

SAIMC CPD Verification Process (VSP Verification)

Version 1.0

This is the formal process SAIMC NPC follows to verify **CPD Service Providers (VSPs)** in accordance with the ECSA CPD Framework

Table of Contents

Verification Process (VSP Verification)	1
Version 1.0	1
1 Purpose of Verification	3
2 Overview of the Verification Workflow	3
3 Detailed Verification Steps	3
3.1 Step 1 — Submission of Application (ECPD7)	3
3.2 Step 2 — Administrative Completeness Check	4
3.3 Step 3 — Technical Assessment	4
3.4 Step 4 — Site Visit (If Required)	4
3.5 Step 5 — Verification Outcome	5
1. Verified	5
2. Verified with Recommendations	5
3. Declined	5
3.6 Step 6 — Issuing of Verification Number	5
3.7 Step 7 — Record-Keeping and Reporting	6
4 Verification Validity	6
5 Monitoring of Verified Providers	6
6 Why This Process Matters	7
Verification Decision Tree	8
1 Step 1 — Does the provider fall within SAIMC NPC’s scope?	8
2 Step 2 — Is the provider’s QMS evidence adequate?	8



SAIMC NPC

2010 / 014 751 / 08

Tel: +27 (0) 11 312 2445
e-mail: ina@saimc.co.za
Address: Postnet Suite # 002
Private Bag X59, Halfway House,
1685
Website: www.saimc.co.za

3	Step 3 — Does the provider demonstrate capacity to deliver high-quality CPD?.....	9
4	Step 4 — Is a site visit required?.....	9
5	Step 5 — Are all presenter requirements met?	10
6	Step 6 — Are all legal and compliance documents valid?	10
7	Step 7 — Final Verification Decision	10
8	Step 8 — Record-Keeping & Monitoring	11
9	Verification Decision Tree (Text Summary).....	11

1 Purpose of Verification

Verification ensures that any organisation wishing to offer CPD Category 1 activities:

- Has the **capacity, competence, and systems** to deliver high-quality training
- Meets the **minimum requirements** set by ECSA
- Operates within a **controlled, auditable framework**
- Can be trusted to uphold the professional standards of the engineering community

Verification is **mandatory** before a provider may submit any CPD activities for validation.

2 Overview of the Verification Workflow

The SAIMC NPC verification process consists of seven controlled steps, each documented and auditable.

3 Detailed Verification Steps

3.1 Step 1 — Submission of Application (ECPD7)

The prospective CPD Service Provider submits:

- Completed **ECPD7** form
- Company profile
- Responsible person details
- Scope of CPD activities
- Registration category, discipline, and area of specialisation
- Valid SARS tax clearance
- Company registration certificate
- Evidence of a **Quality Management System**
- Agreements and contingency plans (if applicable)

This is supported by the QMS text:

“The CPD Service Provider application form (Form ECPD7) must be accompanied by all the required documents.”

3.2 Step 2 — Administrative Completeness Check

SAIMC NPC checks that:

- All required documents are present
- All fields in ECPD7 are completed
- Supporting evidence is valid and current

If incomplete, the application is returned with a request for outstanding items.

3.3 Step 3 — Technical Assessment

The SAIMC NPC assessor evaluates:

- The provider's organisational capacity
- The competence of the responsible person
- The scope of CPD developmental activities
- The provider's internal QMS
- Agreements and contingency plans
- Evidence of ability to deliver high-quality training

This aligns with:

“The SAIMC will assess the documentation and arrange for a site visit if necessary.”

3.4 Step 4 — Site Visit (If Required)

A site visit is conducted when:

- The provider is new
- The scope is complex
- The QMS evidence is insufficient
- Facilities need to be inspected

The visit verifies:

- Training facilities

- Equipment
 - Administrative systems
 - Attendance tracking mechanisms
 - Presenter support systems
-

3.5 Step 5 — Verification Outcome

The SAIMC NPC issues one of three outcomes:

1. Verified

Provider meets all requirements.

2. Verified with Recommendations

Minor issues exist but do not prevent verification.

Provider must address recommendations within a specified timeframe.

3. Declined

Provider does not meet the minimum requirements.

This is supported by:

“The outcome will be: Verified, Verified with specific recommendations, or Declined.”

