Update on Milestone 2

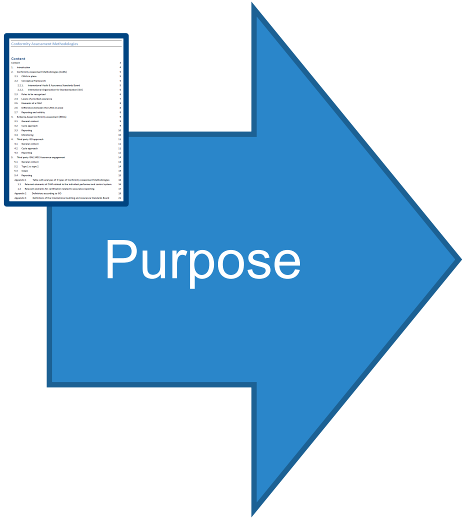
Conformity Assessment Methodologies

Bert Tuinsma MSc RA

Chairman of Zeker-OnLine, Issuer of Trust Certificates for Cloud Services

KEURMERK ZEKER-ONLINE

Conformity Assessment



Conformity Assessment Methodologies

Content

Content 3

1. Introduction 4

2. Conformity Assessment Methodologies (CAMs) 5

2.1 CAMs in place 5

2.2 Conceptual framework 5

2.2.1. International Audit & Assurance Standards Board 5

2.2.2. International Organization for Standardization (ISO) 6

2.3 Roles to be recognized 6

2.4 Levels of provided assurance 7

2.5 Elements of a CAM 8

2.6 Differences between the CAMs in place 8

2.7 Reporting and validity 8

3. Evidence-based conformity assessment (EBCA) 9

3.1 General context 9

3.2 Cycle approach 9

3.3 Reporting 10

3.4 Monitoring 10

4. Third party ISO approach 11

4.1 General context 11

4.2 Cycle approach 11

4.3 Reporting 12

5. Third party ISAE 3402 Assurance engagement 14

5.1 General context 14

5.2 Type 1 vs type 2 14

5.3 Scope 14

5.4 Reporting 15

Appendix 1 Table with analyses of 3 types of Conformity Assessment Methodologies 16

1.1 Relevant elements of CAM related to the individual performer and control system. 16

1.2 Relevant elements for certification related to assurance reporting. 17

Appendix 2 Definitions according to ISO 19

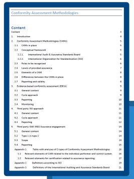
Appendix 3 Definitions of the International Auditing and Assurance Standards Board 21

Purpose

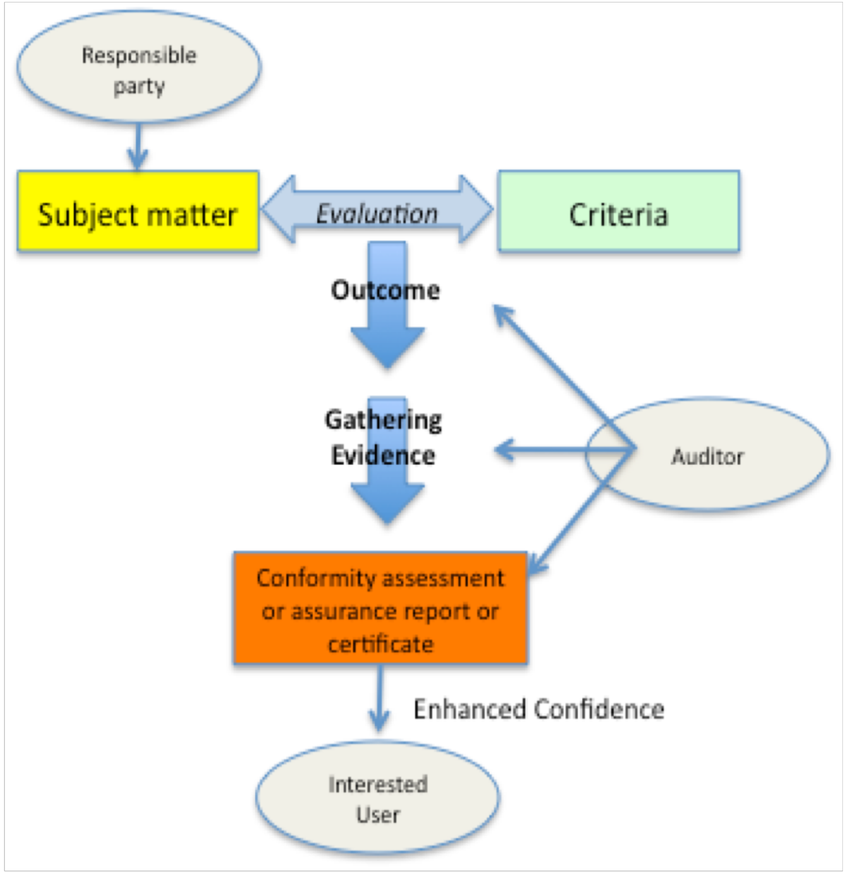
to enhance the credibility (or confidence or trust) towards stakeholders

