Terminal Quality Management Requirements

Version 3.0 – September 2022

Notices

Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both.
This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department.
All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document shall not infringe any third party patents, copyrights, trade secrets or other rights.

Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document shall take precedence over any translated version in any legal proceeding.

Information Available Online	Mastercard provides details about the standards used for this document, including times expressed, language use, excerpted text and contact information on the Publications Support page available on Mastercard Connect®. Go to Support for centralized information.
Assessment Body	Contact with the Assessment Body should be made through: Mrs Alex Stokes TÜV SÜD - Product Service Division TUV SUD Ltd Octagon House Concorde Way Segensworth North Fareham Hampshire PO15 5RL United Kingdom E-mail: Mastercard.TQM@tuv-sud.co.uk

Table of Contents

1 Introduction

This chapter contains information that helps you understand and use this document.

1.1 Scope

This document describes the Mastercard specific requirements that a **Vendor** shall comply with to obtain a Terminal Quality Management Label (**TQM Label**) for contact and contactless **products**.

The compliance to these requirements is assessed during the TQM process. A **TQM Label** is granted at the end of this process. This process is defined in the Terminal Quality Management – Process [TQM/GEN/T01].

1.2 Audience

This document is intended for **Vendors** who wish to obtain a Terminal Quality Management Label.

1.3 Language Use

This document uses U.S. English spelling and grammar rules. Exceptionally, the local English spelling is used for proper nouns.

Verbal Forms: In this document, the following verbal forms are used:

— “shall” indicates a requirement;
— “should” indicates a recommendation;
— “may” indicates a permission;
— “can” indicates a possibility or a capability.

1.4 Related Information

The following reference materials may be of use to the reader of this document:
Mastercard Information:

- Terminal Quality Management – Process [TQM/GEN/T01]
- Terminal Integration Process Guide (EMV and Contactless)

ISO standards:

- ISO 9001:2015: Quality management systems - Requirements
- ISO 10007: 2017: Quality management - Guidelines for configuration management
- ISO 19011: 2018: Guidelines for auditing management systems

Other reference materials are listed in the "Technology-specific Terminology and Information" section in the Appendices.

The use of an acronym, abbreviation or definition is shown in **Bold**, its meaning is described in the Appendices.

Information marked as "NOTE" is for guidance in understanding or clarifying the associated requirement.

1.5 Revision

The information in this document supersedes and replaces all previous versions (including drafts) issued.

Information in this document is subject to change. Any such changes shall update the current version of the document.

1.6 Terminal Quality Management (TQM)

Mastercard has developed and relies on comprehensive test and approval processes for **products** in order to promote world-wide interoperability at an acceptable time and cost to all parties.

The objective of these processes is to ensure that each terminal: *Operates Everywhere, Every time*

One of these processes is the Terminal Type Approval Level 1 (EMVCo **TTA L1**). During EMVCo **TTA L1**, the **IFM** or the **PCD** is tested against the related **Technical Specifications**.

Another process is Terminal Quality Management (TQM) that is Mastercard's way of ensuring that samples received for EMVCo **TTA L1** Test are:

- Representative: ensuring that the samples are valid examples of the **product** which has been designed.
- Repeatable: ensuring that the samples are valid examples of the **product** which is to be delivered in production volumes in the future.
- Reliable: ensuring that evolutions of the tested **product** remain compliant with **Technical Specifications**.

TQM defines in this document, a set of requirements **Vendors** shall meet. Meeting these requirements results in the granting of a **TQM Label**. The **product TQM Label** is mandatory for Acquirers going through Mastercard's Terminal Integration Process (M-TIP).

These requirements mandate the **Vendor** to operate a **Configuration Management System** to:

- Define and follow the configuration of its **Products** and the impact of changes on their compliance with the relevant **Technical Specifications** throughout their life cycle.

The purpose is to obtain confidence that any **Products** used in the field and embedding a **PCD** or an **IFM** that has successfully passed Terminal Type Approval Level 1 remains compliant with the **Technical Specifications**.

