



COA¹ Service

Trust Management: Impact Sensitivity Categorization

Introduction

Information must be classified using an appropriate Classification Scheme as defined in the Jericho Forum's Information Classification² position paper. The classification of information will define associated information protection requirements in terms of restricting the circulation of information based on identity, legality, and temporal components. Confidentiality, Integrity, Availability and Authenticity (CIA&A) must also be considered for information created within organisations. Thus, information must be categorized to reflect the level of business impact that would occur if any of these requirements were not correctly enforced.

Business impact is generally financial and will vary in magnitude depending on the size and economic health of the organisations. Financially healthy companies will suffer less than financially healthy companies with the same value of impact.

The Problem

The access and usage of information controlled using Enterprise Information Protection and Control³ (EIP&C) tools in de-perimeterised environments should reflect not only the restricted circulation of information as required by an Information Classification Scheme, but also the storage, handling, transport and environmental restrictions associated with the information in terms of impact sensitivity should its Confidentiality, Integrity, Availability or Authenticity be compromised.

For example, information classified as "Amber" using the Traffic Light Information Classification Scheme has associated information protection requirements that represent the need to limit the circulation of that information to a specific domain such as internal organisation or a collaborative working group. The business impact of access (confidentiality) or modification (integrity) of that information outside of this domain; the lack of availability of the information when required within the domain; and changes to the information without the consent of the data originator (authenticity) within the domain, will reflect the economic impact associated with any of these occurrences.

¹ The Collaboration Oriented Architectures (COA) paper and associated COA Framework paper are available at <http://www.opengroup.org/jericho/publications.htm>

² Information Classification paper – available at <http://www.opengroup.org/jericho/publications.htm>

³ EIP&C paper – available at <http://www.opengroup.org/jericho/publications.htm>

Why Should I Care?

Without appropriate classification, information circulation cannot be restricted appropriately. From a confidentiality point of view, encryption and access controls can suffice without information classification for maintaining information protection in de-perimeterised environments, as long as appropriate de-perimeterised access controls are used. However, for integrity, availability and authenticity, a different model is required. Impact Sensitivity Categorization can define appropriate information usage and handling controls in relation to these requirements.

Recommended Solution

The requirement here is to develop a common language (taxonomy) and set of trust levels defining impact sensitivity of information, based on measures of its Confidentiality, Integrity, Availability and Authenticity. (Note that Service or System Criticality is potentially a separate area of classification.)

We propose 6 levels:

- T5 Catastrophic
- T4 Material
- T3 Major
- T2 Minor
- T1 Insignificant
- T0 None

The magnitude in terms of financial impact will vary depending on the economic size of the organisation. Based on the FAIR Risk Assessment Guide⁴, the table below defines the numeric value of magnitude for a large Fortune 100 company. What has significant impact for them may be catastrophic for an SME, so the \$ values must be adjusted to suit each organisation.

Magnitude	Range Low End	Range High End
Disaster	1,000's of Deaths	
Catastrophic	Death / Company Ceases to Trade	
Material	\$250,000,000	→
Severe (SV)	\$10,000,000	\$100,000,000
High (H)	\$1,000,000	\$9,999,999
Significant (Sg)	\$100,000	\$999,999
Moderate (M)	\$10,000	\$99,999
Low (L)	\$1,000	\$9,999
Very Low (VL)	\$0	\$999

Background and Rationale

The business impact level associated with information, together with the information classification label, drive the requirement for controls to be applied to manage the way in which users access and handle data. Controls to consider include the following 5 items.

⁴ FAIR (Factor Analysis of Information Risk) Assessment Guide G081, available from The Open Group Online Bookstore - <http://www.opengroup.org/bookstore/catalog/>

Information Creation

It is important to consider the impact sensitivity of new or recreated information. Sometimes information can be secured by not actually creating it at all if there is no real requirement for it. For example, creating information that contains multiple types of personal identifiable information from different data sources for the sake of ease of access to all information could have high impact sensitivity if not properly secured and is not actually of importance to business process; therefore it should not be created in the first place.

Information Storage

The risk associated with storing information must be considered both internally and in de-perimeterised environments. From a confidentiality aspect, the information may require secure storage, i.e. storage on encrypted file systems. From an integrity point of view, the modification of information may require audit or tamper-evident data storage to be used so that any changes to the information can be detected and traced. The availability requirement may suggest multiple backups and mirrors of the information to be supported in case any of the file servers become unavailable. It may also be essential to continually monitor the state of the backups and mirrors to ensure guaranteed access to information in the event of system failure. There is no point having backups if they are also offline.

Information Sharing

CIA&A requirements must be considered before sharing any classified information. Simply encrypting and providing access controls may suffice for confidentiality, but in some business process this requirement is not adequate to support secure business process. Where availability, integrity and authenticity are important aspects of information sensitivity, appropriate consideration should be given to the circulation of the information and who may gain access and modification control of it.

Information Transfer

Information transfer over inherently insecure protocols must be secured using appropriate mechanisms. Confidentiality, Integrity and Authenticity should be protected from information interception and/or modification in transfer. Availability may be an essential requirement in critical information systems. Thus, the information transfer mechanisms must guarantee availability and end-to-end transfer at all times.

Information Deletion

Information with high business impact in terms of CIA&A must be securely destroyed when its useful lifetime ends. Simply deleting it (moving to “trash”) does not destroy the content. Secure “digital data shredding” must be performed.

Challenges to Industry

The ability to consistently classify information at all points in its lifecycle and across the entire IT infrastructure is critical. If the information cannot be classified correctly then it also cannot be managed appropriately. Static classification of information by the information owner is not workable in today’s global environment; therefore consistent automation is also required.

Defining an agreed, standardised taxonomy for information classification is essential to the success of Trust Management in de-perimeterised environments.