



<b>Date:</b>	Jan.'24	<b>Release:</b>	Publication
<b>Author:</b>	Corp.Sec.		
<b>Owner:</b>	CyberDefenceDynamics		
<b>Document Number:</b>	POLMAN_QA		


## Revision History

### Date of next review

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
05/01/22	01/07/21	Structural adjustment	
07/01/23	05/01/23	Verification	
09/01/24	07/01/23	Verification and validity checks.	

## Approvals

This document requires the following approvals. A signed copy should be placed in the project files.

Name	Signature	Title	Date of Issue	Version
D.Strudwick		Managing Director	09/01/24	1.02

## Purpose

This policy is designed to ensure that CDD operates a quality controlled and properly benefiting audit and process assurance policy that provides meaningful results that can be acted upon and constitutes part of a library of other business related process policy including:

- Safety Criticality in Software Engineering
- Health and Safety
- Ethics and Behaviours
- Cyber Security & Contingency Planning
- Environmental and Energy
- Government Security Management
- Special Projects
- Board Management
- Equality Diversity
- Development Policy
- Commercial Contractual Engagement
- Commercial/Professional Insurance

# Quality Assurance & Audit Overview

**Contents** *The areas encompassed by the policy include the following topics.*

Executive Summary.....	2
Background and approach.....	2
Existing risk and assurance practices and requirements.....	2
Application and Benefit of the Quality Assurance and Audit Policy.....	3
Driving measurable value and benefits.....	3
Addressing concerns with pragmatic solutions.....	3
Timelines, Resource Engagement and Other Adjustment .....	4
Setting the Audit Requirements.....	4
Impactful Reports.....	5
Overall QA&A Review.....	5

**Advice** *The policy is designed to provide a flexible an efficient approach to the business' processes and product development, but this provides the foundation to product excellence and efficiency, but only unless it is followed.*

---

## **Executive Summary**

The approach to quality assurance (as an integral part of systems and service design & development integrated within the audit process) is designed to ensure the integrity of engineering quality enshrined within the process as a whole.

## **Background and approach**

The approach to the business' audit function is intended to provide as light-touch on the processes of quality controlled service provision and software development.

The principle concept is that it is easier to undertake the work correctly the first time, and to make sure things are right, before moving on, than to make repeated iterations around the design cycle, recovering from errors or omissions, that may otherwise impede rapid developmental progress.

## **Existing risk and assurance practices and requirements**

The assessment of risk is undertaken in the following areas of business process approaches including the following:

- Cyber Security (which describes CDD's outline information practices)
- Government Security Management
- Development Policy

Technical risk management and addressed in the technical approach including the following instruments:

- Project Risk Report & Management Strategy
- Design Options Verification (TWINDA)
- Interoperability + Process Integrity
- Coding and Data Verification

## **Application and Benefit of the Quality Assurance and Audit Policy**

The policy provides an approach whereby all the various strands of process output can be pulled together into a coherent report attracting considerable impact to the process of obtaining a proper and fair overview of the matters under consideration.

### **Driving measurable value and benefits**

It is essential that CDD's service product and design and development processes do in fact give rise to demonstrably assurable output. This is largely achieved by the judicious application of PASCAL and Peddle. There is a third class of activities described in the Ethical and Development Framework(EDF) which is applied to advanced research programmes.

The following areas constitute the EDF and are fully described in the development and test harness with TheBrain and PASCAL materials (i.e. Project Activity Log[PAL] instrument).

- Accuracy, Recursion and Explanation
- Algorithmically Constrained Generalization
- Composition & Control
- Scale Elasticity
- Chronometric Analytics
- Transparent Interoperability
- Legacy Architecture and Interoperability
- Legal Liability, Accountability and Responsibility
- Limitation and Adaptation
- Model and System Composition
- Model Security and Trustworthiness
- Operational Impact Analysis <sup>1</sup>

The necessary instruments therefore exist to form the basis of measurable benefits arising from the developmental processes.

### **Addressing concerns with pragmatic solutions**

Where concerns arise from the project board or the client (such as to the chosen technical developmental approach), it is essential that a development approach can be properly examined and can either provide direction to the project in terms of adjustments determined to be necessary. A revised risk assessment can be undertaken and all issues having arisen can also be addressed.

---

<sup>1</sup> It should be noted that not all of the above activities are appropriate for all programmes, however, processes exist to provide required results.

## **Practical implementation challenges**

The main area of implementation is found in the provision of technical services to clients, the undertaking of both internally and externally funded research and the subsequent development and preparation of products.

The principal quality control processes include:

PASCAL -

- Communications Management Strategy
- Project Quality Management Strategy
- Project Configuration Control Strategy

PEDDLE -

- Requirements Engineering
- System Design Options Analytics
- Underpinning Design Architecture Analysis
- Project Modularity and Logical Arrangement
- Coding Standards and Application Design Preparation
- Design Options Verification (TWINDA)
- Requirements Verification and Sanity Assurance
- Design Ethics, System Safety and Legality
- Operational Design Architecture Verification
- Modularity and Logical Design Verification
- Coding and Data Verification

These are the subject of specific technical policy control instruments.

## **Timelines, Resource Engagement and Other Adjustment**

The quality audit and assurance approach can examine the resources allocated to a programme of work and all documents relating to the work (and output in terms of technical product) can and must be made available to the examining board.

## **Setting the Audit Requirements**

It is essential that the audit requirements align with the system requirements can best be established properly and meaningfully.

It is unlikely that an audit will descend to individual code or data species level, but the capability exists. What is much more likely is that requirements, their feasibility, the most appropriate technical approach to their achievement and discharge during overall implementation and verification has been undertaken.

There are a number of instruments that take these matters into account including:

PASCAL

- Project Brief
- High-Level Product Description

## **Quality Assurance & Audit**

- Modular-Level Product Description
- Project Configuration Control Strategy

### PEDDLE

- Advanced Project Brief
- Programme/Project Quality Criteria & Metrication
- Requirements Engineering
- Requirements Verification and Sanity Assurance
- System Design Options Analytics
- Project Modularity and Logical Arrangement
- Requirement Feasibility Analytics
- Technical Research Analytics

## **Impactful Reports**

The resulting quality assurance and audit processes are fully accommodated by the preparation of appropriate information as progressing through the normal product preparation, design and development processes.

These are generally based on data that is accessible in .xls format (therefore no special processing or skills are required to access or manipulate the information).

## **Overall QA&A Review**

This is undertaken on an annual basis to ensure of its validity and to uncover any necessity for update on an *ad hoc* basis.