Citicus ONE:
Background information

Citicus Limited
www.citicus.com

Introduction

Citicus™ ONE is a customisable, web-based application system which enables you to:

- reliably measure the risk posed by your enterprise's mission-critical information systems in meaningful, business-oriented terms
- manage information risk across your enterprise efficiently.

These slides provide useful supporting information. Specifically, they:

- Explain what 'information risk' means and how it relates to other areas of risk
- Reveal key statistics that underpin **Citicus ONE**
- Present the theory of control embodied by **Citicus ONE**
- Explain key terms (information incidents, controls, information resources)
- Show how information risk relates to other areas of risk
- Provide background information about the FIRM methodology which is applied by **Citicus ONE** and explain the relationship between Citicus and the Information Security Forum

Other presentations in the same series explain:

- what **Citicus ONE** can do for your organisation
- **Citicus ONE**'s technology, deployment options, pricing, capabilities and supporting services

*Years of research and practical experience has made **Citicus ONE** the world's most advanced tool for measuring and managing information risk successfully.*

'Information risk' is the chance or possibility of harm being caused to a organization as a result of a loss of the confidentiality, integrity or availability of information

citicusone

What is 'information risk' exactly?

Probability of suffering harm

Nature and level of harm

Information risk is the **chance or possibility** of **harm** being caused to a business as a result of a loss of the **confidentiality, integrity or availability** of **information**

The 3 key properties of information to be protected

Exists in varying forms:

- held in people's heads
- communicated face-to-face
- recorded in deeds and other securities
- entered into, stored, processed, transmitted and presented via IT

*The **method** of protection depends on the **form** taken by information*

***Citicus ONE** focuses on managing the risk posed by **IT-based information** since that is the largest and fastest growing segment of the problem in most organizations.*

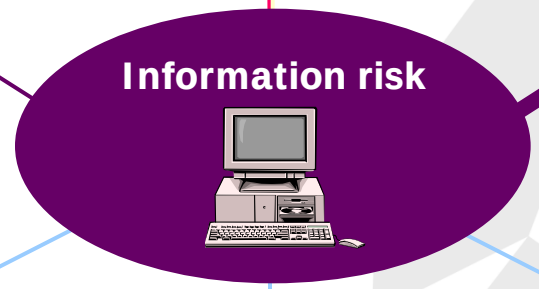
citicusone

How information risk influences other business risks

Market risk
(ie factors beyond the control of management such as interest and currency rates)

Financial risk
(eg uncertainties about projected earnings or expenditure)

Operational risk
(eg **information risk**, theft, fraud, loss of facilities or key employees).



Information risk intensifies all other business risks

Information risk is an increasingly important component of operational risk

- *Borrowings and investment positions*
- *Projected rates of interest*
- *Projected cash flows*
- *External developments*

- *Sales forecasts*
- *Forecast expenditure*
- *Actual sales and expenditure*
- *Key variances*

- *Information risk status reports*
- *Identity of key assets (equipment, facilities and employees)*
- *Status of continuity arrangements*

Sound information is needed to manage each category of risk. Thus, managing information risk well is essential.

citicusone

Key statistics: The harm caused by information incidents can be substantial

A sample of 253 worst-case incidents reduced the value of the businesses concerned by $1.4 million, on average. Impact of identified incidents included:

