FAIR INSTITUTE

Applying Quantification to NISTIR 8286

Connecting cybersecurity to Enterprise Risk Management

- Maximise Good Risks
- Communicate cyber risk in dollar value
- Demonstrate “Duty of Care”

Denny Wan

- Cyber risk practitioner - Principal Consultant, Security Express
- Certified auditor – PCI DSS, ISO 27001
- Researcher @ Macquarie University
- Chair – FAIR Institute Sydney Chapter
- Chair – Australian Cyber Insurance Think Tank

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

Agenda

- NISTIR 8286 Mission
- What are good risks?
- Risk appetite and tolerance
- ERM Principles
- Qualitative vs Quantitative Analysis
- Applying FAIR Methodology

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

NISTIR 8286 Mission

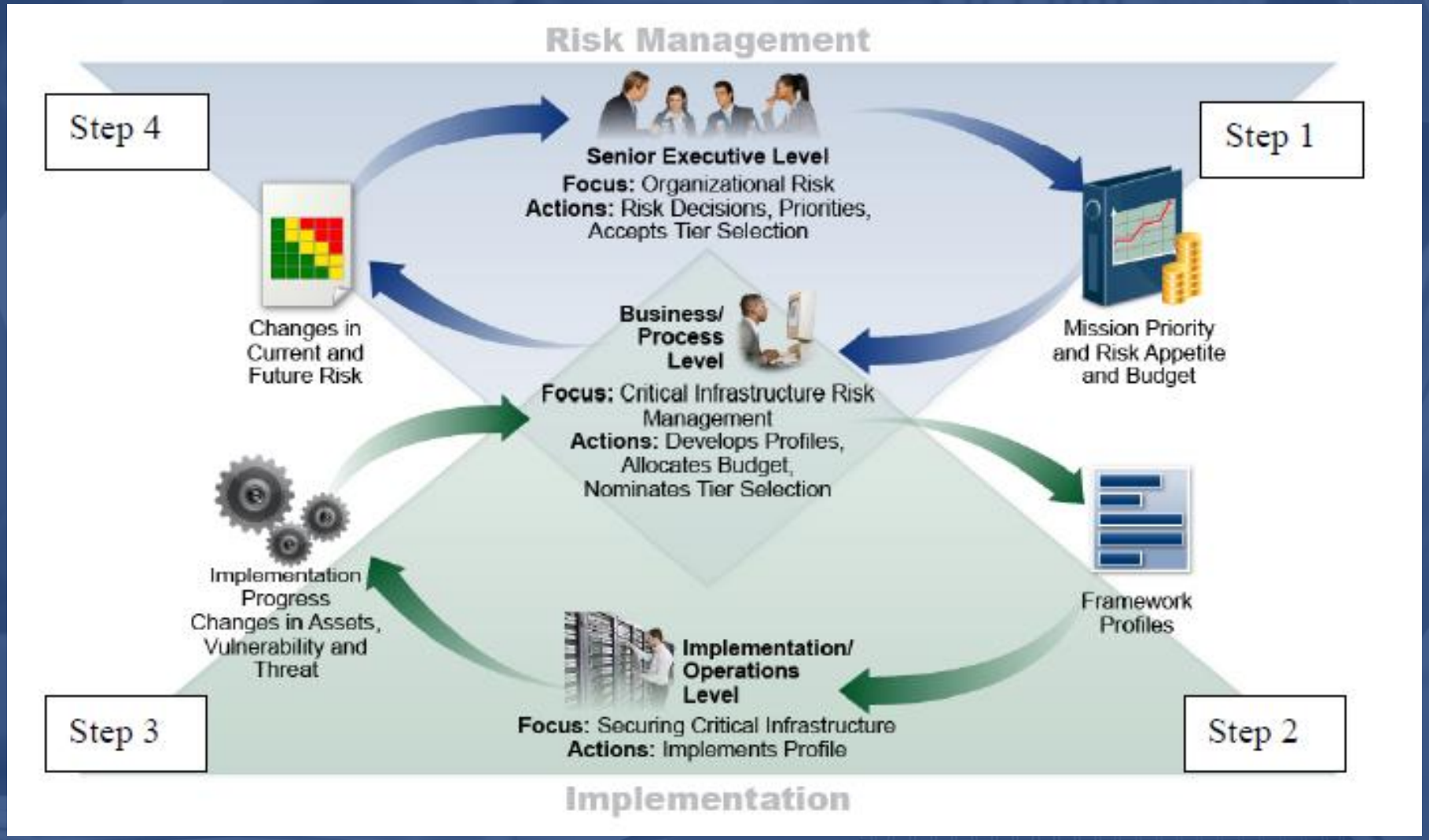
- 1. Ensures that cybersecurity risk is receiving appropriate attention within ERM
- 2. Improves their cybersecurity risk information as inputs to ERM
- 3. Enables enterprises to better identify, assess, and manage their cybersecurity risks
- 4. Focusing on the use of risk registers to set out cybersecurity risk
- 5. Explains the value of rolling up at lower system and organization levels to enterprise level

