CIS RAM and FAIR integration

By Denny Wan

Peer reviewed by Chris Cronin

Synopsis

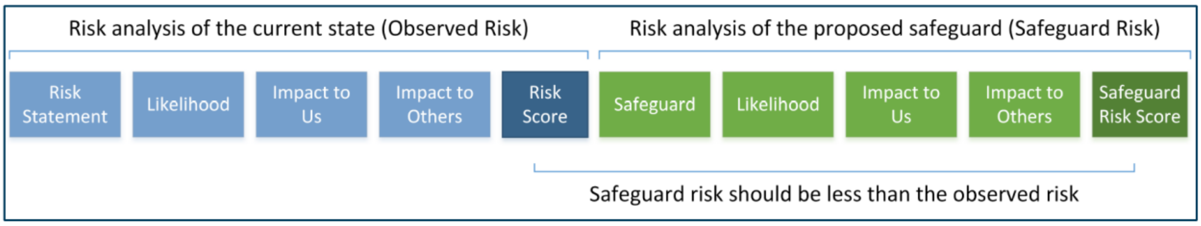
The Center for Internet® Security Risk Assessment Method (CIS RAM) is a documented process for conducting risk assessments that address requirements for security, business, regulations, and duty of care requirements. It also assists in the selection and prioritisation of safeguards discussed in the CIS Controls framework. Results are expressed as a risk score on an ordinal scale of 1-25. It is proposed to integrate the Open Group FAIR framework[1] into the risk quantification process to produce risk scores on a continual scale expressed as statistical distributions. Continual scale is better suited for the calculation of Return on Investment (ROI) on the proposed safeguards.

CIS RAM principles

CIS RAM helps organizations determine whether security controls are reasonable given the potential harm that may come to others, and the burden those controls may pose to an organization. CIS RAM is based on the Duty of Care Risk Analysis (DoCRA) standard[2] which expresses risk in terms that are equally meaningful to security technicians, business management, and legal authorities that interpret negligence and regulatory compliance using 'due care' and 'negligence' constructs. Developed in the United States, and applicable to other national legal systems, DoCRA principles address the need to demonstrate balance between risk to the public, and the business goals of organizations that pose that risk. The three principles in the Duty of Care Risk Analysis (DoCRA) standard are:

1. Consider the interests of all parties that may be harmed by the risk
2. Reduce risks to an acceptable level
3. Safeguards must not be more burdensome than the risks they protect against

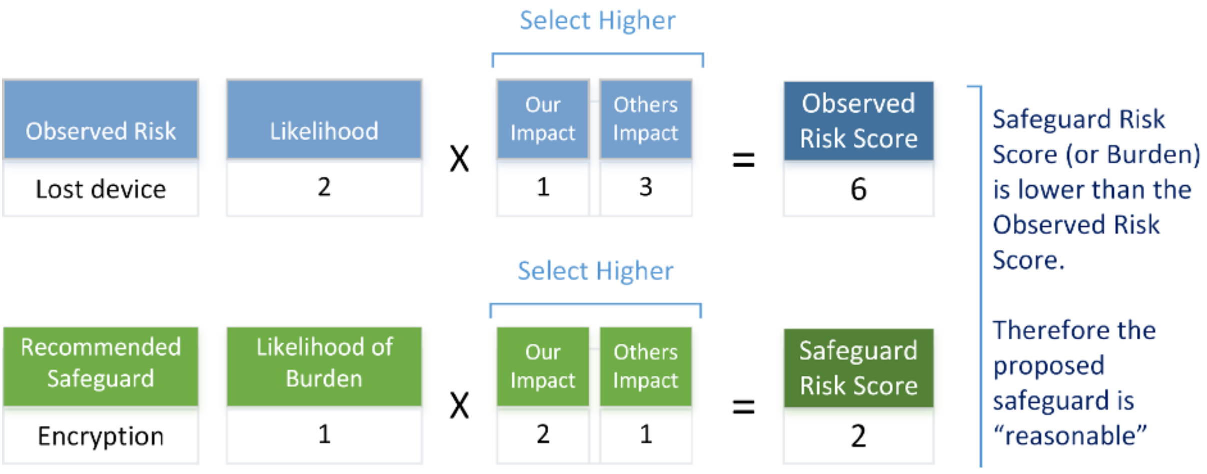
The application of these principles to CIS RAM is depicted below:


Risk analysis of the current state (Observed Risk)
Risk analysis of the proposed safeguard (Safeguard Risk)
Risk Statement
Likelihood
Impact to Us
Impact to Others
Risk Score
Safeguard
Likelihood
Impact to Us
Impact to Others
Safeguard Risk Score
Safeguard risk should be less than the observed risk