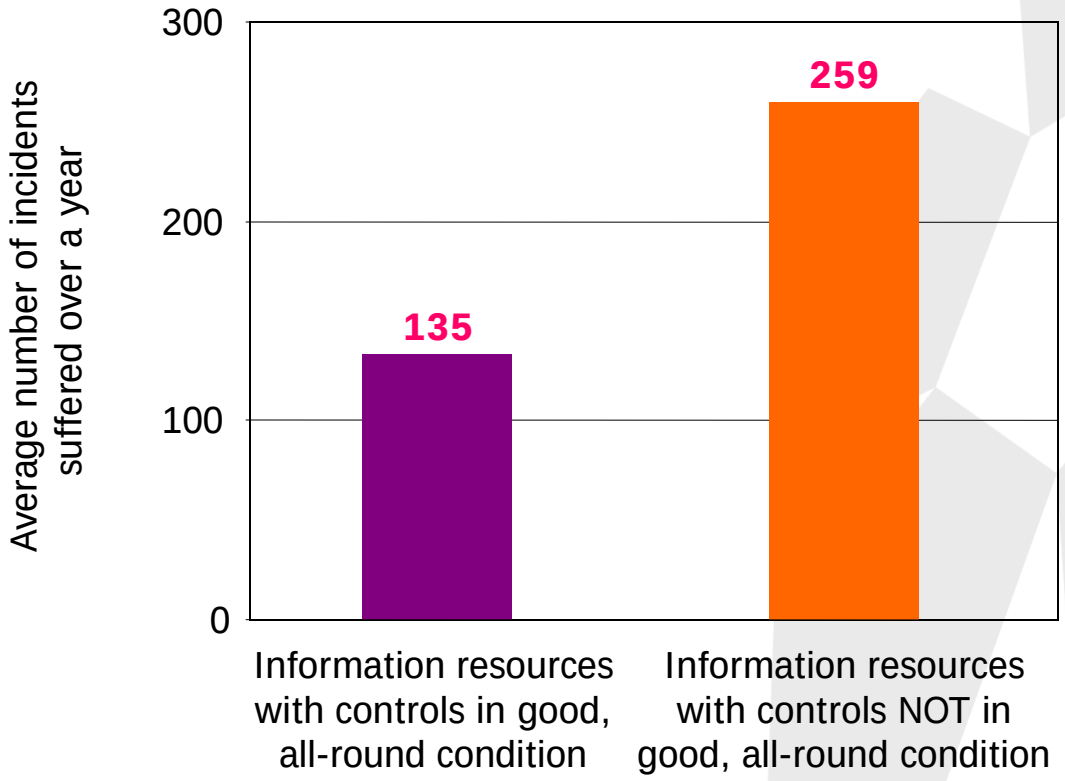
- £200 million of sales lost
- $105 million could not be recovered
- 5,000 customer queries unanswered
- 20,000 emails permanently lost
- $400,000 stolen
- confidential data belonging to key business partners destroyed
- 40 fraudulent fund transfers from client accounts
- 3,100 wrong entries on customer accounts
- $5.25 million of IT equipment destroyed and business data unavailable for 4 weeks
- 4,000 staff disrupted

Details of major incidents extracted from *It could happen to you: a profile of major incidents*; Information Security Forum, 2000 and analysis of 253 worst-case incidents published in ***Driving information risk out of the business***; Information Security Forum, 1999.

citicusone

Key statistics: Good controls drive down the **volume** of incidents

The average number of information incidents[1] suffered a year by an information resource[2] is halved when controls[3] are in 'good, all-round condition'