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

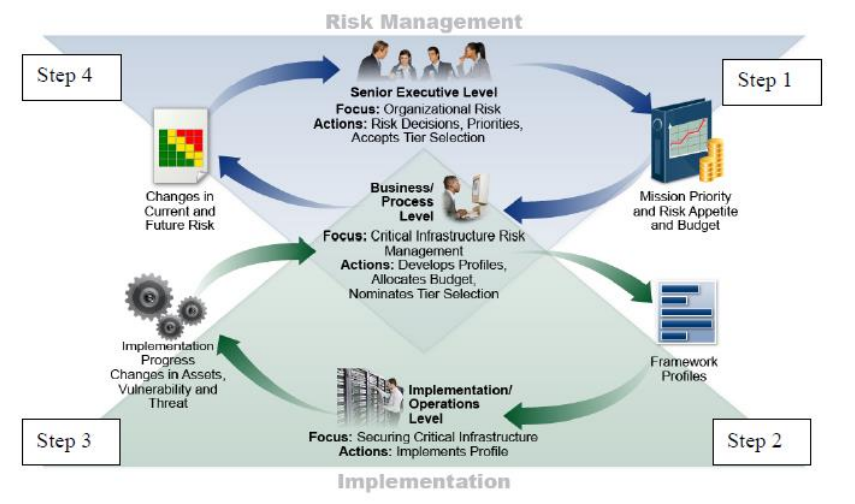
FAIR INSTITUTE

AISA Australian Information Security Association

NISTIR 8286 Mission



NISTIR 8286 Mission



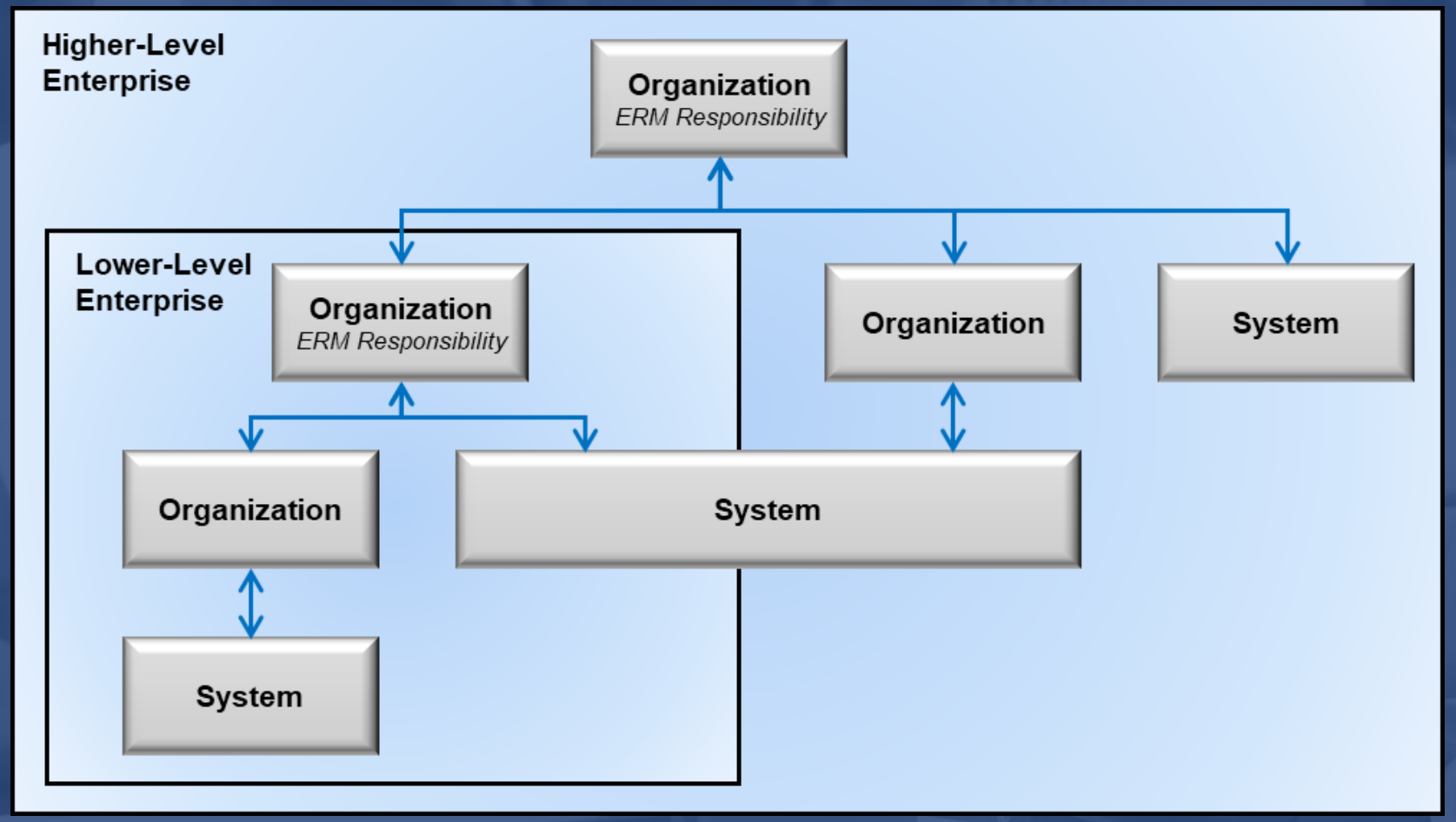
- Step 1: Setting mission and financial guidance at the business/process level
- Step 2: Develop Profiles, Allocates Budget, Nominates Tier Selection
- Step 3: Manage risk at system level through risk registers
- Step 4: Translating Cybersecurity to ERM