3.6 Step 6 — Issuing of Verification Number

If verified, SAIMC NPC:

- Generates a unique verification number
- Records it in the Microsoft database
- Issues a formal verification letter
- Stores all documents in OneDrive for audit purposes

This satisfies ECSA’s requirement for:

- A documented numbering system
- A database containing VSP approvals, recommendations, and rejections

3.7 Step 7 — Record-Keeping and Reporting

All verification records are stored in:

- **Microsoft database** (structured data)
- **OneDrive filing system** (documents, evidence, letters, agreements)

Records include:

- ECPD7 form
- Supporting documents
- Assessment notes
- Site visit reports
- Verification outcome
- Verification number
- Correspondence

This aligns with:

“Records must be kept... The documentation used for the events... The presenters... The assessments results... Validity dates...”

4 Verification Validity

Verification is valid for three years, provided:

- No material changes occur
- No quality issues arise
- The provider remains compliant with ECSA requirements

If changes occur (e.g., new QMS, new ownership, new training scope), the provider must be re-verified.

5 Monitoring of Verified Providers

SAIMC NPC monitors verified providers by:

- Reviewing validated activities

- Checking attendance registers
- Reviewing feedback forms
- Conducting random audits
- Responding to complaints
- Requiring re-verification if quality issues arise

This ensures ongoing compliance and protects the integrity of the CPD system.

6 Why This Process Matters

ECSA expects Licensed Bodies to:

- Apply consistent, documented, auditable processes
- Maintain a database of all VSPs
- Ensure only competent providers deliver CPD activities
- Protect the engineering profession from low-quality training

The SAIMC NPC verification process meets all these requirements.

Verification Decision Tree

START

— Has the provider submitted a complete ECPD7 application?

If NO →

Outcome: “Application Incomplete”

Send request for outstanding documents.

Stop process until complete.

If YES →

Proceed to Step 1

1 Step 1 — Does the provider fall within SAIMC NPC’s scope?

(Mechatronics, Automation, Instrumentation, Control Systems, Measurement Systems, Enterprise Integration Practitioner)

If NO →

Outcome: “Declined – Outside SAIMC NPC Scope”

Refer provider to appropriate Licensed Body.

If YES →

Proceed to Step 2

2 Step 2 — Is the provider’s QMS evidence adequate?

(QMS document, procedures, attendance tracking, certification, feedback, contingency plans)

If NO →

Outcome: “Verified with Recommendations – QMS Improvements Required”

Provider must submit corrective evidence before validation of any activities.

If YES →

Proceed to Step 3

3 Step 3 — Does the provider demonstrate capacity to deliver high-quality CPD?

(Training facilities, presenter competence, administrative systems)

If NO →

Outcome: “Declined – Insufficient Capacity”

Provider may reapply once capacity is improved.

YES →

Proceed to Step 4

4 Step 4 — Is a site visit required?

Required if:

- New provider
- Complex scope
- Weak QMS evidence
- High-risk activities
- Unclear facilities or systems

If YES →

Conduct Site Visit

After visit:

- If satisfactory → Proceed to Step 5
- If unsatisfactory → “Verified with Recommendations” or “Declined”

If NO →

Proceed to Step 5

5 Step 5 — Are all presenter requirements met?

(CV, certified ID, experience, availability confirmation)

If NO →

Outcome: “Verified with Recommendations – Presenter Documentation Required”

If YES →

Proceed to Step 6

6 Step 6 — Are all legal and compliance documents valid?

(SARS tax clearance, CIPC registration, agreements, contingency plans)

If NO →

Outcome: “Application On Hold – Compliance Documents Missing/Expired”

If YES → Proceed to Step 7

7 Step 7 — Final Verification Decision

If all criteria met →

Outcome: “Verified”

- Generate verification number
- Record in database
- Issue verification letter
- File all documents in OneDrive

If minor issues exist →

Outcome: “Verified with Recommendations”

- Provider may operate but must correct issues within defined timeframe

If major issues exist →

Outcome: “Declined”

- Provide written reasons
- Provider may reapply after corrective action

8 Step 8 — Record-Keeping & Monitoring

Regardless of outcome:

- Store ECPD7, supporting documents, assessment notes, and decision letter
- Update Microsoft database
- File evidence in OneDrive
- Add provider to monitoring schedule

9 Verification Decision Tree (Text Summary)

Decision Point	Yes →	No →
Complete ECPD7?	Step 1	Incomplete – stop
Within SAIMC scope?	Step 2	Declined
Adequate QMS?	Step 3	Verified w/ Recommendations
Capacity adequate?	Step 4	Declined
Site visit needed?	Visit	Step 5
Presenter requirements met?	Step 6	Verified w/ Recommendations
Compliance documents valid?	Step 7	On Hold
Final decision	Verified	Declined / Recommendations