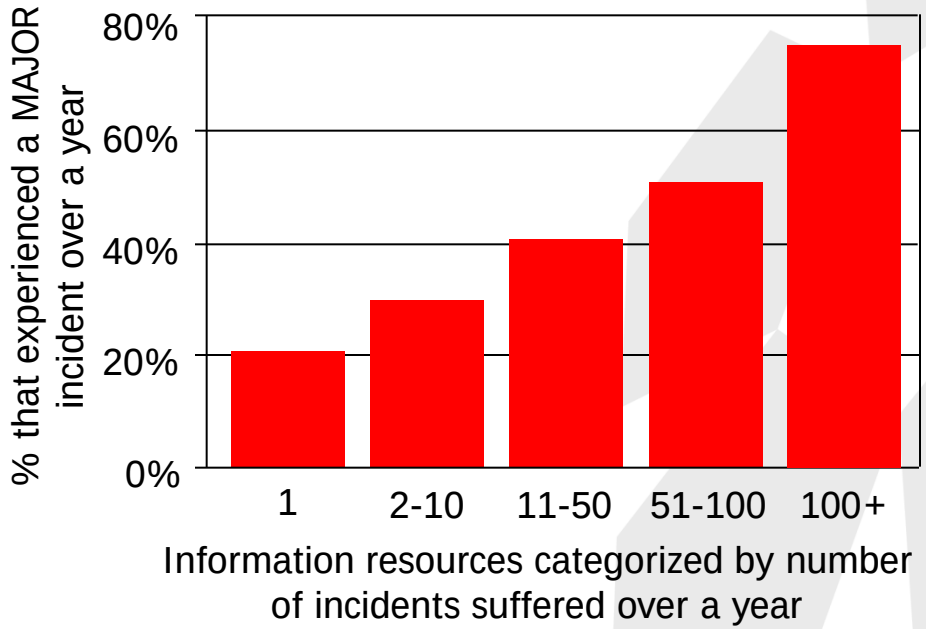


Citicus analysis of some 210,000 incidents affecting 844 information resources covered by the Information Security Forum's 2000-2002 Security Status Survey.

[1, 2, 3] For definitions of these key terms, see the slide entitled ***Other key terms***

Key statistics: Why reducing the **volume** of information incidents is important

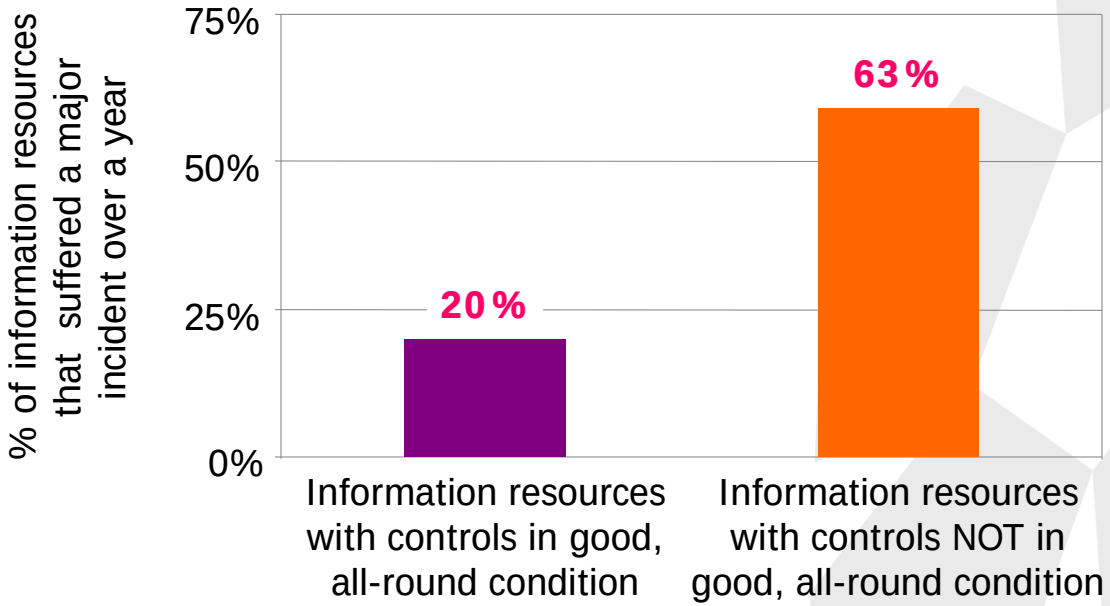
Eliminating minor information incidents is important, since the chance of suffering a MAJOR incident climbs as the number of minor incidents increases



Citicus analysis of incidents affecting 844 information resources covered by the Information Security Forum's 2000-2002 Security Status Survey.