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

NISTIR 8286 Mission

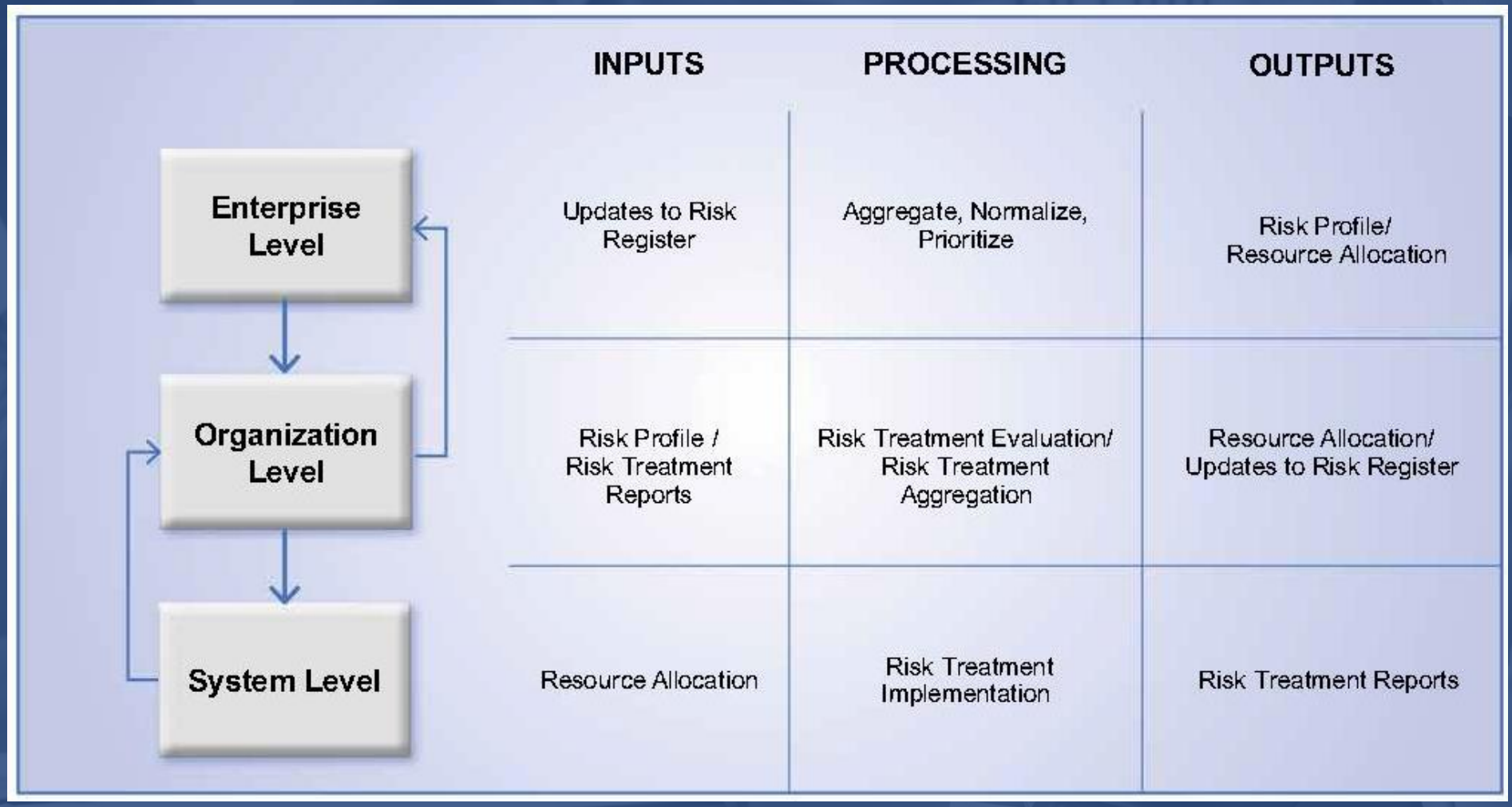


RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

NISTIR 8286 Mission

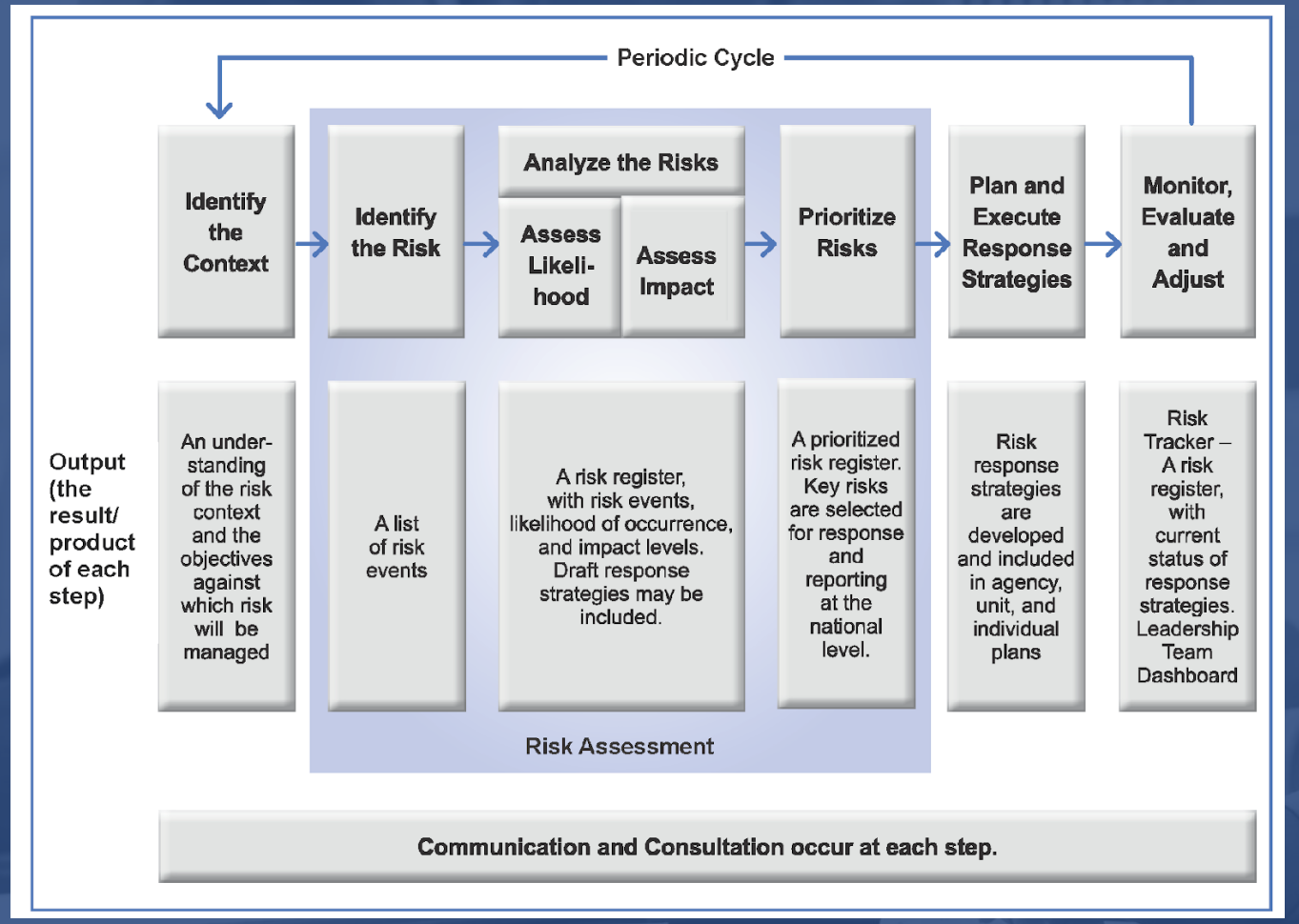


RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

NISTIR 8286 Mission



RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

What are good risks?

risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks."

Assumptions may occur at all levels of the organization, so it is important to determine internal and external stakeholders' expectations regarding risk communications—and to use readily understandable and agreed upon terms and categories such as strategic objectives, organizational priorities, decision-making processes, and risk reporting or tracking methodologies (e.g., regular risk management committee discussions and meetings).

An effective ERM program defines and communicates enterprise risk appetite so that meaningful risk tolerance statements can be created, used and monitored. Risk appetite also serves as a guidepost and reflects strategic risk direction from leadership. As adopted from COSO, OMB Circular A-123 defines risk appetite as "the broad-based amount of risk an enterprise is willing to accept in pursuit of its mission/vision." With strategic risk direction communicated to the organizational and system levels of the enterprise, cybersecurity officers can apply the guideline when establishing risk expectations at organization and system levels. Risk management strategy should also include direction regarding the risk register, such as how entries should be categorized. The use of common risk categories supports the aggregation of various types of risk across the enterprise.