of a statement expressed by a cloud service provider (CSP) that its cloud process, product or service (including those from sub-service providers) meets the requirements of a pre-defined set of control objectives and a related set of measures, as defined under Milestone 1.

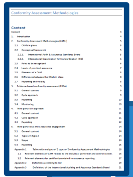
Conformity Assessment



Conceptual Framework



Conformity Assessment



Conformity Assessment Methodologies

Content

Content 3
1. Introduction 4
2. Conformity Assessment Methodologies (CAMs) 5
2.1 CAMs in place 5
2.2 Conceptual framework 5
2.2.1. International Audit & Assurance Standards Board 5
2.2.2. International Organization for Standardization (ISO) 6
2.3 Roles to be recognized 6
2.4 Levels of provided assurance 7
2.5 Elements of a CAM 8
2.6 Differences between the CAMs in place 8
2.7 Reporting and validity 8
3. Evidence-based conformity assessment (EBCA) 9
3.1 General context 9
3.2 Cycle approach 9
3.3 Reporting 10
3.4 Monitoring 10
4. Third party ISO approach 11
4.1 General context 11
4.2 Cycle approach 11
4.3 Reporting 12
5. Third party ISAE 3402 Assurance engagement 14
5.1 General context 14
5.2 Type 1 vs type 2 14
5.3 Scope 14
5.4 Reporting 15
Appendix 1 Table with analyses of 3 types of Conformity Assessment Methodologies 16
1.1 Relevant elements of CAM related to the individual performer and control system. 16
1.2 Relevant elements for certification related to assurance reporting. 17
Appendix 2 Definitions according to ISO 19
Appendix 3 Definitions of the International Auditing and Assurance Standards Board 21

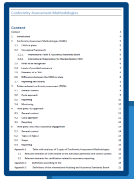
Levels of provided assurance

Three levels of Assurance

- Basic
- Substantial
- High

It’s the user (risk owner) who determines the level of confidence needed for a specific cloud service, taking into account the risk of a failure happening and the impact that would have.

Conformity Assessment



Conformity Assessment Methodologies

Content

Content 3
1. Introduction 4
2. Conformity Assessment Methodologies (CAMs) 5
2.1 CAMs in place 5
2.2 Conceptual framework 5
2.2.1. International Audit & Assurance Standards Board 5
2.2.2. International Organization for Standardization (ISO) 6
2.3 Roles to be recognized 6
2.4 Levels of provided assurance 7
2.5 Elements of a CAM 8
2.6 Differences between the CAMs in place 8
2.7 Reporting and validity 8
3. Evidence-based conformity assessment (EBCA) 9
3.1 General context 9
3.2 Cycle approach 9
3.3 Reporting 10
3.4 Monitoring 10
4. Third party ISO approach 11
4.1 General context 11
4.2 Cycle approach 11
4.3 Reporting 12
5. Third party ISAE 3402 Assurance engagement 14
5.1 General context 14
5.2 Type 1 vs type 2 14
5.3 Scope 14
5.4 Reporting 15
Appendix 1 Table with analyses of 3 types of Conformity Assessment Methodologies 16
1.1 Relevant elements of CAM related to the individual performer and control system. 16
1.2 Relevant elements for certification related to assurance reporting. 17
Appendix 2 Definitions according to ISO 19
Appendix 3 Definitions of the International Auditing and Assurance Standards Board 21