Key statistics: Good controls slash the odds of suffering **major** incidents

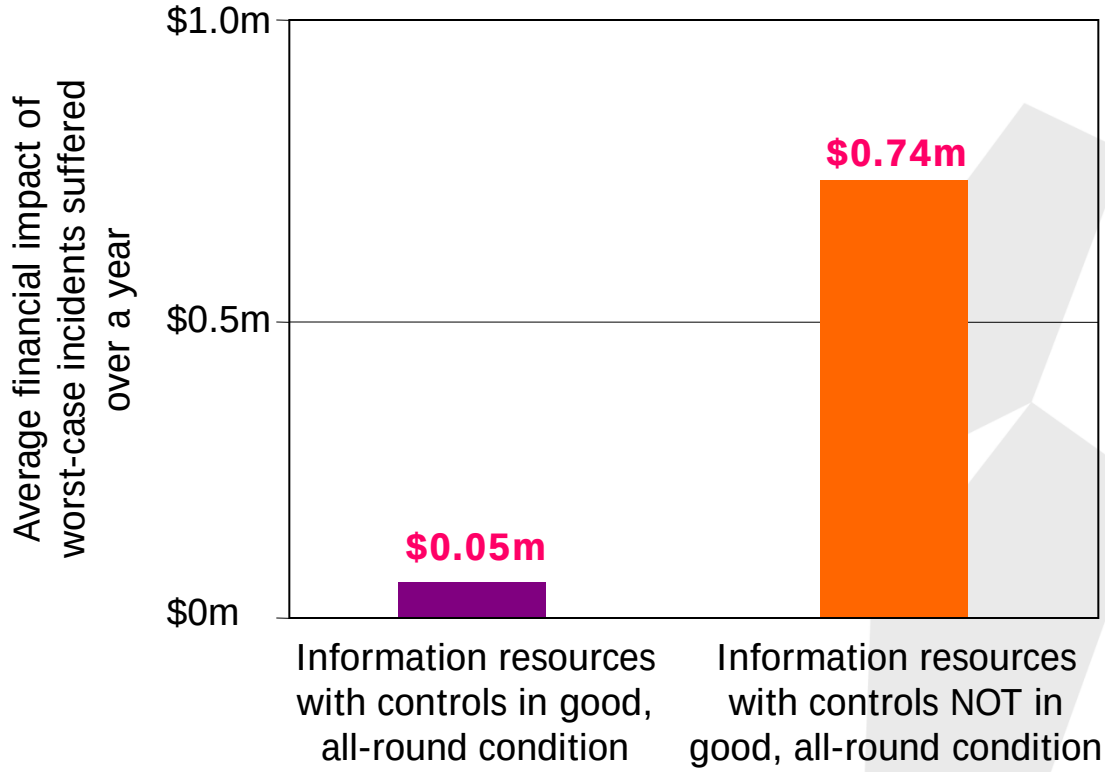
Controls that are in 'good, all-round condition' reduce the probability of experiencing MAJOR incidents by more than a factor of three



Analysis of incidents affecting 663 information resources covered by the Information Security Forum's 2000-2002 Security Status Survey.

Key statistics: Good controls lead to big savings

*Controls that are in 'good, all-round condition' also dramatically reduce the **financial impact** of worst-case incidents*