The scope of the auditing activities associated with this scheme extends to the **configuration management** by **Vendors** for all elements of a **product** in which an **IFM** or **PCD** is embedded, including the elements of a **product** that have been tested by EMVCo or Mastercard (L2 requirements).

Vendors shall declare in which **Products** their **IFM**s and **PCD**s are to incorporated/integrated.

Note: The **configuration management** of L2 software is within the scope of TQM. The **configuration management** of L2 software will not be assessed during a TID or VOD review but shall be within the scope of a TQM audit.

1.7 TQM Process

The TQM label application, assessment and audit process is defined in TQM/GEN/T01.

1.7.1 TID Submission

A **Vendor** submits a TID questionnaire plus supporting documents for every **IFM** or **PCD**, the TID

- Describes the EMVCo Level 1 type approval configuration
- Describes the current configuration including where revisions have been made (See change control)
- List of the payment terminals (**Products**) embedding the **IFM**/**PCD**

TIDs are submitted when an **IFM** or **PCD** is entered into the scheme, the TID is resubmitted and reassessed when:

- TQM relevant changes are made to the payment terminal (**product** in which **IFM** / **PCD** are integrated, see change control)
- An **IFM** or **PCD** is changed or updated (See change control)
- When any other relevant changes are made

The TID records the manufacturing documentation of the payment terminal (for which **IFM** / **PCD** are integrated). The information within the TID shall be subject to audit.

Note: An example of the TID documentation is listed in the "Guide to the required TID documents" appendix of this document.

1.7.2 VOD Submission

The **Vendor** submits a VOD questionnaire plus supporting documents describing their TQM **configuration management system** and the implementation of the requirements of this document within their QMS.

Note: An example of the VOD documentation is listed in the "Guide to the required VOD documents" appendix of this document.

The VOD is submitted when an **IFM** or **PCD** is initially entered into the scheme and shall be resubmitted and reassessed when any changes occur (refer to TQM/GEN/T01, TQM Questionnaire Completion).

The information within the VOD shall be subject to audit.

1.7.3 ODM / OEM Components Submissions

TQM defines two types of component submissions.

The **TQM label** is issued to the party (**Vendor**) to whom the Level 1 **LoA** is issued and referenced on the EMVCo website.

1.7.3.1 Configuration / Assembly control

Vendors who utilise an **OEM product** and are responsible for the final assembly, maintenance of configurable **items**, software loading or personalization of the **products** are required to submit, as a minimum, the following documents to support their TQM application:

- Documented processes and procedures demonstrating the **Vendor's** control of the design, **configuration management** and on-going TQM compliance of the **OEM** components

Vendors who utilise an **OEM product** and are responsible for the final assembly, maintenance of configurable **items**, software loading or personalization of the **products** shall facilitate Mastercard audits at all of the **OEM** premises (Design and Manufacturing) as well as all of the appropriate Vendor facilities (Manufacturing) to ensure on-going compliance.

Note: These requirements are in addition to all other TID and VOD supporting documentation

1.7.3.2 Off the shelf purchase

Vendors who utilise an **ODM product** and have no responsibility for final assembly, maintenance of configurable **items**, software loading or personalization of the **products** shall be required to submit documentation to demonstrate contractual agreements between them and the **ODM** manufacturer to verify:

- They have no direct control of the configuration or maintenance of compliance for the **product**
- Ensure that the **ODM** maintains the compliance of the **IFM**(s) / **PCD**(s) with the EMVCo Level 1 type approval configuration & Level 2 kernel
- Ensure that the **ODM** maintains the compliance of the **IFM**(s) / **PCD**(s) with the EMVCo Level 2 kernel

The **Vendor** shall hold records of the hardware and software configuration at EMVCo L1 approval as well as all configuration changes of the **IFM**(s) / **PCD**(s) from the **ODM**.

Vendors who have no control of the configuration or maintenance of compliance for a **product** shall be required to have a statement of compliance issued on an annual basis.

Vendors who have no control of the configuration or maintenance of compliance for a **product** shall facilitate Mastercard audits at all of the **ODM** premises (Design and Manufacturing), to ensure on-going compliance.