CAMs in place

- Self-assessment
  - Evidence-based conformity assessment
- Third Party Assurance
  - Based upon ISO defined approach
  - Based upon ISAE defined approach
- Continuous Monitoring [in development]

Conformity Assessment

Conformity Assessment Methodologies

Content

Content 3
1. Introduction 4
2. Conformity Assessment Methodologies (CAMs) 5
2.1 CAMs in place 5
2.2 Conceptual framework 5
2.2.1. International Audit & Assurance Standards Board 5
2.2.2. International Organization for Standardization (ISO) 6
2.3 Roles to be recognized 6
2.4 Levels of provided assurance 7
2.5 Elements of a CAM 8
2.6 Differences between the CAMs in place 8
2.7 Reporting and validity 8
3. Evidence-based conformity assessment (EBCA) 9
3.1 General context 9
3.2 Cycle approach 9
3.3 Reporting 10
3.4 Monitoring 10
4. Third party ISO approach 11
4.1 General context 11
4.2 Cycle approach 11
4.3 Reporting 12
5. Third party ISAE 3402 Assurance engagement 14
5.1 General context 14
5.2 Type 1 vs type 2 14
5.3 Scope 14
5.4 Reporting 15
Appendix 1 Table with analyses of 3 types of Conformity Assessment Methodologies 16
1.1 Relevant elements of CAM related to the individual performer and control system. 16
1.2 Relevant elements for certification related to assurance reporting. 17
Appendix 2 Definitions according to ISO 19
Appendix 3 Definitions of the International Auditing and Assurance Standards Board 21

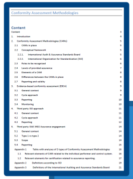
Reporting and validity

- Evidence based: No reporting

- ISO features a full scale 3-year and audit cycle. Result is a certification

- ISAE 3402 Type II is an attestation report on the design, implementation and operating effectiveness over a past period

Conformity Assessment



Conformity Assessment Methodologies

Content

Content 3

1. Introduction 4

2. Conformity Assessment Methodologies (CAMs) 5

2.1 CAMs in place 5

2.2 Conceptual framework 5

2.2.1. International Audit & Assurance Standards Board 5

2.2.2. International Organization for Standardization (ISO) 6

2.3 Roles to be recognized 6

2.4 Levels of provided assurance 7

2.5 Elements of a CAM 8

2.6 Differences between the CAMs in place 8

2.7 Reporting and validity 8

3. Evidence-based conformity assessment (EBCA) 9

3.1 General context 9

3.2 Cycle approach 9

3.3 Reporting 10

3.4 Monitoring 10

4. Third party ISO approach 11

4.1 General context 11

4.2 Cycle approach 11

4.3 Reporting 12

5. Third party ISAE 3402 Assurance engagement 14

5.1 General context 14

5.2 Type 1 vs type 2 14

5.3 Scope 14

5.4 Reporting 15

Appendix 1 Table with analyses of 3 types of Conformity Assessment Methodologies 16

1.1 Relevant elements of CAM related to the individual performer and control system. 16

1.2 Relevant elements for certification related to assurance reporting. 17

Appendix 2 Definitions according to ISO 19

Appendix 3 Definitions of the International Auditing and Assurance Standards Board 21