Risk appetite and tolerance

This document draws on ERM principles regarding integration with culture, strategy, and performance. One such principle is that an "organization must manage risk to strategy and business objectives in relation to its *risk appetite*—that is, the types and amount of risk, on a broad level, it is willing to accept in its pursuit of value" [8]. OMB adapted this language for government use in Circular A-123 by similarly stating risk appetite "is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision." Risk appetite is established by the organization's most senior-level leadership (enterprise) and serves as the guidepost for decisions such as setting strategy and selecting objectives.

Another important ERM concept is *risk tolerance*—the organization or stakeholders' readiness to bear the remaining risk *after responding to or considering the risk* in order to achieve its objectives (while recognizing that such tolerance can be influenced by legal or regulatory requirements) [6].[10] OMB again adapted the COSO language by stating that risk tolerance "is the acceptable level of variance in performance relative to the achievement of objectives."

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

Risk appetite and tolerance

appetite is narrower, stating: "Email services shall not be interrupted more than five minutes during core hours."

Senior enterprise executives provide risk guidance (including advice regarding mission priority, risk appetite and tolerance guidance, and capital and operating budgets to manage known risks) to the organizations within their purview. Risk appetite and risk tolerance statements are the usual means for communicating this guidance. Organizations then manage and monitor processes that properly balance the risks and resource allocation with the value created by information and technology. Measurements (e.g., from key risk indicators, or KRIs) demonstrate where risk tolerances have been exceeded or validate that the enterprise is operating within the defined appetite. A subsequent report in this series (NISTIR 8286A) will provide detailed examples of risk appetite and risk tolerance statements and how they are interrupted and applied with the associated risk defined, managed, and communicated back to executive management via the risk register.

ERM Principles

- "Target residual risk is the amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions to alter the severity of the risk."
- "Actual residual risk is the risk remaining after management has taken action to alter its severity. Actual residual risk should be equal to or less than the target residual risk."

Cybersecurity risk identification is comprised of four inputs:

1. Identification of the organization's mission-supporting assets and their valuation
2. Determination of potential threats that might jeopardize the confidentiality, integrity, and availability of those assets and potential information and technology opportunities that might benefit the organization
3. Consideration of the vulnerabilities of those assets
4. Evaluation of the potential consequences of risk scenarios

Qualitative vs Quantitative Analysis

From NISTIR 8286:

- Risk appetite may be communicated using qualitative, quantitative, and semi-qualitative methods (NIST SP 800-30)
- Qualitative analysis is based on the assignment of a descriptor
- Quantitative analysis involves numerical values, which are assigned to both impact and likelihood
- Common ERM practices include both qualitative and quantitative types of risk analysis

Qualitative vs Quantitative Analysis

How to Bridge the Gap Between Qualitative and Quantitative Risk Analysis

Mar 31, 2016 4:30:00 PM / by **Steve Poppe**

Tweet Share Like 0 Share

All the traditional risk management frameworks use "heat maps" or some variant – a color-coded matrix of "likelihood" against "impact."

The "quants" in the new generation of risk analysts believe (I plead guilty) that there are much better ways to express risk than the fake math implied by fake-multiplying a subjective likelihood by a subjective impact to get a super-subjective risk level.

https://www.fairinstitute.org/blog/how-to-bridge-the-gap-qualitative-and-quantitative-risk-analysis

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

Qualitative vs Quantitative Analysis

Qualitative analysis as a stepping stone to Quantitative analysis:

4.2.2 Stage 2: Evaluate Loss Event Frequency (LEF)

4.2.2.1 Estimate the Threat Event Frequency (TEF)

Some people demand reams of hard data before they are comfortable providing quantitative estimates. Unfortunately, because we sometimes don't have useful or credible data for scenarios, the Threat Event Frequency (TEF) is often ignored altogether. When we ignore the frequency component of risk, however, we are no longer talking about risk. So, in the absence of hard data, what's left? One answer is to use a qualitative scale, such as Low, Medium, or High. And, while there's nothing inherently wrong with a qualitative approach in many circumstances, a quantitative approach provides better clarity and is more useful to most decision-makers – *even if it's imprecise*. For example, I may not have years of empirical data documenting how frequently cleaning crew employees abuse usernames and passwords on sticky-notes, but I can make a reasonable estimate using ranges, particularly if I have been trained in how to make estimates effectively.