[1] http://www.opengroup.org/subjectareas/security/risk

[2] https://docra.org/

Furthermore, CIS RAM assesses risk impact from multiple dimensions reflecting the organisational mission, objectives and obligations. The highest impact score amongst these dimensions is then used to calculate the risk score by multiplying it with the likelihood as depicted below:



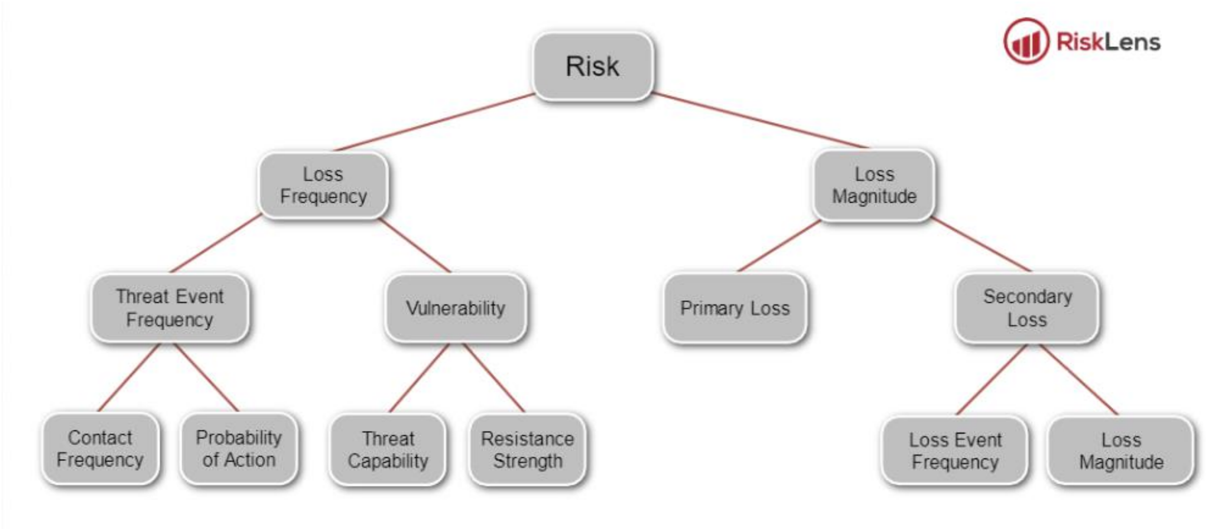
Safeguard Risk Score (or Burden) is lower than the Observed Risk Score.

Therefore the proposed safeguard is "reasonable"

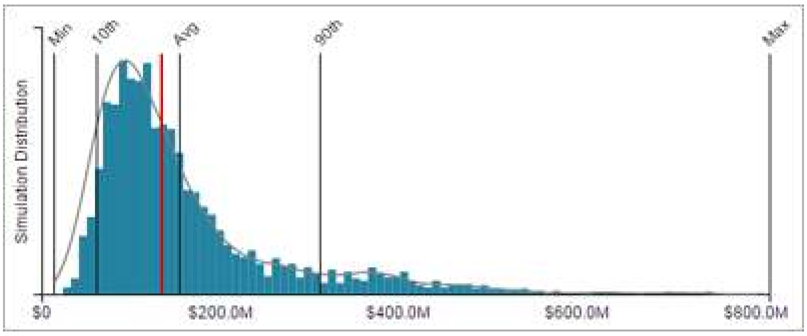
The final risk scores are expressed in an ordinal scale of 1-25 which is subject to interpretation by assessors and reviewers of the risk analysis. Potential differences in interpretation can lead to communication gaps in the risk management process, particularly when the risk analysis and recommendations on safeguards are to be presented to audiences not familiar with the targeted risk areas.

Integration with the Open Group FAIR framework

The Open Group FAIR framework is a commonly accepted cyber risk quantification framework using a published risk taxonomy and risk analysis standard to describe the risk quantification approach. The resultant risk score is expressed in a continual scale expressed as statistical distributions. The FAIR Risk Taxonomy and associated loss exceedance curve are depicted below:



