IT Project Guidance

Glossary of IT Specific Terms:   
Certification & Accreditation

Version:

0.2

## Description

A Glossary of common IT Terms -- specifically related to the Certification & Accreditation process -- to establish a common understanding, while reducing duplication of effort in downstream documents.

## Synopsis

Included are the meanings of acronyms and industry terms used during the Certification and Accreditation process.

## Contents

[Description 1](#_Toc150844238)

[Synopsis 1](#_Toc150844239)

[Contents 2](#_Toc150844240)

[Introduction 3](#_Toc150844241)

[Objective 3](#_Toc150844242)

[Terms & Acronyms 4](#_Toc150844243)

[Service Accreditation and Governance Terms & Acronyms 4](#_Toc150844244)

[Accreditation 4](#_Toc150844245)

[ATO 4](#_Toc150844246)

[Authority to Operate 4](#_Toc150844247)

[C&A 4](#_Toc150844248)

[Certification & Assurance 4](#_Toc150844249)

[C&A Memo 4](#_Toc150844250)

[Certification 5](#_Toc150844251)

[Controls Validation Audit 5](#_Toc150844252)

[Control Validation Plan (CVP) 5](#_Toc150844253)

[CVA: 5](#_Toc150844254)

[CVP 5](#_Toc150844255)

[Provisional ATO 5](#_Toc150844256)

[Residual Risks 5](#_Toc150844257)

[Simple Risk 5](#_Toc150844258)

[Security Risk Assessment (SRA) 5](#_Toc150844259)

[SRA 6](#_Toc150844260)

[SRMP 6](#_Toc150844261)

[STA 6](#_Toc150844262)

[System Threshold Analysis (STA) 6](#_Toc150844263)

[Appendices 7](#_Toc150844264)

[Appendix A - Document Information 7](#_Toc150844265)

[Versions 7](#_Toc150844266)

[Images 7](#_Toc150844267)

[Tables 7](#_Toc150844268)

[References 7](#_Toc150844269)

[Review Distribution 7](#_Toc150844270)

[Audience 7](#_Toc150844271)

[Diagrams 7](#_Toc150844272)

## Introduction

## Objective

To develop a common understanding of terms used to deliver services with an IT component.

# Terms & Acronyms

## Service Accreditation and Governance Terms & Acronyms

#### Accreditation

: the formal acceptance of the residual risks posed by a solution and grants permission -- from a security perspective -- for that solution to operate.   
The risks considered include system and environment risks, but also operation risks (lack of maintenance documentation, establishment of support channels, etc.)

The risk acceptance is then done in 2 parts:

1. the Business Owner accepts the risks on behalf of their business unit,
2. the Accrediting Authority (i.e., the *CISO*) accepts the risks on behalf of the Organisation.

Note: For the organisation the certification sign-off is combined with the accreditation as part of the *C&A Memo*.

#### ATO

: see *Authority to Operate*.

#### Authority to Operate

: what a CAB provides to a system when it has determined that all relevant stakeholders are satisfied with the system going live.  See *Provisional ATO*.

#### C&A

: see *Certification & Accreditation.*

#### Certification & Assurance

: the process which a Security Specialist follows to ensure:

* the system’s data classification has been obtained,
* a PTA/PIA has been developed and signed off on,
* a technical assessment of the system (generally involving a Pen test)
* (optionally) an S*TA* for the solution and develop
* the C&A document circulated for signature on behalf of a project before it is presented to the CAB board, along with evidence that the ASG, SSP, DI, TSR have been accepted.

#### C&A Memo

: the outcome of the C&A process.

Summarises:

* the business purpose of the solution (see *SAD*)
* the activities undertaken
* the state of the control environment (see *CVA*)
* the residual risk profile
* any remedial work required to address control deficiencies (see *CVP*).
* formally requests certification and accreditation until a specified date.

See *Provisional ATO*.

#### Certification

: issued by the Certifying Authority to signify a robust security design, build, and assessment process has been completed; and that as a result the residual risk statements are a fair reflection of the risks posed by the solution.

#### Controls Validation Audit

: once the CVP’s defined risk controls are built and implemented, the CVA establish their effectiveness by testing them according to the CVP’s instructions.

#### Control Validation Plan (CVP)

: identifies the key Security Risk Assessment (SRA) controls that must be operating effectively to mitigate risks to an accepting level, *and the method by which they will be tested*.

Developed and made available to the project right after the initial SRA is completed, so that developers can implement the controls. See *Simple Risk*.

#### CVA:

See *Controls Validation Audit.* See *Simple Risk.*

#### CVP

: see *Control Validation Plan*.

#### Provisional ATO

: CAB may recommend a Provisional ATO be provided to a service, tied to caveats for tasks to be complete subsequently.

#### Residual Risks

: risks remaining after a *Control Validation Plan* has been developed, implemented and audited (via an *Control Validation Audit*). See *Simple Risk*.

#### Simple Risk

: the combination of the CVA and Residual Risk.

#### Security Risk Assessment (SRA)

: during the design phase, the Security Consultant identifies and assesses the cyber security concerns based on several inputs – Solution Architecture Design (SAD) (from which the business purpose and context, information involved, and intended audience can be determined), Privacy concerns (PTA/PIA); workshops; environmental/external factors.

The design’s mitigating controls are considered.

Mitigating controls to address the remaining identified risks are selected from the organisation’s control catalogue, which is based on NZISM and the Secure Controls Framework (SCF).

The output of this assessment is then documented in a SRA.

A CVP is prepared immediately.

*Note: Replacing the older STA approach.*

#### Security Risk Management Plan

:

identifies any remedial activities required to address control deficiencies found during the CVA & TSA.

#### SRA

: see *Security Risk Assessment*.

#### SRMP

*: see security Risk Management Plan.*

#### STA

: see *System Threshold Analysis*

#### System Threshold Analysis (STA)

: [no longer used]. A document prepared by a Security Specialist during the C&A process. The NZISM based process is about determining and measuring risks, along with proposed technical or procedural mitigations, and define what remains: the residual risk.    
This assessment is what is signed of on in the C&A process.

Appendices

Appendix A - Document Information

### Authors & Collaborators

Author: Sky Sigal, Solution Architect

### Versions

* 1. Initial Draft
  2. Minor corrections

### Images

**No table of figures entries found.**

### Tables

**No table of figures entries found.**

### References

**There are no sources in the current document.**

### Review Distribution

The document was distributed for review as below:

|  |  |
| --- | --- |
| Identity | Notes |
| Sandy Britain, Enterprise Architect |  |
| Amy Orr, Data Architect |  |
| Roger Govind, Security Architect |  |
| Archana Sahani, Business Analyst |  |
| Dijana Sneath, Business Analyst |  |
| Vincent Weirdsma, Lead Developer |  |

### Audience

The document is technical in nature, but parts are expected to be read and/or validated by a non-technical audience.

### Diagrams

Diagrams are developed for a wide audience. Unless specifically for a technical audience, where the use of industry standard diagram types (ArchiMate, UML, C4), is appropriate, diagrams are developed as simple “box & line” monochrome diagrams.