Source: FAIR Taxonomy standard section 4.2.2

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

Applying FAIR Methodology

Factor Analysis of Information Risk (FAIR) is the only international standard quantitative analysis model for information security and operational risk

- A Standard Taxonomy for Information and Operational Risk
- A Methodology for Quantifying and Managing Risk in Financial Terms in Any Organization
- A Complementary Analytics Model to existing Risk Frameworks, such as ISO 31000, COSO, NIST CSF
- A Standard of The Open Group

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

THE COMMUNICATION CHALLENGE

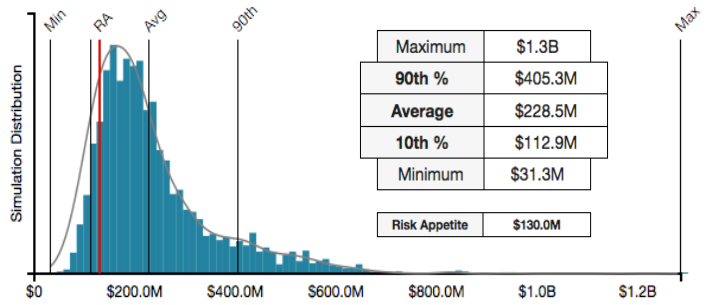
RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

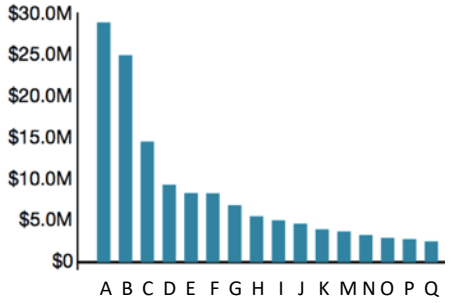
Communicating Cyber Risk in dollar value

"HOW MUCH RISK DO WE HAVE?"

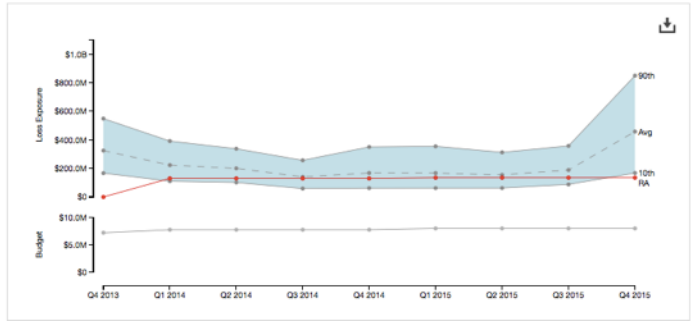


Maximum	$1.3B
90th %	$405.3M
Average	$228.5M
10th %	$112.9M
Minimum	$31.3M
Risk Appetite	$130.0M

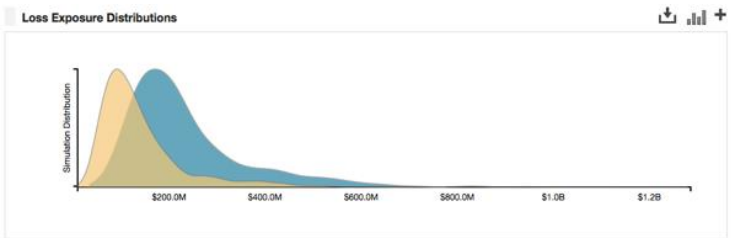
"WHAT ARE OUR TOP RISKS?"



"HOW IS OUR RISK TRENDING VS. APPETITE?"