1.8 Supporting Standards

TQM requirements are based on two international series of standards:

- ISO 9001:2015 for its system management principles.
- ISO 10007:2017 for its configuration management principles.

1.9 Management System Requirements

Vendors applying for TQM approval shall ensure that the appropriate sites and organisations hold one of the following for design, manufacturing and **service** activities that are within the scope of the approval:

- ISO 9001:2015 certification
- TL 9000 Release 6 certification
- IATF 16949:2016 certification

This certification shall be accredited by a National Accreditation Body that is a signatory to the IAF MoU (http://www.iaf.nu//articles/IAF_MEMBERS_SIGNATORIES/4)

Note: Refer to TQM/GEN/T01 V3.0 clause 4.5.2 for **Vendors** without ISO 9001 (or equivalent) certification.

1.10 Configuration Management Principles

Configuration management principles provide structure for managing identification and **traceability**, the status of its physical and functional requirements and access to accurate information in all phases of the life cycle.

Configuration management (as defined in ISO 10007:2017) is based on four activities:

- **Product Configuration Identification**: identify and document the functional and physical characteristics of **Configuration Items (CIs)**.
- **Product Change Control**: control changes to CIs and their related documentation.
- **Product** Configuration Status Accounting: record and report information needed to manage CIs effectively, including the status of proposed changes and the implementation status of approved changes.
- **Product Configuration Audit**: audit the CIs to verify conformance to specifications, **interface** control documents and other requirements.

1.11 Configuration Management System (CMS)

TQM defines requirements for a **Configuration Management System** for **Products** that are or are intended to be used within the Mastercard payment network.

An organization that adopts the above approach (See **Management System** Requirements and Configuration Management Principles) creates confidence in the capability of its processes and the configuration management of its **products** and provides a basis for continual improvement.

Note: It is not a requirement of TQM that a **Vendor** fully implements the requirements of ISO 10007:2017.

1.12 Audit of the TQM Requirements

Every **product** included in **TQM label**(s) shall be subject to audit by Mastercard to these requirements.

Each **Vendor** audit shall include the **configuration management** controls for both L1 hardware and software as well as L2 software for each approved **Product** or **Implementation**.

The audit process is described in TQM/GEN/T01.

1.13 TQM Requirements Overview

The following paragraphs provide an overview of each chapter of these requirements.

1.13.1 Management Responsibility

This chapter defines management requirements for the **Vendor** in order to obtain its commitment to develop, implement, maintain and improve on meeting TQM requirements.

- Management commitment
- Configuration management policy
- Configuration management planning
- Responsibility and authority
- TQM Manager
- **Approval Authority**
- Management review
- **Supplier** Management
- **Product** release and **service** delivery

1.13.2 Operation

This chapter defines the general requirements applicable to managing TQM activities.

- Documentation requirements
- Resource management
- **Supplier** management
- Organizational interface management
- Customer communication

1.13.3 Product Design

This chapter defines the requirements for the management of the **Product**'s design.

- General requirements
- **Product configuration management**
- **Configuration Identification**
- **Configuration Information**
- Naming and numbering conventions
- Configuration baselines
- Component Identification
- Requirements for assessing alternative components
- Change control
- **Product** Configuration Status Accounting

The **Vendor** shall perform audits to determine if the **Product** Design process is operated correctly and efficiently. These audits shall lead to analysis and preventive and corrective actions in order to improve the **Product** Design processes including **configuration management**.

1.13.4 Manufacturing and Service

This chapter defines the requirements for manufacturing and servicing a **Product** from a **Vendor** control perspective as well as the perspective of the facility or organization carrying out the activities.

