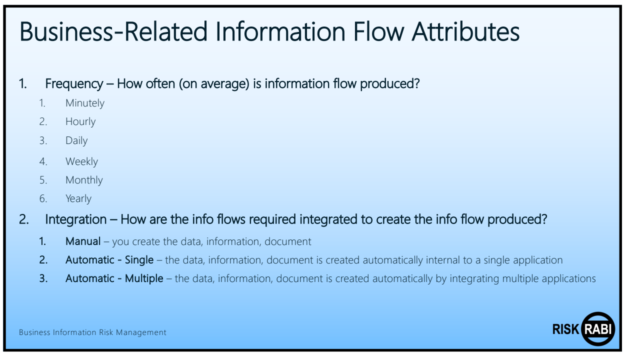
Business Information Flow Attributes

1. Business-Related Attributes
   1. **Frequency** – How often on average is information flow?
   2. **Integration** – How is the info flows required integrated to make info flow produced?
2. Security-Related Attributes
   1. **Confidentiality** – How confidential is the information flow?
   2. **Integrity** – How important is it to control who changes the information flow?
   3. **Availability** – How important is it to the business that the Info flow is available?
   4. Government Security / Sensitivity Classification (Optional)

Business Information Risk Management

RISK RABI

43



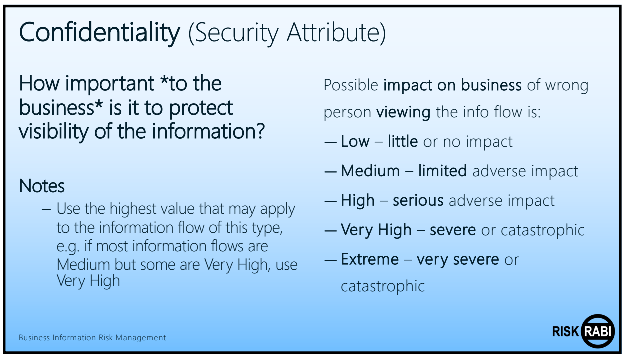
Business-Related Information Flow Attributes

1. Frequency – How often (on average) is information flow produced?
   1. Minutely
   2. Hourly
   3. Daily
   4. Weekly
   5. Monthly
   6. Yearly
2. Integration – How are the info flows required integrated to create the info flow produced?
   1. **Manual** – you create the data, information, document
   2. **Automatic - Single** – the data, information, document is created automatically internal to a single application
   3. **Automatic - Multiple** – the data, information, document is created automatically by integrating multiple applications

Business Information Risk Management

RISK RABI

44



Confidentiality (Security Attribute)

How important *to the business* is it to protect visibility of the information?

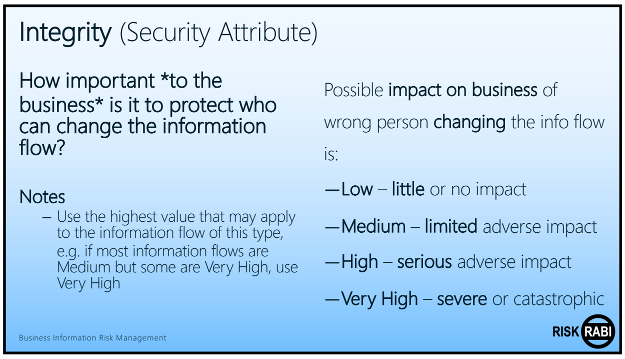
Notes
- Use the highest value that may apply to the information flow of this type, e.g. if most information flows are Medium but some are Very High, use Very High

Possible **impact on business** of wrong person **viewing** the info flow is:
- **Low** – **little** or no impact
- **Medium** – **limited** adverse impact
- **High** – **serious** adverse impact
- **Very High** – **severe** or catastrophic
- **Extreme** – **very severe** or catastrophic

Business Information Risk Management

RISK RABI

45



Integrity (Security Attribute)

How important *to the business* is it to protect who can change the information flow?

