CEN

WORKSHOP

AGREEMENT

CWA 15929

February 2009

ICS 35.040

English version

Best Practices for the Design and Development of Critical Information Systems

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: Avenue Marnix 17, B-1000 Brussels

TABLE OF CONTENTS

1. FOREWORD

The purpose of this CEN Workshop is to develop a first level European agreement on best practices for market players to ensure quality in designing, developing, maintaining and operating critical information systems, including both applications and infrastructure.

This CEN Workshop background, objectives, work program, workshop structure and resource requirements are defined in the Business Plan, version 2.0 dated March 6, 2007 and adopted at the kick-off meeting of the workshop on 07 March 2007.

The final review/endorsement round for this CWA was successfully closed on 23 June 2008. The final text of this CWA was submitted to CEN for publication on 17 November 2008.

The CEN Workshop members who have supported the document are (in alphabetical order):

ARMA International, ASD, CS (Initiator), NYSE EURONEXT Technology, EISIS (Etudes et Ingénierie des Systèmes d'InformationS), Groupement des Cartes Bancaires, INFOCERT, La Banque Postale (Initiator), Prologism (Initiator), RexConseil, THALES, VOLANS Informatica.

The resulting deliverable consists of the present CWA (CEN Workshop Agreement). This document provides guidelines for the design, development and maintenance of information systems requiring a high level of quality of service (including performance and availability).

The workshop addresses mission-critical Management (or Business) Information Systems. It does not cover mission-critical systems in the scientific, industrial (control-command, etc.) and embedded systems domains, for example. In those domains, practices and technologies already focus on "technical" requirements whereas their "functional" requirements are generally specific, stand-alone and dedicated to a limited set of specifications.

The lifecycle of an IT project can be divided into three phases: Design, Build, and Run. This CEN Workshop addresses the practices required in the Design and Build phases, with a particular focus on how those practices impact the Run phase.

Finally, the workshop addresses practices required to fulfil technical specifications (or quality of service requirements), i.e. "Build it right and make it efficient". It does not address the practices required for functional specifications (or business requirements), i.e. "Build the right thing".

This CEN Workshop Agreement is publicly available as a reference document from the National Members of CEN : AENOR, AFNOR, ASRO, BDS, BSI, CSNI, CYS, DIN, DS, ELOT, EVS, IBN, IPQ, IST, LVS, LST, MSA, MSZT, NEN, NSAI, ON, PKN, SEE, SIS, SIST, SFS, SN, SNV, SUTN and UNI.

Comments or suggestions from the users of the CEN Workshop Agreement are welcome and should be addressed to the CEN Management Centre.

2. TERMS AND DEFINITIONS

2.1. Definition of a critical information system (CIS)

A business information system aims at performing functions to achieve a desired result. There are critical business functions and non-critical business functions.
Once translated into a computer system, each critical business function will be performed by one or more critical applications and infrastructures.
In addition, one particular critical application may cover both critical and non-critical business functions.

For the purpose of clarity, we will use simple and common sense definitions in this document.

For the purpose of this document, a *critical information system* is defined as any application and/or infrastructure which performs one or more critical business functions, as well as a set of applications and infrastructure whose combination performs one or more critical business functions.

"A critical information system (CIS) is one whose quality of service is essential to the successful functioning of the organization in which it is used: **a failure in its quality of service results in the failure of the entire information system and has significant impact on the operations of the organisation in which it is used."**

For the IT specialist, this definition is interpreted as follows:
"Technical specifications for CIS requirements demand just as much if not more effort than those for the functional requirements."

A CIS must provide:

- A high level of quality of service during the Run phase.
- A high level of life cycle control during the initial and on-going Design, Build and Run phases.

Although risk management is an important issue as far as Critical Information Systems (CISs) are concerned, it is outside the scope of this CEN Workshop. We recommend referring to the following standards and set of best practices:

- ISO/IEC FCD 27005: Information technology - Security techniques - Information security risk management.
  Status: International standard under development (Not available presently).
- ISO/IEC 16085:2006: Systems and software engineering - Life cycle processes - Risk management.
  Status: Published International Standard.
- AS/NZS 4360: Risk management.
  Status: Australian / New Zealand published standard.

2.2. Definition of CIS requirements

2.2.1. General

This section provides, for the purpose of this document, specific definitions of requirements crucial to a CIS. For a given CIS, only one or just a few requirements may be a major concern.

Two types of specific requirements may be crucial for a CIS:

- **Quality of service requirements** (generally addressing the concerns of both business process owners, stakeholders and IT specialists):
    - Integrity.
    - Availability.
    - Performance.
    - Capacity.
    - Security[1].
- **Quality of system requirements** (generally addressing the concerns of IT specialists):
    - Maintainability.
    - Resilience.
    - Usability.

2.2.2. Integrity

"The system shall render the service without errors and/or loss or corruption of data."

2.2.3. Availability

"An available system is one that renders the expected service at the desired time i.e. with the expected timeliness and priority."

Availability also covers the capability of a CIS to return to a normal condition within a specified time interval after a problem or a failure occurs.

Availability is different from continuity of service (IT survival plan, disaster recovery plan, business continuity plan, etc.).

2.2.4. Performance

"The system shall render the service in the best possible elapsed time, within the required limits, under specified circumstances."

2.2.5. Capacity

"The system shall render the service within the specified volume and flows limits, and it shall react appropriately in case of an overflow."

2.2.6. Security

It is recommended to refer to ISO/IEC 27001 (formerly 17799-2005): "Information security is the protection of information from a wide range of threats in order to ensure business

[1] *Security is a special requirement:*
- it is an essential requirement for any application, be it critical or not.
- the eight other requirements addressed in the CIS approach must be considered systematically when designing any security solution.