Manufacturing (**Vendor** responsibilities)

- Manufacturing control
- Validation of processes for manufacturing
- Control of nonconforming product
- Minimum requirements for final testing of **Products** and **Implementations**

Manufacturing (**Manufacturer** responsibilities)

- General Responsibilities
- Control of documents and records
- Internal audit
- Control of changes
- Monitoring and measurement
- Control of nonconforming product
- Purchasing
- Competence
- Complaints, nonconformity and corrective action
- Manufacturing control

Post manufacturing **service** provisions (**Vendor** responsibilities)

- Repair levels
- **Service** site categorization
- **Service** site controls

Post manufacturing **service** provisions (**Service** facility responsibilities)

- General Responsibilities
- Control of documents and records
- Internal audit
- Control of changes
- Purchasing
- Competence
- Complaints, nonconformity and corrective action
- **Service** control

1.13.5 Measurement, Analysis and Improvement

This chapter defines requirements for the implementation of processes for measurement, analysis and improvement of the **product** design processes including **configuration management**.

- General requirements
- Interoperability Issues
- Internal audit
- Monitoring and measurement of configuration processes
- Monitoring and measurement of **Product** Configuration
- Control of Nonconforming Product
- Analysis of data
- Continual improvement
- Feedback Process on TQM Compliance

2 Management Responsibility

2.1 Management Commitment

Top management shall provide evidence of its commitment to the development, implementation, maintenance and improvement of the TQM system requirements:

- Communicating to the organization the importance of meeting these TQM requirements
- Establishing the configuration management policy
- Ensuring that measurable configuration management objectives are established
- Conducting management reviews
- Ensuring the availability of resources.

Note 1
Configuration management objectives should be **SMART** (See the Terminology Appendix)

Note 2
Configuration management objectives should include improvement of the effectiveness of the **Configuration Management System**, improvement of the effectiveness of the TQM processes, improvement of **Product** interoperability, improvement of **Product configuration identification** and when necessary, resources.

2.2 Configuration Management Policy

Top management shall ensure that the configuration management policy:

- Is appropriate to the purpose of the organization
- Includes a commitment to comply with these requirements (TQM/GEN/T02)
- Includes a commitment to continually improve the effectiveness of the **configuration management system**
- Provides a framework for establishing and reviewing configuration management objectives
- Is communicated and understood within the organization
- Is reviewed for continuing suitability.

2.3 Configuration Management Planning

Top management shall ensure that:

- Planning of **configuration management** is carried out in order to meet TQM requirements.
- The integrity of **configuration management** is maintained when changes to the **configuration management system** are planned and implemented.

2.4 Responsibility and Authority

Top management shall ensure that responsibilities and authorities are defined and communicated within the organization for all employees involved in activities described in these requirements.

2.5 TQM Manager

Top management shall appoint a member of management who, irrespective of other responsibilities, shall have responsibility and authority that includes:

- Ensuring that the processes needed to meet the requirements of this document are established, implemented and maintained.
- Ensuring that the documentation needed for TQM is established, implemented and maintained.
- Reporting to top management on meeting these requirements and any need for improvement.
- Ensuring the awareness of TQM requirements throughout the organization.

Note 1 The responsibility of a TQM Manager can include liaison with external parties on matters relating to TQM requirements.

Note 2 The TQM Manager is the contact person for the purposes of TQM.

2.6 Approval Authority (Design Authority)

For each **Product**, top management shall assign a person or a group of people (the **Product Approval Authority**) with responsibility and authority to make decisions on **Product** Configuration.

The **Product Approval Authority** shall be competent and knowledgeable about compliance with the relevant **Technical Specifications**, the relevant sections of these requirements and the implementation of **configuration management**.

Note: **Product Approval Authority** can also be the Dispositioning Authority, Configuration Control Board, Change Approval Board or **Product** Approval Board.

2.7 Management Review

Top management shall review the implementation of the requirements of this document at planned intervals (no greater than 12 months apart), to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes, including the configuration policy and configuration objectives.