FAIR Risk Taxonomy

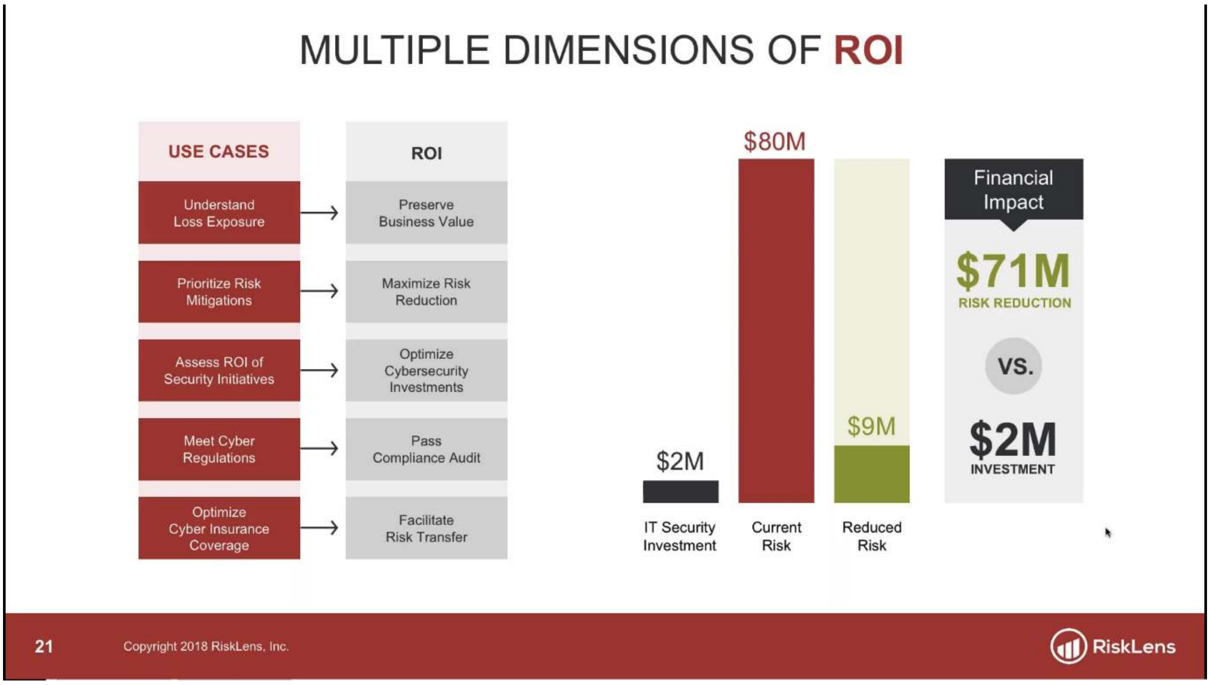


Loss exceedance curve

Mapping of CIS RAM terminology to the FAIR framework:

CIS RAM terminology	FAIR framework terminology
Likelihood	Loss Frequency
Impact	Loss Magnitude
Risk = Likelihood x Impact	Risk = Loss Frequency x Loss Magnitude

The FAIR quantification approach allows reviewers of the risk analysis to understand the assumptions and data sources used to derive the risk score. The expression of the risk score as a statistical distribution facilitates the calculation of ROI on the proposed safeguards as depicted below:



MULTIPLE DIMENSIONS OF ROI

USE CASES		ROI
Understand Loss Exposure	→	Preserve Business Value
Prioritize Risk Mitigations	→	Maximize Risk Reduction
Assess ROI of Security Initiatives	→	Optimize Cybersecurity Investments
Meet Cyber Regulations	→	Pass Compliance Audit
Optimize Cyber Insurance Coverage	→	Facilitate Risk Transfer

Financial Impact

$71M RISK REDUCTION

VS.