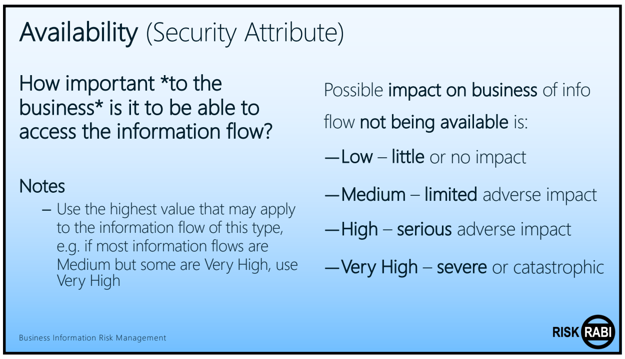
Notes
- Use the highest value that may apply to the information flow of this type, e.g. if most information flows are Medium but some are Very High, use Very High

Possible **impact on business** of wrong person **changing** the info flow is:
- **Low** – **little** or no impact
- **Medium** – **limited** adverse impact
- **High** – **serious** adverse impact
- **Very High** – **severe** or catastrophic

Business Information Risk Management

RISK RABI

46



Availability (Security Attribute)

How important *to the business* is it to be able to access the information flow?

Notes

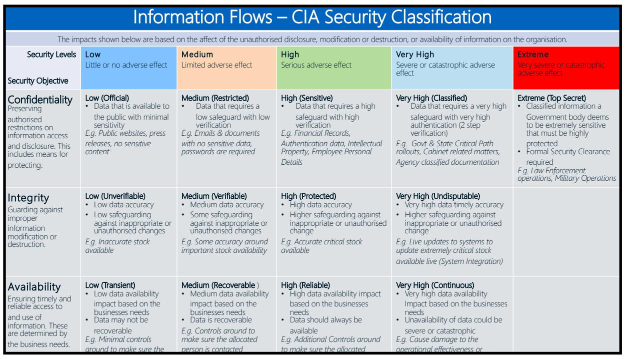
- Use the highest value that may apply to the information flow of this type, e.g. if most information flows are Medium but some are Very High, use Very High

Possible **impact on business** of info flow **not being available** is:

- **Low** – **little** or no impact
- **Medium** – **limited** adverse impact
- **High** – **serious** adverse impact
- **Very High** – **severe** or catastrophic

Business Information Risk Management

47

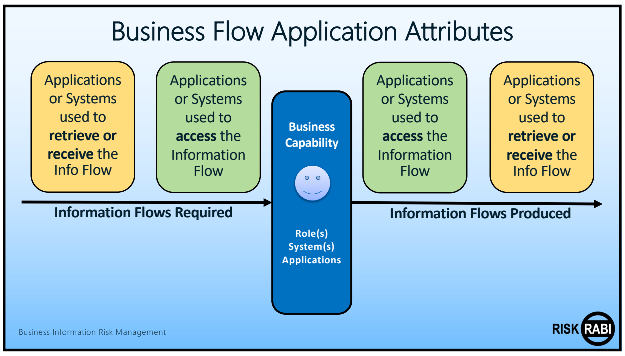


Information Flows – CIA Security Classification

The impacts shown below are based on the affect of the unauthorised disclosure, modification or destruction, or availability of information on the organisation.

Security Levels Security Objective	**Low** Little or no adverse effect	**Medium** Limited adverse effect	**High** Serious adverse effect	**Very High** Severe or catastrophic adverse effect	**Extreme** Very severe or catastrophic adverse effect
Confidentiality Preserving authorised restrictions on information access and disclosure. This includes means for protecting.	**Low (Official)** • Data that is available to the public with minimal sensitivity *E.g. Public websites, press releases, no sensitive content*	**Medium (Restricted)** • Data that requires a low safeguard with low verification *E.g. Emails & documents with no sensitive data, passwords are required*	**High (Sensitive)** • Data that requires a high safeguard with high verification *E.g. Financial Records, Authentication data, Intellectual Property, Employee Personal Details*	**Very High (Classified)** • Data that requires a very high safeguard with very high authentication (2 step verification) *E.g. Govt & State Critical Path rollouts, Cabinet related matters, Agency classified documentation*	**Extreme (Top Secret)** • Classified information a Government body deems to be extremely sensitive that must be highly protected • Formal Security Clearance required *E.g. Law Enforcement operations, Military Operations*
Integrity Guarding against improper information modification or destruction.	**Low (Unverifiable)** • Low data accuracy • Low safeguarding against inappropriate or unauthorised changes *E.g. Inaccurate stock available*	**Medium (Verifiable)** • Medium data accuracy • Some safeguarding against inappropriate or unauthorised changes *E.g. Some accuracy around important stock availability*	**High (Protected)** • High data accuracy • Higher safeguarding against inappropriate or unauthorised change *E.g. Accurate critical stock available*	**Very High (Undisputable)** • Very high data timely accuracy • Higher safeguarding against inappropriate or unauthorised change *E.g. Live updates to systems to update extremely critical stock available live (System Integration)*	
Availability Ensuring timely and reliable access to and use of information. These are determined by the business needs.	**Low (Transient)** • Low data availability impact based on the businesses needs • Data may not be recoverable *E.g. Minimal controls around to make sure the*	**Medium (Recoverable)** • Medium data availability impact based on the businesses needs • Data is recoverable *E.g. Controls around to make sure the allocated person is contacted*	**High (Reliable)** • High data availability impact based on the businesses needs • Data should always be available *E.g. Additional Controls around to make sure the allocated*	**Very High (Continuous)** • Very high data availability Impact based on the businesses needs • Unavailability of data could be severe or catastrophic *E.g. Cause damage to the operational effectiveness or*	