As a minimum, the following inputs shall be included in the management review:

- Status and review of actions from previous management reviews
- Review of the suitability of Configuration Management policy
- Review of the Configuration Management objectives
- Review of changes to the **Configuration Management System**
- Changes that can affect the **Configuration Management System**
- Results of audits (internal audits, external audits and audits of **supplier**s)
- Review of interoperability issues
- Process performance
- **Product** configuration conformity
- Status of preventive and corrective actions
- Resources (Personnel and infrastructure)
- Recommendations for improvement for each input above

Note
External audits include ISO 9001 certification body audits and TQM audits by Mastercard
Process performance includes characteristics and trends of configuration management processes

As a minimum, the following outputs shall be included in the management review. Decisions, actions or recommendations for improvement, including but not limited to:

- Improvement of the effectiveness of the **Configuration Management System**
- Improvement of the effectiveness of the TQM processes
- Improvement of **Product** interoperability
- Improvement of **Product configuration identification**
- Resource needs

Records from management reviews shall be maintained (see Control of Records).

2.8 Supplier Management

Top management shall ensure that all **suppliers** are managed in accordance with these requirements.

2.9 Product release and service delivery

Product release and delivery shall not proceed until the planned arrangements (see Configuration Management Planning) have been satisfactorily completed, unless otherwise approved by a relevant authority and where applicable, by the customer.

3 Operation

3.1 Documentation Requirements

TQM documentation shall include:

1. Documented processes required by these requirements
2. Documented statements of a configuration policy and configuration objectives
3. Documentation needed by the **Vendor** to ensure the effective planning, operation and control of its processes
4. Records and reports required by these requirements.

3.1.1 Control of Documents

Documents required by the **Configuration Management System** and these requirements shall be controlled. Records are a special type of document and shall be controlled according to the requirements given in Control of Records.

A documented procedure shall be established to define the controls needed:

- To approve documents for adequacy prior to issue
- To review and update as necessary and re-approve documents
- To ensure that changes and the current revision status of documents are identified
- To ensure that relevant versions of applicable documents are available at points of use
- To ensure that documents remain legible and readily identifiable
- To ensure that documents of external origin, are identified and their distribution controlled
- To prevent the unintended use of obsolete documents and to apply suitable identification to them if they are retained for any purpose

3.1.2 Control of Records

Records shall be established and maintained to provide evidence of conformity to requirements and of the effective operation of the **configuration management system**.

Records shall remain legible, readily identifiable and retrievable. A documented procedure shall be established to define the controls needed for the identification, control of changes (e.g. version control), storage, protection, retrieval, retention time and disposition of records.

Configuration Information shall be retained for at least 5 years after delivery of the last **Product** covered by the relevant **TQM Label**.

3.2 Resource Management

The **Vendor** shall determine and provide the resources needed to implement and maintain the requirements of this document and continually improve their effectiveness.

Personnel performing work affecting **product** configuration shall be competent on the basis of appropriate education, training, skills and experience.

The **Vendor** shall:

- Determine the necessary competence for personnel performing work affecting **product** configuration
- Provide training or take other actions to satisfy these needs
- Evaluate the effectiveness of the actions taken
- Ensure that its personnel are aware of the relevance and importance of their activities and how they contribute to the achievement of the configuration objectives
- Maintain appropriate records of education, training, skills, experience and TQM competence (see Control of Records).

The **Vendor** shall determine, provide and maintain the infrastructure needed to achieve conformity to requirements of this document. Infrastructure includes:

- Process equipment (test tools, configuration management database(s), support software)
- Supporting services (such as communications)

3.3 Supplier management

3.3.1 Supplier Categorization

Suppliers of services, components and parts to **Vendor**s (and **Vendor**'s **suppliers**, where applicable) are categorized as follows:

Category 1: A **supplier** who supplies services, components or parts that are not critical to compliance of the **product** with TQM requirements.

Category 2: A **supplier** who supplies services, components or parts which may have an effect on compliance of the **product** with TQM requirements, e.g. a **supplier** of **critical components** or a **supplier** who purchases **critical components** under their control, **service** or repair.

Note 1: Category 2 "components or parts" include **supplier**s of part A and part B1 components. The **supplier** could be the **Component Manufacturer** (if purchased direct) or a **Distributor**.

Category 3: **Suppliers** who supply services, components or parts which are critical to the compliance of the **product** with the TQM requirements e.g. **suppliers** who carry out design, validation testing, manufacturing - PCB assembly (e.g. SMT), manufacturing – product assembly, software loading, manufacturing testing, critical processes.

