Privasec | GRC
GOVERNANCE AND INFORMATION SECURITY PARTNERS

FAIR Cyber Risk Quantification Service
Fact Sheet v1.6

OUR SERVICE

The FAIR Cyber Risk quantification Service helps companies to quantify and measure their cyber risks in the same way that financial and operational risks are measured by executives, boards and risk committees.

- Calculate the expected financial loss from cyber-attacks and frauds.
- Prioritise security investments based on measurable Return on Investment (ROI)
- Compatible with the APRA CPS 234 standard by assessing information security capability commensurate the size and extent of threat exposure.

Articulate cyber risks in financial metric with which business executives and board are familiar.

WHAT IS APRA CPS 234?

APRA CPS 234 is an Information Security standard demanding regulated entities to become resilient against information security incidents by maintaining an information security capability commensurate with information security vulnerabilities and threats. Compliance with CPS234 for regulated entities becomes mandatory from 1st July 2019.

WHAT IS FAIR?

FAIR (Factor Analysis of Information Risk) is a global standard which provides a structured and consistent methodology to breakdown information risk scenarios and measure the expected financial loss. FAIR is part of the NIST Informative Reference Catalogue.

FAIR is followed by 30% of the Fortune 1000, including many large financial institutions such as Bank of America, FannieMae, Fderal Reserve. FAIR is also rapidly being adopted by other industries throughout the US, EMEA and APAC.

GOOD TO KNOW

The FAIR quantification analysis is compatible with most risk assessment and management frameworks such as NIST CSF, ISO 27001 or PCI DSS which do not have a structured quantification methodology or component.

Our service does not impact the current risk assessment and management process. It adds value to them by supporting the prioritisation of the identified risks in a way that business executives and boards understand.

HOW THIS SERVICE WORKS

1. We apply FAIR analysis against existing and new investments in information security to support and tune the investment prioritisation process and to measure the maturity of your security processes against the NIST CSF and/or ISO27005 (depending on your organisation)
2. We work with your team to adopt the FAIR framework to build your internal cyber risk quantification process which produces consistent and repeatable.measurements on the potential financial loss from cyber-attacks, before and after the security solution uplift.
3. We create a repeatable cyber risk report templates tailored to the relevant boards and committees within your organisations.

Our consultants are certified FAIR and information security professionals.

The quantification process uses historical breach data and financial loss information to accurately profile the financial loss exposure of the organisation to information security risk, no longer relying on industry average loss which might not be relevant to the current operating environment and market condition of the organisation.

KEY BENEFITS

A FAIR risk quantification:

- Provides concrete measurements on the business benefits from investment in information security
- Creates a common business language for cyber risk discussion.
- Promotes a culture of prudent investment practice in information security.

WHAT DO YOU GET

- A structured and repeatable cyber risk quantification process (based on historical breach data and financial loss) which gives confidence to the organisation that expected reduction in financial loss from cyber-attack is achievable and measurable.
- A repeatable executive dashboard which aligns cyber risk with other business risk metrics which business executive and board can actually understand.
- Knowledge-transfer to internal team to build for these repeatable processes.

NEXT STEPS

Speak to a consultant to book a demo. We'll show you how its works and see how we can best support you.

Privasec

GRC GOVERNANCE AND INFORMATION SECURITY PARTNERS

RED RED TEAMING & ADVANCED ETHICAL HACKING

+61 1800 996 001 (AU)
+65 6610 9597 (SG)
+64 9 222 4725 (NZ)

info@privasec.com

www.privasec.com

New South Wales Office
Level 12, 234 George Street
Sydney 2000
NSW, Australia

New Zealand Office
Level 4, 17 Albert Street
Auckland CBD 1010
New Zealand

Victoria Office
Level 6, 276 Flinders Street
Melbourne 3000
VIC, Australia

Singapore Office
10 Anson Road
International Plaza #34-06
Singapore 079903

Queensland Office
Level 6, 200 Adelaide Street
Brisbane 4000
QLD, Australia

Malaysia Office
B-5-8 Plaza Mont Kiara
Mont Kiara 50480
Kuala Lumpur, Malaysia