48



Business Flow Application Attributes

Applications or Systems used to **retrieve or receive** the Info Flow

Applications or Systems used to **access** the Information Flow

Business Capability

Role(s)
System(s)
Applications

Applications or Systems used to **access** the Information Flow

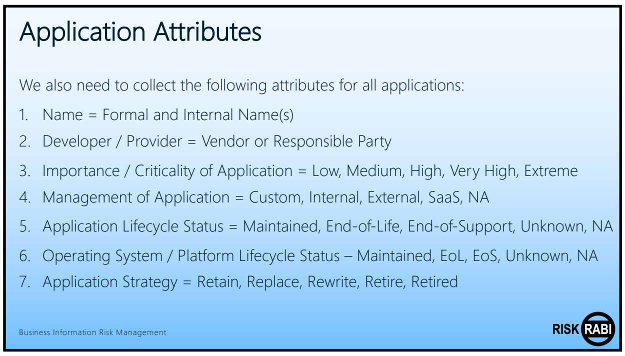
Applications or Systems used to **retrieve or receive** the Info Flow

Information Flows Required

Information Flows Produced

Business Information Risk Management

49



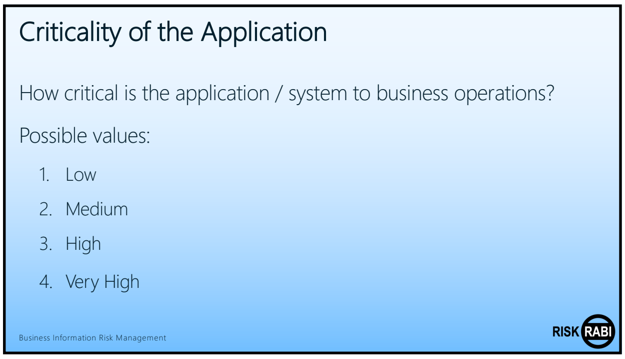
Application Attributes

We also need to collect the following attributes for all applications:

1. Name = Formal and Internal Name(s)
2. Developer / Provider = Vendor or Responsible Party
3. Importance / Criticality of Application = Low, Medium, High, Very High, Extreme
4. Management of Application = Custom, Internal, External, SaaS, NA
5. Application Lifecycle Status = Maintained, End-of-Life, End-of-Support, Unknown, NA
6. Operating System / Platform Lifecycle Status – Maintained, EoL, EoS, Unknown, NA
7. Application Strategy = Retain, Replace, Rewrite, Retire, Retired

Business Information Risk Management

50



Criticality of the Application

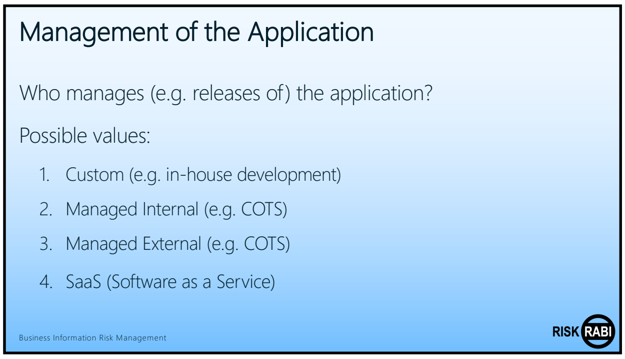
How critical is the application / system to business operations?