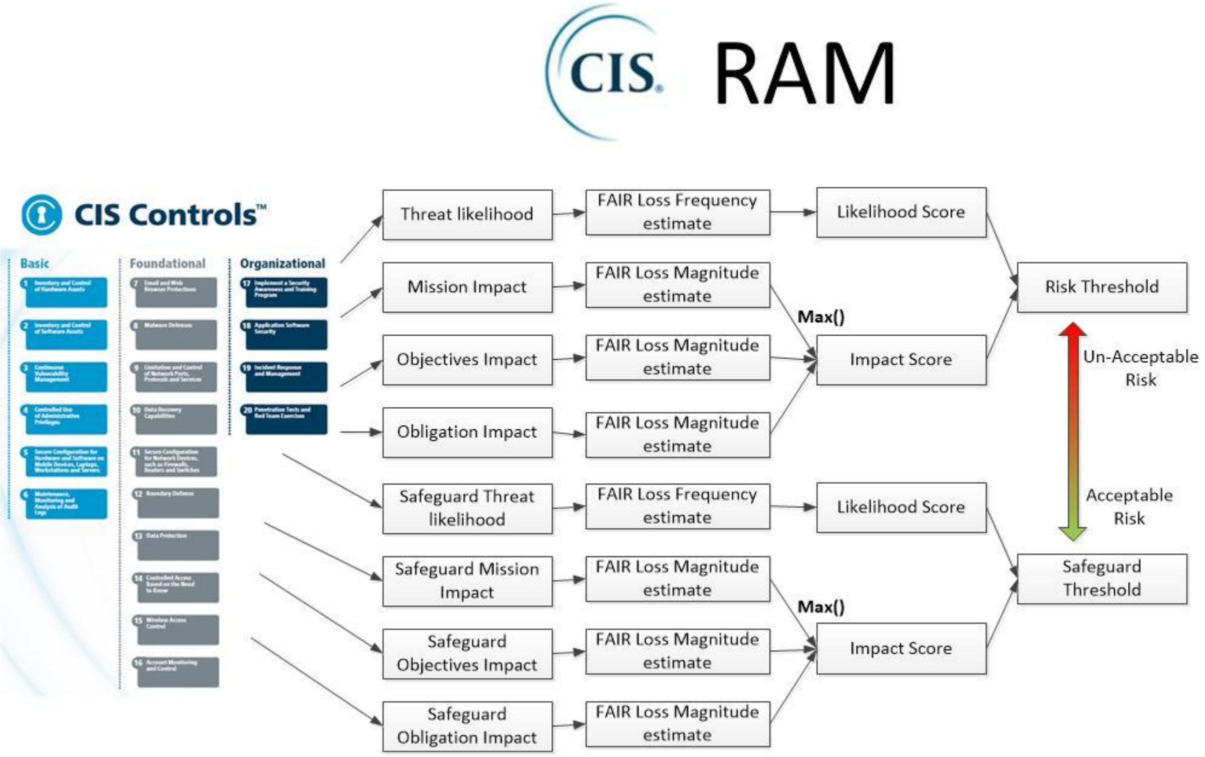
$2M INVESTMENT

21 Copyright 2018 RiskLens, Inc. RiskLens

Sample calculation of the ROI in cyber security management investments

A quantified risk analysis approach

The Integration between CIS (Controls and RAM) and the FAIR framework is depicted below:


CIS RAM
CIS Controls™
Basic
1 Inventory and Control of Hardware Assets
2 Inventory and Control of Software Assets
3 Continuous Vulnerability Management
4 Controlled Use of Administrative Privileges
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6 Maintenance, Monitoring and Analysis of Audit Logs
Foundational
7 Email and Web Browser Protections
8 Malware Defenses
9 Limitation and Control of Network Ports, Protocols and Services
10 Data Recovery Capabilities
11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring and Control
Organizational
17 Implement a Security Awareness and Training Program
18 Application Software Security
19 Incident Response and Management
20 Penetration Tests and Red Team Exercises
Threat likelihood
FAIR Loss Frequency estimate
Likelihood Score
Mission Impact
FAIR Loss Magnitude estimate
Objectives Impact
FAIR Loss Magnitude estimate
Obligation Impact
FAIR Loss Magnitude estimate
Max()
Impact Score
Risk Threshold
Un-Acceptable Risk
Acceptable Risk
Safeguard Threat likelihood
FAIR Loss Frequency estimate
Likelihood Score
Safeguard Mission Impact
FAIR Loss Magnitude estimate
Safeguard Objectives Impact
FAIR Loss Magnitude estimate
Safeguard Obligation Impact
FAIR Loss Magnitude estimate
Max()
Impact Score
Safeguard Threshold

By combining FAIR and CIS RAM, we could present a risk assessment method that more objectively evaluates risk and ROI while also demonstrating due care for others.

This whitepaper is available for downloaded here[3]

[3] https://www.securityexpress.com.au/wp-content/uploads/2019/03/CIS-RAM-FAIR.pdf

About the author

Denny Wan is the principal consultant of Security Express and has over 20 years' experience in cyber risk management, audit and infrastructure design. He is a certified PCI QSA and CISSP. Denny is chair of the Sydney Chapter of the FAIR Institute and a postgraduate research at Optus Macquarie University Cyber Security Hub researching into cyber insurance pricing strategies. He is a frequent speaker and presenter at information security conferences and events.

About the reviewer

Chris Cronin is an ISO 27001 Auditor and has over 15 years of experience helping organizations with policy design, security controls, audit, risk assessment and information security management systems within a cohesive risk management process. Chris is Chair of The DoCRA Council and the principal author of CIS Risk Assessment Method (RAM). He is a frequent speaker and presenter at information security conferences and events. Chris earned his Master of Arts from Case Western Reserve University.