Note 2: Category 3 "components or parts" include an **IFM** or **PCD** as a sub assembly. **OEM** / **ODM** suppliers are also Category 3 suppliers.

Note 3: **Intermediary companies** used by the **Vendor** to access suppliers and services covered by the TQM requirements shall be declared on the VOD.

No specific requirements apply to Category 1 **suppliers**.

Category 2 and 3 **suppliers** shall hold one of the following for sites supplying products or services used by the **Vendor**:

- ISO 9001:2015 certification
- TL 9000 Release 6 certification
- IATF 16949:2016 certification

Note 4
This certification shall be accredited by a National Accreditation Body that is a signatory to the IAF MoU (http://www.iaf.nu//articles/IAF_MEMBERS_SIGNATORIES/4)

In addition, for Category 2 & 3 **suppliers**, planned audits of the **supplier** shall be undertaken by the **Vendor** to ensure that the applicable requirements of this document are implemented, maintained and in use. Records of these audits shall be made available to Mastercard (See Control of Records).

Audits of Part A and Part B1 component **suppliers** (other than **component manufacturers**, e.g. a **distributor**) shall ensure the integrity of the **supply chain**. (ref: Supplier responsibilities)

Note 5
Activities to ensure the integrity of the **supply chain** include counterfeit component control as well as knowledge of the **supplier**'s source of the components.

Note 6
Part A and Part B1 component supplier audits can be physical or remote audits. Remote audits can be in the form of a self-assessment questionnaire.

If the **Vendor** delegates the purchase of components to another company, including a group company, the manufacturing (or **service**) facility or organization etc. and that facility or organization carries out the audits, the **Vendor** shall have sight of the audit content and audit results.

Supplier audits shall be carried out every 12 months unless another period can be justified. The justification shall be clear and robust. The analysis and conclusion of the justification shall be recorded with the supporting records and / or data.

Mastercard reserves the right to audit Category 2 **suppliers** if doubt is raised during a Category 3 audit or during a VOD assessment that the Category 2 **supplier** should be classified as a Category 3 **supplier**. Category 3 **suppliers** shall be audited on behalf of Mastercard as part of the TQM **Vendor** approval process.

3.3.2 Supplier selection

The **Vendor** shall evaluate and select **suppliers** based on their ability to supply services or product in accordance with the **Vendor**'s requirements. Criteria for selection, evaluation and re-evaluation shall be established. Records of the results of evaluations, re-valuations and any necessary actions arising from the evaluation shall be maintained (see Control of Records).

For determining criteria for re-evaluation of **suppliers**, this section (supplier management) applies.

Note
Supplier selection records shall include any **intermediary company** used.

3.3.3 Supplier Agreement

The **Vendor** shall establish, document and maintain an agreement with the **supplier** about Quality and **Configuration Management**.

The agreement shall document, among others, the **Vendor**'s specifications for the interface between the **supplier** and the **Vendor** in terms of:

- Product and process requirements
- Procedures and criteria to be used in monitoring the **supplier** performance
- Criteria for qualification of sub-contracted process(es)
- Product acceptance criteria.

Note 1
Any **Vendor** / **OEM** / **ODM** supplier agreements should define which parts of these requirements the **OEM** / **ODM** is responsible for as well as how the **Vendor** monitors and confirms that these requirements have been met.

Note 2
Any **Vendor** agreement with an **intermediary company** should define the **intermediary company**'s responsibilities that ensures the **Vendor**'s responsibilities under the TQM requirements are met.

3.3.4 Manufacturing qualification process

The **Vendor** shall implement a **manufacturing qualification process**. The qualification process shall be applied to each **product** at each manufacturing site or organisation and is a precondition for the application of any product acceptance plan.

Note:
The manufacturing qualification process can be included in NPI (New Product Introduction) or FAI (First Article Inspection) activities.

3.3.5 Supplier responsibilities

The **supplier** shall not invalidate or jeopardize the integrity of the EMVCo L1 **LoA** or the L2 **LoA**. The **Vendor** shall take reasonable actions to ensure this.