Elements of a CAM

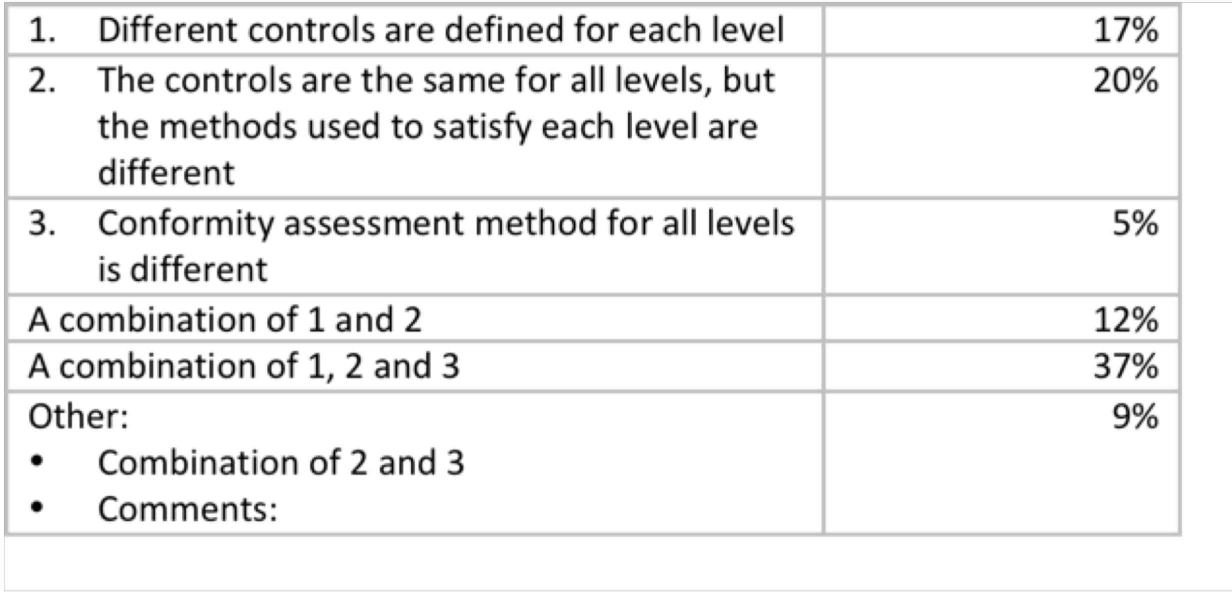
- Independence
- Competency/Expertise
- Professional standards
- Code of conduct
- Qualification
- Accreditation
- Accountability
- Liability
- Monitoring and supervision

Appendix analysis the first three Conformity methodologies

Conformity Assessment

Open consultation

The Cybersecurity Act establishes three levels of assurance (basic, substantial and high). How do you believe that these should be defined?



1. Different controls are defined for each level	17%
2. The controls are the same for all levels, but the methods used to satisfy each level are different	20%
3. Conformity assessment method for all levels is different	5%
A combination of 1 and 2	12%
A combination of 1, 2 and 3	37%
Other: • Combination of 2 and 3 • Comments:	9%