Possible values:

1. Low
2. Medium
3. High
4. Very High

Business Information Risk Management

51



Management of the Application

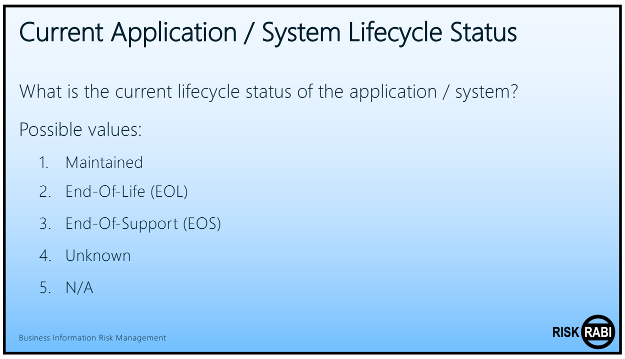
Who manages (e.g. releases of) the application?

Possible values:

1. Custom (e.g. in-house development)
2. Managed Internal (e.g. COTS)
3. Managed External (e.g. COTS)
4. SaaS (Software as a Service)

Business Information Risk Management

52



Current Application / System Lifecycle Status

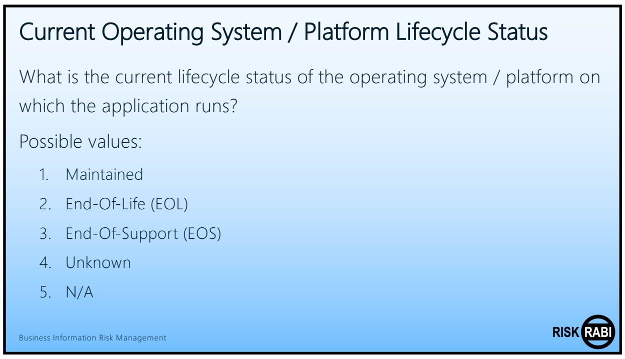
What is the current lifecycle status of the application / system?

Possible values:

1. Maintained
2. End-Of-Life (EOL)
3. End-Of-Support (EOS)
4. Unknown
5. N/A

Business Information Risk Management

53



Current Operating System / Platform Lifecycle Status

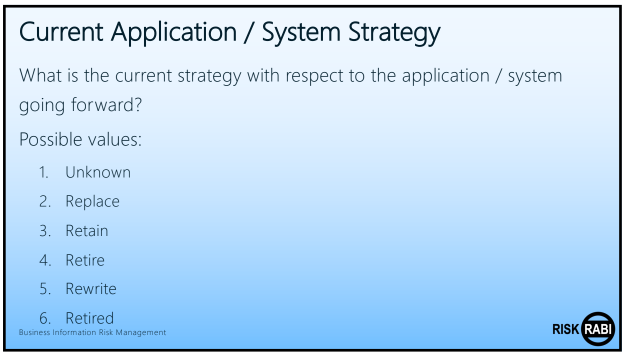
What is the current lifecycle status of the operating system / platform on which the application runs?

Possible values:

1. Maintained
2. End-Of-Life (EOL)
3. End-Of-Support (EOS)
4. Unknown
5. N/A

Business Information Risk Management

54



Current Application / System Strategy

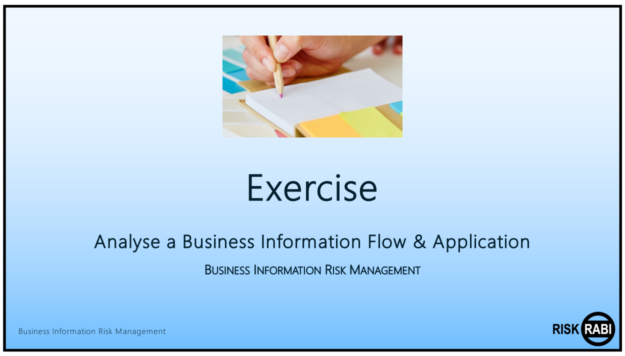
What is the current strategy with respect to the application / system going forward?