3.3.6 Supplier management and monitoring

Prior to using a sub-contract manufacturing facility, the **Vendor** shall include an audit of their quality **management system** (including their ability to implement customer specific requirements and manage changes to the manufacturing information from the **Vendor**) as well as verifying the capability of the **Manufacturer**.

The **Vendor** shall have full control over every element of design, supply and fabrication and have processes in place to ensure that any proposed changes are notified and approved before implementation into manufacture.

3.4 Organizational Interfaces Management

The **Vendor** shall define and maintain documents describing the interface between the different entities identified in the **Product** Configuration Management Plan in terms of:

- Deliverables exchanged between the different entities.
- Responsibilities and authorities of both entities to provide / receive and review deliverables from each other (including **release** management)
- Standards and procedures to be followed.
- Common reviews to be conducted.

Note 1
The entities which are not part of the **Vendor** internal organization are called **Suppliers**. Design, Manufacturing and **Service** providers can be **Suppliers**. Any **Intermediary companies** used shall be included in these documents.

Note 2
Responsibilities and authorities include project management (can include contract / agreements etc.), purchasing / sales, engineering (technical), quality management, material quality control, logistics etc.

3.5 Customer Communication

The **Vendor** shall inform all entities purchasing TQM approved devices regarding their compliance with the **Technical Specifications** of the devices and shall provide the related EMVCo L1 **LoA** and **TQM Label**.

If there are any restrictions associated with the EMVCo L1 **LoA** this shall be disclosed.

Mastercard's customer (i.e the Vendor's customer) entering into M-TIP should refer to the latest process guide found at Mastercard connect portal for all requirements relating to the deployment of Contact and Contactless approved products.

4 Product Design

4.1 General Requirements

The **Vendor** shall establish, document, implement and maintain **product** design processes including **configuration management** and continually improve its effectiveness in accordance with these TQM requirements.

The **Vendor** shall:

1. Identify the processes needed for the **Configuration Management System** and their application throughout the organization
2. Determine the sequence and interaction of these processes
3. Determine criteria and methods needed to ensure that both the operation and control of these processes are effective
4. Ensure the availability of resources and information necessary to support the operation and monitoring of these processes
5. Monitor, measure and analyze these processes
   (See "Monitoring and measurement of configuration processes" and "Analysis of Data")
6. Implement actions necessary to achieve planned results and continual improvement of these processes

These processes shall be managed by the **Vendor** in accordance with these TQM requirements.

Note 1 **Product** design processes include: development, design review, **change control** (including alternative component assessment), approval and **release** to production.

Where a **Vendor** chooses to outsource any process that affects **product** configuration (a Category 3 **supplier**), it shall ensure control over such processes (see Supplier Management). Control of such outsourced processes shall be identified within the **configuration management system**.

4.2 Product Configuration Management

4.2.1 Product Life Cycle Model

The **Vendor** shall establish and maintain an integrated set of requirements that covers the life cycle of its **Products** and **Implementations**.

These requirements shall define:

- The **Product** and Implementation life cycle stages
- The configuration processes, activities and tasks that are appropriate to each stage of the **Product** and Implementation life cycle including:
  1. **Configuration Items** identification and registration
  2. Establishment of **Configuration Items** baselines whenever it is necessary to define a reference for further activities
  3. Configuration review, verification, validation, approval and release
  4. The responsibilities and authorities for **Product** configuration

Note 1 These requirements shall help the **Vendor** to identify and manage the interfaces between different groups, within and outside the organization, involved in a **Product** life cycle to ensure effective communication and clear assignment of responsibility.

Note 2 **Product** and Implementation life cycle stages should include: concept, definition, development, design review, approval and **release** to production, production, operation, maintenance (including **Change Control** and **release** to production) spanning the **Product** and Implementation life cycle.

4.2.2 Configuration Management Plan

The **Vendor** shall plan and control the **configuration management** by establishing and maintaining a configuration management plan based on the **product** life cycle model for each **product**.