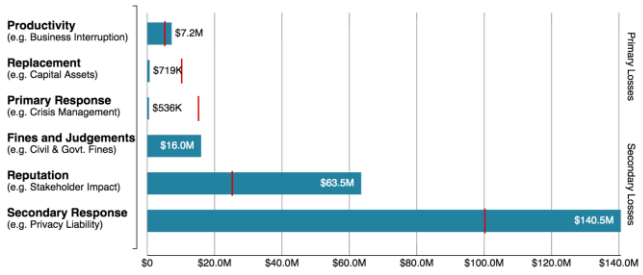


"HAVE WE REDUCED RISK?"

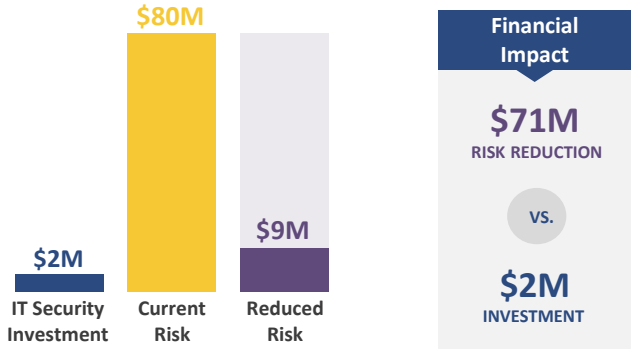


Analysis	Reporting Period	Minimum	10th %	Average	90th %	Maximum
Annual Baseline Enterprise Analysis	Quarter 1 2014	$31.3M	$112.9M	$228.5M	$405.3M	$1.3B
Quarterly Updated Enterprise Analysis	Quarter 3 2014	$9.4M	$58.3M	$137.8M	$254.7M	$781.5M

"WHAT TYPE OF LOSS CAN WE EXPECT?"



"WHAT IS THE COST/BENEFIT OF THIS PROJECT?"



(Source: RiskLens)

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

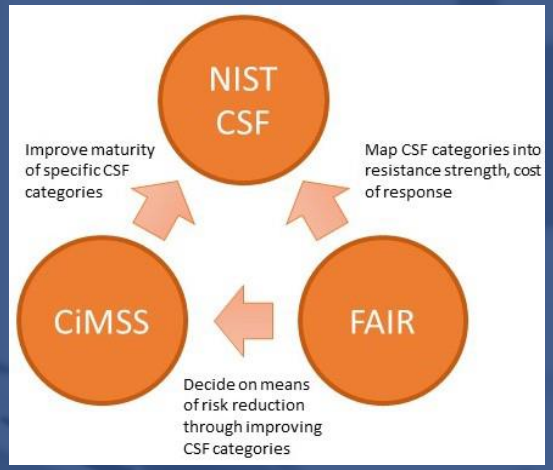
FAIR INSTITUTE

AISA Australian Information Security Association

Applying FAIR to NIST CSF

"Taking more risks is only possible when you can accurately and consistently measure it. Utilizing CSF and FAIR allows us to get a clear understanding of our risk and security maturity and direct our risk management in a reasoned fashion."

Ian Amit, Chief Security Officer, Cimpress



https://www.nist.gov/cyberframework/success-stories/cimpress-fair

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

Panel Session

- Quick intro to the chapters
- Resource available to members
- Collaboration opportunities between communities

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

Kerry McGoldrick

- Recognised leader in governance, risk and resilience
- Vice President of the RMIA NSW Chapter
- Partner - ShineWing Australia
- Member, Risk Management Committee (OB-007), Standards Australia

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

Kerry McGoldrick

- AISA Sydney Branch Executive
- AISA's 2019 Branch Chair of the Year award
- Founder & Executive Director of Dragonfly Technologies
- Co-founder of a healthcare startup, VAXXIN8
- knowledgeable and engaging speaker on cybersecurity and business

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association

Panellists

RMIA

FAIR Institute

AISA

AISA & FAIR Institute
Combined Sydney Chapter Meeting

- Tuesday 24th Nov 2020 12noon (AEST)
- Deep Dive in FAIR and NISTIR 8286
- Extended Panel Session on practical use cases

RMIA RISK MANAGEMENT INSTITUTE OF AUSTRALASIA

FAIR INSTITUTE

AISA Australian Information Security Association