Possible values:

1. Unknown
2. Replace
3. Retain
4. Retire
5. Rewrite
6. Retired

Business Information Risk Management

55



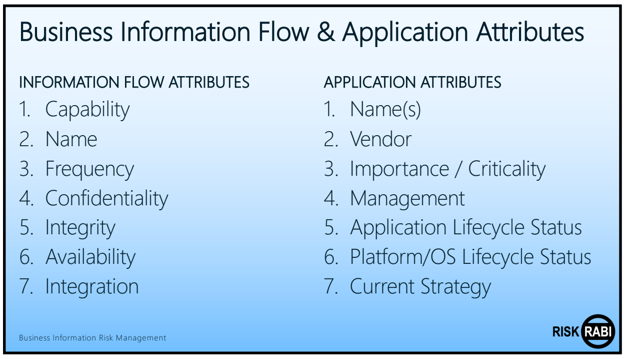
Exercise

Analyse a Business Information Flow & Application

BUSINESS INFORMATION RISK MANAGEMENT

Business Information Risk Management

56



Business Information Flow & Application Attributes

INFORMATION FLOW ATTRIBUTES

1. Capability
2. Name
3. Frequency
4. Confidentiality
5. Integrity
6. Availability
7. Integration

APPLICATION ATTRIBUTES

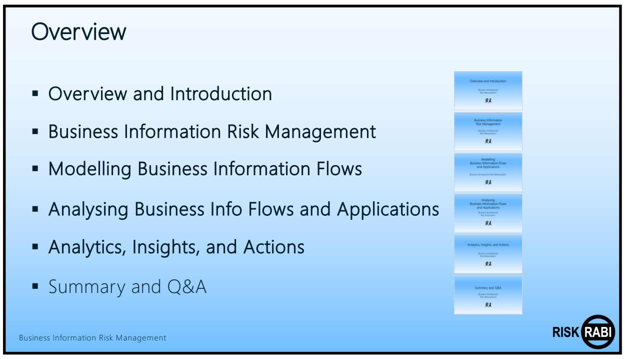
1. Name(s)
2. Vendor
3. Importance / Criticality
4. Management
5. Application Lifecycle Status
6. Platform/OS Lifecycle Status
7. Current Strategy

Business Information Risk Management

57

Any Questions?

58

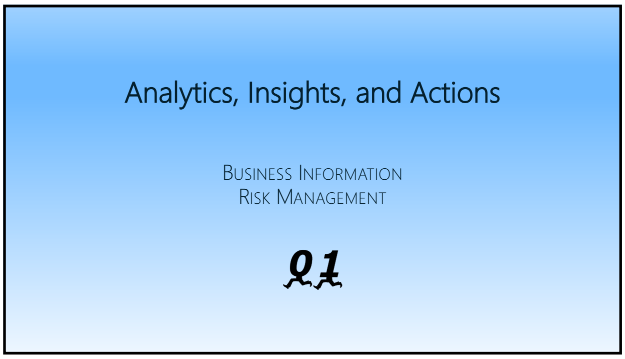


Overview

- Overview and Introduction
- Business Information Risk Management
- Modelling Business Information Flows
- Analysing Business Info Flows and Applications
- Analytics, Insights, and Actions
- Summary and Q&A

Business Information Risk Management

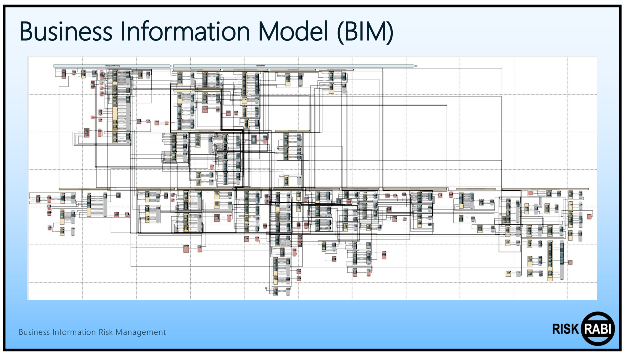
59



Analytics, Insights, and Actions

BUSINESS INFORMATION
RISK MANAGEMENT

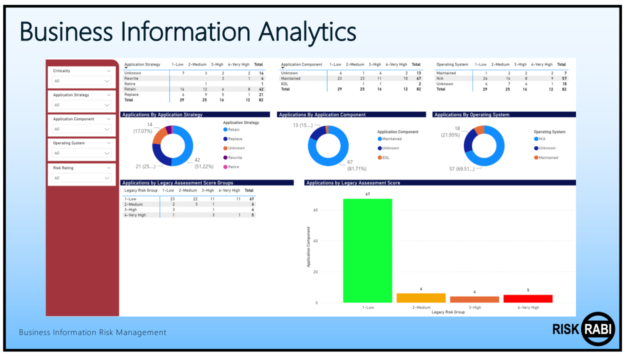
60



Business Information Model (BIM)