Conformity Assessment

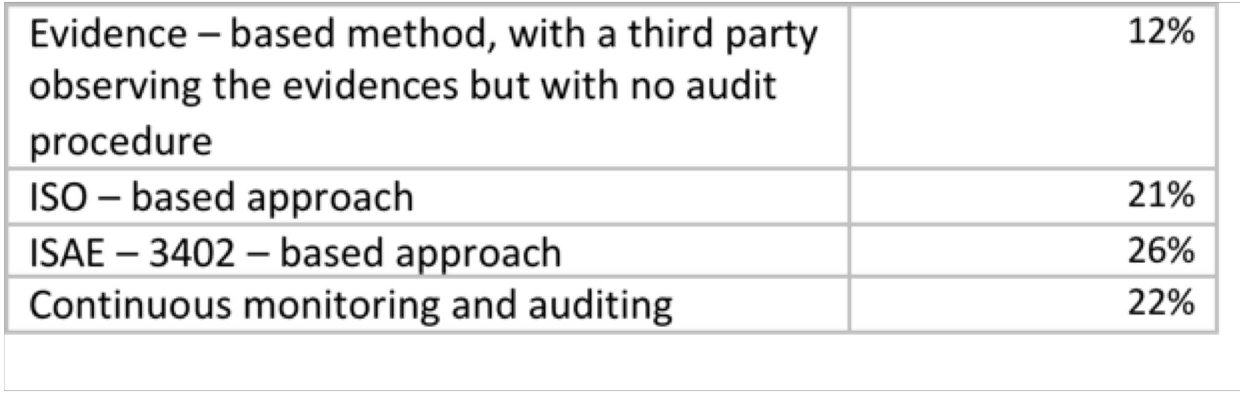
Conformity Assessment Methodologies

Content

Content 3
1. Introduction 4
2. Conformity Assessment Methodologies (CAMs) 5
2.1 CAMs in place 5
2.2 Conceptual framework 5
2.2.1. International Audit & Assurance Standards Board 5
2.2.2. International Organization for Standardization (ISO) 6
2.3 Roles to be recognized 6
2.4 Levels of provided assurance 7
2.5 Elements of a CAM 8
2.6 Differences between the CAMs in place 8
2.7 Reporting and validity 8
3. Evidence-based conformity assessment (EBCA) 9
3.1 General context 9
3.2 Cycle approach 9
3.3 Reporting 10
3.4 Monitoring 10
4. Third party ISO approach 11
4.1 General context 11
4.2 Cycle approach 11
4.3 Reporting 12
5. Third party ISAE 3402 Assurance engagement 14
5.1 General context 14
5.2 Type 1 vs type 2 14
5.3 Scope 14
5.4 Reporting 15
Appendix 1 Table with analyses of 3 types of Conformity Assessment Methodologies 16
1.1 Relevant elements of CAM related to the individual performer and control system. 16
1.2 Relevant elements for certification related to assurance reporting. 17
Appendix 2 Definitions according to ISO 19
Appendix 3 Definitions of the International Auditing and Assurance Standards Board 21

Open consultation

In response to the comparative analysis set out in the linked document, which conformity assessment methods should be applicable in an EU certification framework for cloud services?

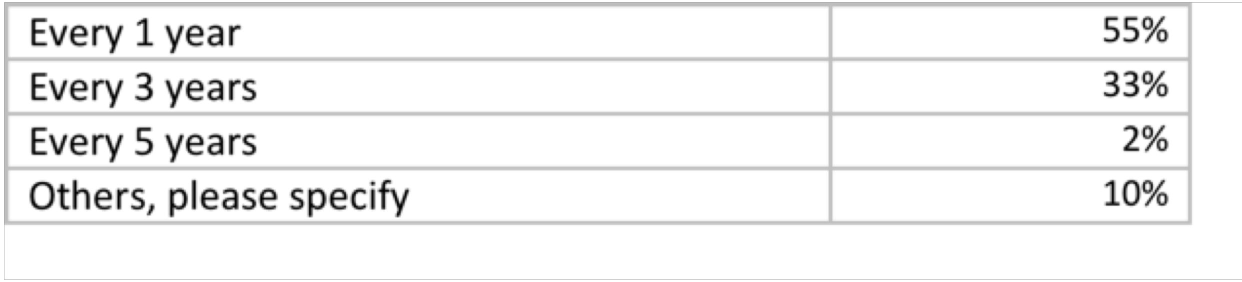


Evidence – based method, with a third party observing the evidences but with no audit procedure	12%
ISO – based approach	21%
ISAE – 3402 – based approach	26%
Continuous monitoring and auditing	22%

Conformity Assessment

Open consultation

Which shall be the recertification period?



Every 1 year	55%
Every 3 years	33%
Every 5 years	2%
Others, please specify	10%

Conformity Assessment

Conformity Assessment Methodologies

Content

Content 3

1. Introduction 4

2. Conformity Assessment Methodologies (CAMs) 5

2.1 CAMs in place 5

2.2 Conceptual framework 5

2.2.1. International Audit & Assurance Standards Board 5

2.2.2. International Organization for Standardization (ISO) 6

2.3 Roles to be recognized 6

2.4 Levels of provided assurance 7

2.5 Elements of a CAM 8

2.6 Differences between the CAMs in place 8

2.7 Reporting and validity 8

3. Evidence-based conformity assessment (EBCA) 9

3.1 General context 9

3.2 Cycle approach 9

3.3 Reporting 10

3.4 Monitoring 10

4. Third party ISO approach 11

4.1 General context 11

4.2 Cycle approach 11

4.3 Reporting 12

5. Third party ISAE 3402 Assurance engagement 14

5.1 General context 14

5.2 Type 1 vs type 2 14

5.3 Scope 14

5.4 Reporting 15

Appendix 1 Table with analyses of 3 types of Conformity Assessment Methodologies 16

1.1 Relevant elements of CAM related to the individual performer and control system. 16

1.2 Relevant elements for certification related to assurance reporting. 17

Appendix 2 Definitions according to ISO 19

Appendix 3 Definitions of the International Auditing and Assurance Standards Board 21

Milestone 3

All comments and answers are being considered when drafting Milestone 3 and the final recommendations for ENISA.

Thanks.