



NSAI
Standards

Standard Recommendation
S.R. CWA 15929:2009

Best Practices for the Design and Development of Critical Information Systems

S.R. CWA 15929:2009

Incorporating amendments/corrigenda issued since publication:

<i>This document replaces:</i>	<i>This document is based on:</i> CWA 15929:2009	<i>Published:</i>	
This document was published under the authority of the NSAI and comes into effect on: 12 March, 2009		ICS number: 35.040	
NSAI 1 Swift Square, Northwood, Santry Dublin 9	T +353 1 807 3800 F +353 1 807 3838 E standards@nsai.ie W NSAI.ie	Sales: T +353 1 857 6730 F +353 1 857 6729 W standards.ie	Price Code: U
Údarás um Chaighdeáin Náisiúnta na hÉireann			

CEN

CWA 15929

WORKSHOP

February 2009

AGREEMENT

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	4
2.	TERMS AND DEFINITIONS	5
2.1.	Definition of a critical information system (CIS).....	5
2.2.	Definition of CIS requirements	6
2.2.1.	General	6
2.2.2.	Integrity	6
2.2.3.	Availability.....	6
2.2.4.	Performance	6
2.2.5.	Capacity.....	6
2.2.6.	Security.....	6
2.2.7.	Maintainability	7
2.2.8.	Resilience	7
2.2.9.	Usability	7
2.3.	Additional comments and specific issues.....	8
3.	GLOBAL MODEL OF CIS REQUIREMENTS	9
3.1.	Overview	9
3.2.	Basic assumptions.....	10
3.3.	Economic dimension	11
3.4.	Interdependencies of requirements.....	13
4.	FUNDAMENTAL PRINCIPLES FOR DESIGNING AND BUILDING A CIS	15
4.1.	Introduction	15
4.2.	Identifying and agreeing upon service priorities with stakeholders.....	16
4.3.	Defining service continuity requirements.....	17
4.4.	Identifying and agreeing upon what should be monitored	18
4.5.	Setting up an iterative process	19
4.6.	Assuming that problems will occur during the Run phase.....	20
4.7.	Setting up a control system.....	21
4.8.	Performing risk and requirement based testing	22
5.	BEST PRACTICES FOR DESIGNING AND DEVELOPING A CIS	23
5.1.	List of best practices	23
5.2.	Mapping practices vs. project phases	24
5.3.	Mapping practices vs. CIS requirements.....	25
6.	ANNEX 1 - Best Practices Sheets.....	26
6.1.	BPS # CIS-01 – Modularity.....	26
6.2.	BPS # CIS-02 – Failure anticipation	28
6.3.	BPS # CIS-03 – Error propagation prevention.....	30
6.4.	BPS # CIS-04 – Bottleneck identification.....	32
6.5.	BPS # CIS-05 – Defensive programming.....	34
6.6.	BPS # CIS-06 – Execution time logging.....	36
6.7.	BPS # CIS-07 – Resource consumption survey	38
6.8.	BPS # CIS-08 – Early capacity planning.....	40

6.9.	BPS # CIS-09 – Industrialized testing	42
6.10.	BPS # CIS-10 – Friends and family probes	44
6.11.	BPS # CIS-11 – Transaction ID	46
6.12.	BPS # CIS-12 – Error case logging	48
6.13.	BPS # CIS-13 – Data timestamping	50
6.14.	BPS # CIS-14 – Service monitoring	52
6.15.	BPS # CIS-15 – Shared log service	54
6.16.	BPS # CIS-16 – Runtime reporting	56
6.17.	BPS # CIS-17 – PKI-based traceability	58
6.18.	BPS # CIS-18 – External security audit	60
6.19.	BPS # CIS-19 – Crisis management	62
6.20.	BPS # CIS-20 – Retention management	64
6.21.	BPS # CIS-21 – Failure mode analysis	66
6.22.	BPS # CIS-22 – Compliance with the relevant standards	68
7.	ANNEX 2 - Life Cycle Processes	70
8.	ANNEX 3 - References	72
9.	ANNEX 4 (informative) - Workshop members	73

CWA 15929:2009 (E)

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.

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

-
- [Looking for additional Standards? Visit Intertek Inform Infostore](#)
 - [Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation](#)
-