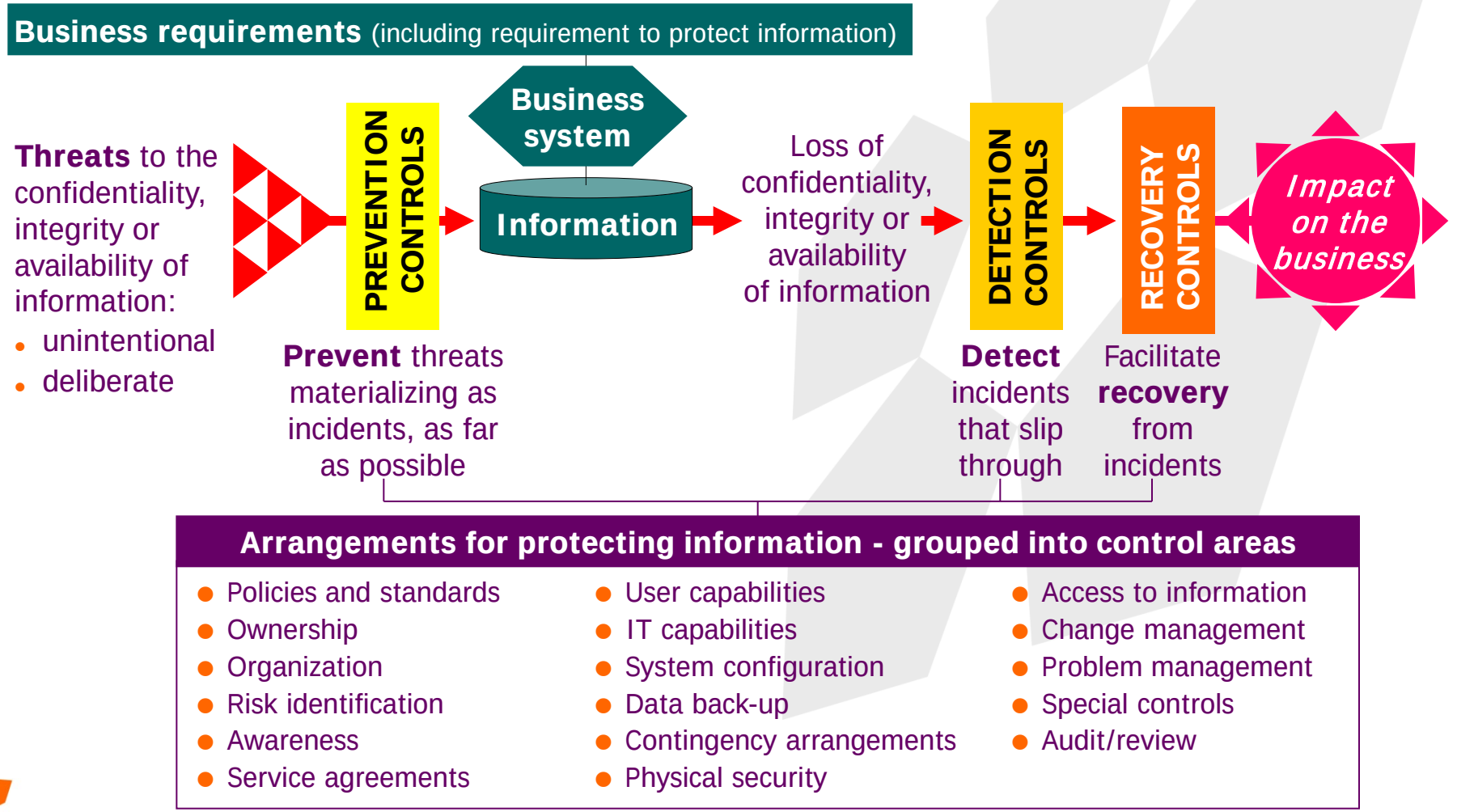


Analysis of 244 worst-case incidents for which financial data was provided covered by the Information Security Forum's 2000-2002 Security Status Survey

Together, these statistics shown that information risk can be slashed by ensuring controls comply with generally-accepted good practice

Citicus ONE implements a coherent theory of control for information risk

Citicus ONE promotes achievement of a balanced system of controls. This is the key to success in keeping information risk at an acceptable level