Business Information Risk Management

61



Business Information Analytics

Application Strategy	1-Low	2-Medium	3-High	4-Very High	Total
Unknown	7	3	2	2	14
Rewrite			3	1	4
Retire		1			1
Retain	16	12	6	8	42
Replace	6	9	5	1	21
Total	29	25	16	12	82

Application Component	1-Low	2-Medium	3-High	4-Very High	Total
Unknown	6	1	4	2	13
Maintained	23	23	11	10	67
EOL		1	1		2
Total	29	25	16	12	82

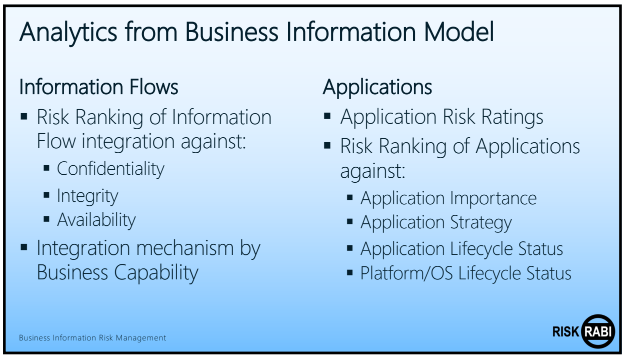
Operating System	1-Low	2-Medium	3-High	4-Very High	Total
Maintained	1	2	2	2	7
N/A	24	16	8	9	57
Unknown	4	7	6	1	18
Total	29	25	16	12	82

Applications by Legacy Assessment Score Groups

Legacy Risk Group	1-Low	2-Medium	3-High	4-Very High	Total
1-Low	23	22	11	11	67
2-Medium	2	3	1		6
3-High	3		1		4
4-Very High	1		3	1	5

Business Information Risk Management

62



Analytics from Business Information Model

Information Flows

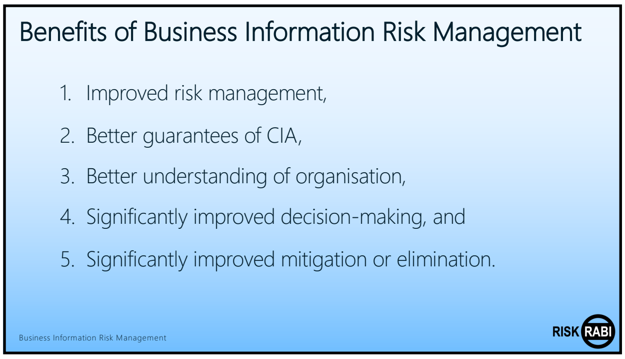
- Risk Ranking of Information Flow integration against:
  - Confidentiality
  - Integrity
  - Availability
- Integration mechanism by Business Capability

Applications

- Application Risk Ratings
- Risk Ranking of Applications against:
  - Application Importance
  - Application Strategy
  - Application Lifecycle Status
  - Platform/OS Lifecycle Status

Business Information Risk Management

63

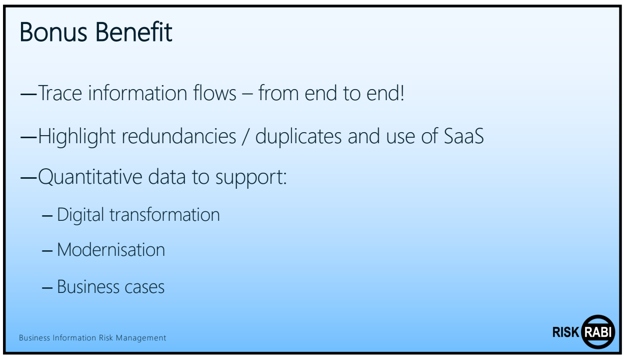


Benefits of Business Information Risk Management

1. Improved risk management,
2. Better guarantees of CIA,
3. Better understanding of organisation,
4. Significantly improved decision-making, and
5. Significantly improved mitigation or elimination.

