



COA¹ Position Paper Risk Lifecycle Management

Problem

The Jericho Forum's Collaboration Oriented Architectures (COA) enable enterprises that build COA-compliant architectures to operate in a secure and reliable manner in an environment of increasing information threat, and where it is the growing norm to interact without boundaries, irrespective of the location of the data or the number of collaborating parties.

COA involves a significant move of security emphasis from infrastructure to applications. This affects information risk management in that it makes information risks:

- more numerous - because the entities at risk are now application rather than infrastructure elements
- more severe - because there is less defence-in-depth and therefore a compromise is more likely to have an immediate business impact.

Why Should I Care?

- Security professionals who propose COA must be able to communicate with management about the risks involved.
- Organisations need to manage and demonstrate compliance in a more complex risk environment.

Jericho Forum Recommendation/Response

The Jericho Forum believes that:

- Organisations need to manage risk in a way that is systematic and closely relates to the organisation's business environment and security architecture.
- Organisations need to express and manage information risks in the same way as any other risk. In particular, they should use methods that are, or can be made to be, quantitative.
- Extensive tool support will be required by all but the smallest organisations to allow information risks to be managed properly.

Background & Rationale

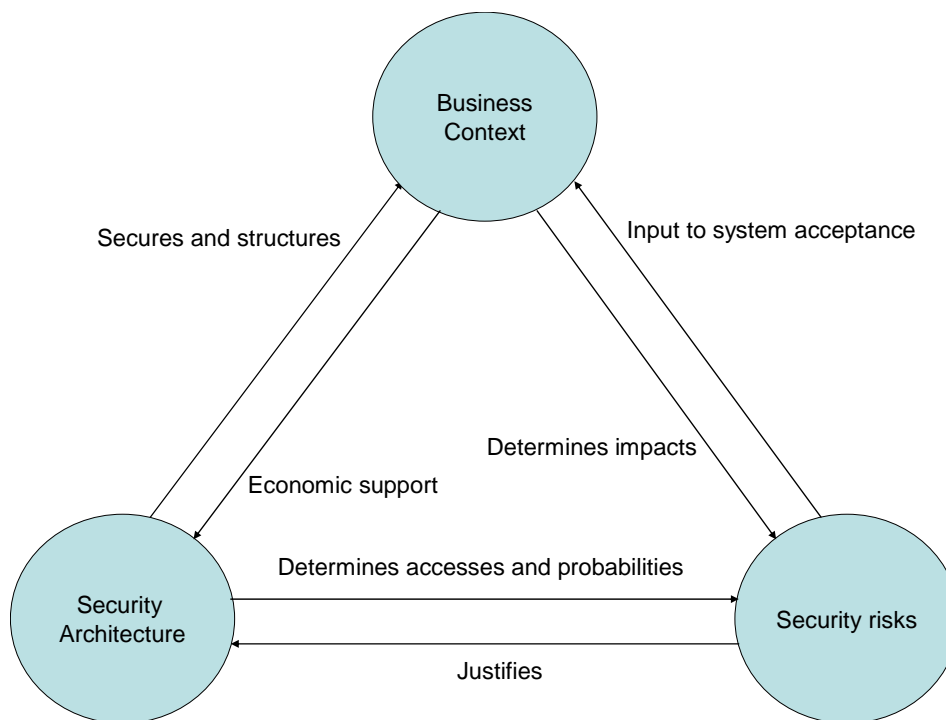
Understanding an organisation's security requires an understanding of three interrelated areas:

- The business context for security – the rules and policies in force, the assets handled and their values, and the stakeholders and users. Expected costs, service levels and benefits are also best understood at this level.
- The security architecture – the structures, links and security controls in place within the organisation. These determine the accesses (from users to assets) and hence the risks.

¹ Collaboration Oriented Architectures (COA, and COA Framework – available at <http://www.opengroup.org/jericho/publications.htm>

- The risks – undesired events with their impacts and probabilities.

The figure below shows how these areas influence each other.



A perimeterised security architecture leads to a complex set of structures, but the security risks are minimised in number. A de-perimeterised security architecture, on the other hand, leads to a flatter, simpler set of structures; assets are potentially exposed to more users, so the risks are more numerous and have more immediate business impact.

Having more risks means that the risks must be structured to ensure they are manageable.

Key Challenges and Next Steps

Standards are required in this area to permit:

- development and application of effective tools.
- evaluation and acceptance of risk, both within and between organisations.

Standards are required for describing the following:

- Security architectures. We already have ISO27001/2 but this standard does not facilitate automated risk management.
- Risk, in 2 key aspects:
 - to establish a standard vocabulary (Risk Taxonomy) for describing the essential common terms in use in the industry. Even critical terms like threat, vulnerability, even risk itself, are used very differently across the industry, making it very difficult to compare different risk assessment approaches for evaluating exposure to risk/loss.
 - to adopt effective risk assessment methodologies which deliver objective, meaningful, consistent results.

The Open Group is developing a set of risk standards based on the FAIR (Factor Analysis of Information Risk) method.

- Security contexts. Interesting approaches in this area include the UK Government's Risk Management Accreditation Document Set standards.