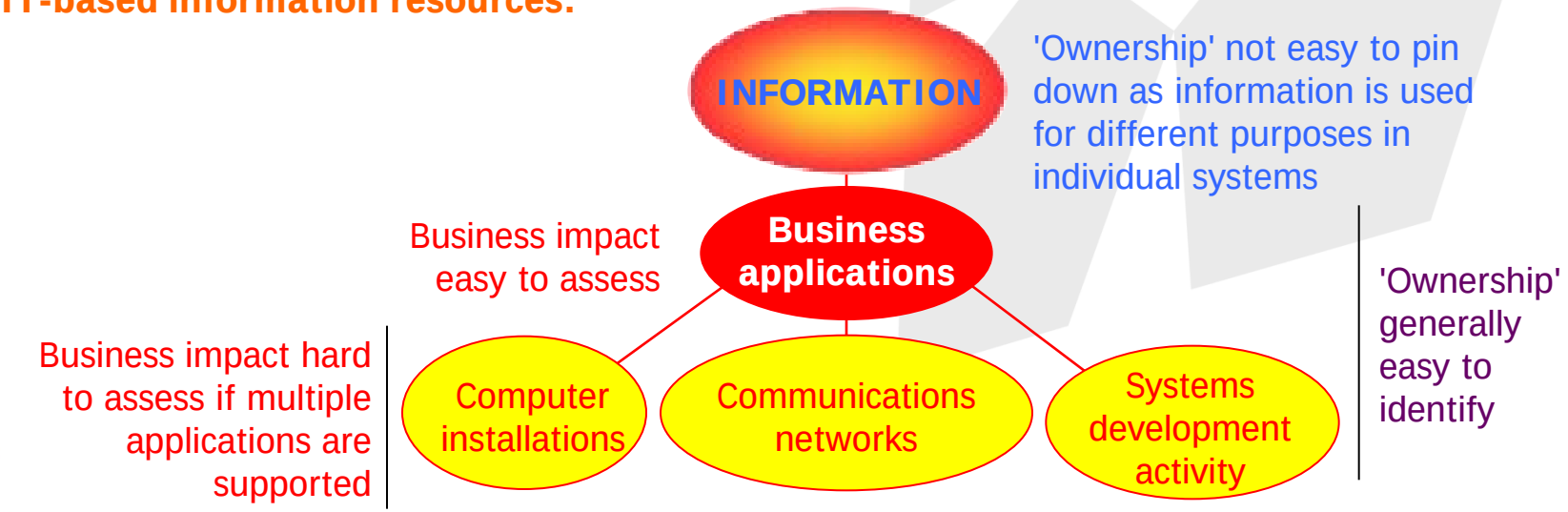
Definitions of other key terms

Information incidents: events (or chains of events) that compromise the confidentiality, integrity or availability of information eg:

- malfunction of software or hardware
- loss of services, equipment or facilities
- overload
- human error
- unforeseen effects of change
- other undesirable acts.

Controls: policies, methods, procedures, devices or programmed mechanisms designed to protect the confidentiality, integrity and availability of information (eg user capabilities, data back-up), or that otherwise influence the level of protection provided (eg training and supervision of IT staff).

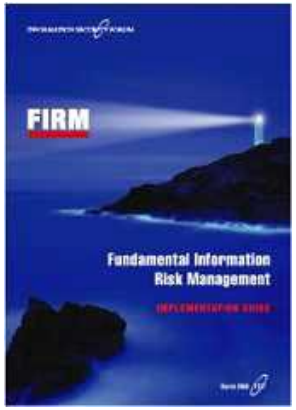
IT-based information resources:



Citicus ONE implements **FIRM** – a ground-breaking risk methodology

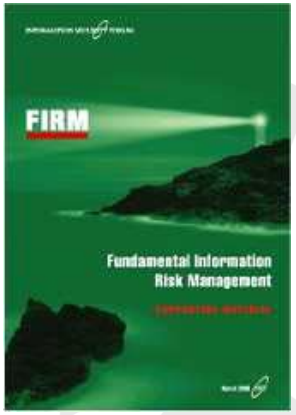
FIRM is a ground-breaking methodology for managing information risk across an enterprise published by the Information Security Forum (ISF):

FIRM IMPLEMENTATION GUIDE (86 pages)