Business Information Risk Management

64



Bonus Benefit

- Trace information flows – from end to end!
- Highlight redundancies / duplicates and use of SaaS
- Quantitative data to support:
  - Digital transformation
  - Modernisation
  - Business cases

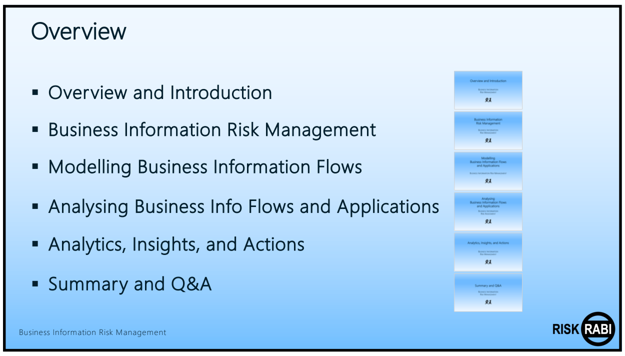
Business Information Risk Management

RISK RABI

65

Any Questions?

66



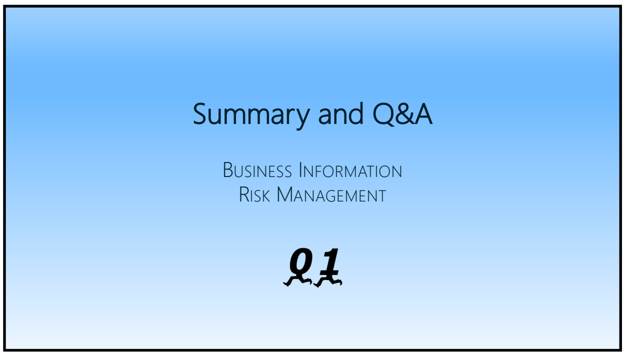
Overview

- Overview and Introduction
- Business Information Risk Management
- Modelling Business Information Flows
- Analysing Business Info Flows and Applications
- Analytics, Insights, and Actions
- Summary and Q&A

Business Information Risk Management

RISK RABI

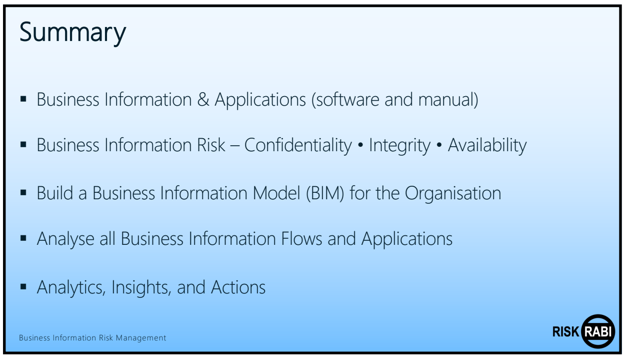
67



Summary and Q&A

BUSINESS INFORMATION
RISK MANAGEMENT

68



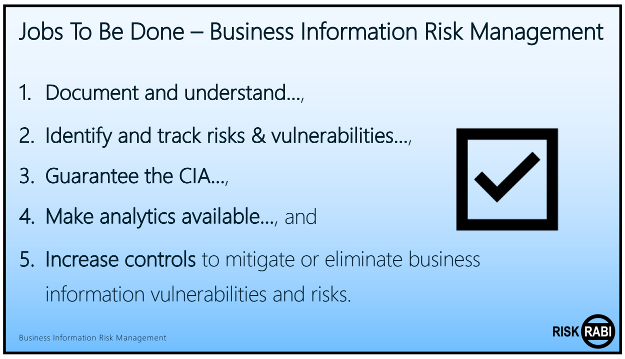
Summary

- Business Information & Applications (software and manual)
- Business Information Risk – Confidentiality • Integrity • Availability
- Build a Business Information Model (BIM) for the Organisation
- Analyse all Business Information Flows and Applications
- Analytics, Insights, and Actions

Business Information Risk Management

RISK RABI

69



Jobs To Be Done – Business Information Risk Management

1. Document and understand…,
2. Identify and track risks & vulnerabilities…,
3. Guarantee the CIA…,
4. Make analytics available…, and
5. Increase controls to mitigate or eliminate business information vulnerabilities and risks.

Business Information Risk Management

RISK RABI

70

Any Questions?

71

Thank You

Please complete the short survey... http://bit.ly/birmsurvey

Running Code Productions • www.runningcode.com.au

Dr Ashley Aitken • @AshleyAitken • ashley.aitken@runningcode.com.au

https://www.riskrabi.com

RISK RABI

72