- Problem definition (why information risk management processes often fail)
- The key challenges
- **FIRM** methodology
- Implementation process

SUPPORTING MATERIAL (120 pages)



- Terminology, concepts and role definitions
- Risk management diagnostic
- Operational tools
- Examples of successful practice

FIRM stands for Fundamental Information Risk Management:

- the methodology is based on extensive **statistical research** into the effectiveness of controls applied to thousands of mission-critical systems and is supported by continuing analysis of the massive body of statistics collected by the ISF as part of its core activities
- it distils **lessons learnt** and examples of **successful practice** from some of the world's most advanced users of IT
- its **chief architect**, Marco Kapp, is a co-founder of Citicus Limited and other Citicus directors also contributed to its development. Citicus has the **exclusive right** to develop and sell automation which enables organisations to implement the FIRM methodology.

citicusone

Citicus Limited's relationship with the Information Security Forum (ISF)

Information Security Forum	Citicus Limited
An international association of over 250 leading organisations	Independent company, founded by world's top experts on **FIRM**
Funds a practical research programme in information security, including development of **FIRM** methodology	Develops and sells automated risk management tools and supporting services

Unique, collaborative relationship since October 2001

ISF owns the published **FIRM** methodology and extension to e-commerce	Citicus has exclusive, world-wide right to develop and sell **FIRM** automation, including its extension to e-commerce
ISF receives a royalty on sales of **Citicus ONE**	Citicus pays a royalty to the ISF on each sale of **Citicus ONE**
ISF Members obtain **Citicus ONE** at a 12% discount	Citicus offers **Citicus ONE** to ISF Members at a 12% discount

Commitment to work together on on-going development of **FIRM** and related activities (eg ISF's **FIRM** training workshops for Members, Citicus input into ISF IRAM project)

citicusone

About Citicus Limited

- Formed in 2000 to provide world-class automated risk management tools and supporting services
- Offers **Citicus ONE** - the world's foremost tool for driving down information risk (ie the business risk posed by mission-critical, IT-based information systems) and other areas of risk
- Continuing relationship with the ISF (eg on IRAM and FIRM development)
- Exclusive, worldwide right to sell **FIRM** automation - reflecting Citicus directors' lead role in the development of this ground-breaking ISF risk methodology
- Provides the training and support needed to deploy **Citicus ONE**, plus advice / assistance with implementations either directly or via our Implementation partners

Partners

ISF – Protecting your business in the information age

GAI NetConsult

infraccent

regency IT Consulting

eFortresses – Security & Compliance Solutions

Selected customers

Unilever

kraft foods

StoraEnso

AXA

RWE – The energy to lead

E.ON

improvement service

Safaricom

NCB الأهلي

Travelport

Hampshire Police – Protect, Help, Reassure

Recognition

SC Magazine Awards 2010 Europe – Highly Commended

irm – Leading the risk profession

IDG Network Awards 04

SC Magazine Awards 2010 Europe – Excellence in Information Integrity

SC Magazine Awards 2010 Europe – Shortlisted

Bloor Research

ovum

Butler Group

2009 European Risk Management Awards – Strategic Risk

Forrester

SC Magazine

SC Magazine Awards 2003

computing 30th anniversary

citicusone

For further information

You can contact us at Citicus Limited either directly or via our head office:

Direct contact

Simon Oxley
Email simon.oxley@citicus.com
Tel +44 (0)1729 825 555

Marco Kapp
Email marco.kapp@citicus.com
Tel +44 (0)1306 742 072

Sian Alcock
Email sian.alcock@citicus.com
Tel +44 (0)20 8870 9279.

Head office

Citicus Limited
Holborn Gate
330 High Holborn
London WC1V 7QT.
Email info@citicus.com
Web www.citicus.com
Tel +44 (0)20 7203 8405
Fax +44 (0)20 7203 8409.

Our Implementation Partners will also be pleased to help you.

Their contact details can be found at www.citicus.com

citicusone