In the situation where the **implementation** is intended to be used in several **products**, the **Vendor** shall establish and maintain a configuration management plan for each **implementation**.

In planning the **Product** or **Implementation** configuration, the **Vendor** shall determine the following:

- Configuration objectives and requirements for the **Product** and **Implementation** configuration (including those specified in these TQM requirements).

The need to establish processes, documentation (including **configuration information**), baselines and to provide resources specific to the **Product** and **Implementation** configuration

- Required verification, validation, monitoring, inspection and test activities specific to the Product configuration and the criteria for **Product** and **Implementation** configuration acceptance
- Records needed to provide evidence that the configuration processes and resulting **Product** and **Implementation** configuration meet requirements (see Control of Records)
- Relevant standards, configuration management procedure(s) and tools to be used
- Project organizational structure including:
    - Identification of the interfaces between different groups and entities, within and outside the organization (See organizational interface management)
    - Definition of project roles and responsibilities regarding **configuration management**
    - Qualification and training needs for **configuration management** and TQM.

The output of this planning shall be documented, approved and controlled in a form suitable for the organization's method of operations.

Note 1
Interfaces between internal groups, for example but not limited to: Product Development (R&D) / Production Control, Product Development (R&D) / Purchasing, Product Development (R&D): Software Team / Hardware Team / Validation Team, Product Development (R&D) / Product Support (Bugs and Interoperability Issues) etc.

Interfaces with external organizations, for example but not limited to: **Suppliers** (including any **intermediary companies**), Test Laboratories, EMVCo, TQM Assessment Body, Mastercard etc.

Note 2
The **Product** or **Implementation** configuration management plan may be an independent document, a part of another document, or comprised of several documents. TQM questionnaires (VOD and TID) can be used to define parts of the **Product** configuration management plan.

Note 3
General work instructions defining tasks and responsibilities common to all projects need not be replicated as part of a **Product** configuration management plan.

Note 4
If the configuration management plan is not an independent document, then there should be a document that contains references to all of the individual documents that apply to each part of these requirements.

Note 5
Standards include the relevant EMVCo specifications and test standards as well as these TQM requirements (including version information)

4.3 Configuration Identification

4.3.1 Configuration Items

The **Product Configuration Items (CI)** are divided into three sets, as illustrated in the Figure below:

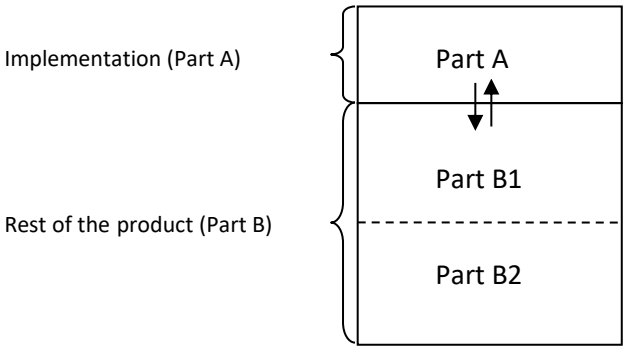


Figure 4-1 - Product partition for TQM

Part A: the set of CIs the **Vendor** defines as the **Implementation**, fulfilling all requirements of the relevant **Technical Specifications**. It includes the hardware and software dedicated to and/or involved in the **Implementation** functionalities. This part is defined by the **Vendor**'s internal specification for the **Implementation**.

Part B1: the set of CIs that are not part of the **Implementation**, but are those that **interface** with the **Implementation** (for example used by Part A / connected to Part A) or have a direct impact on the behavior of the **Implementation**. This part, also called **Implementation Environment**, shall be compliant with the **Implementation Interface** specification.

Part B2: the set of CIs of the rest of the **Product** that have no direct link with part A and do not impact the **Implementation** behavior. These CIs are not relevant for TQM purposes and are not required to be noted against the CI information.

Note 1:
Where hardware and software resources are shared by the **Implementation** and the rest of the **Product**, the **Vendor** is responsible for determining whether they are part A components or can be considered as part B1 components which will depend on the **product** architecture. Examples of such resources include Power supply, CPU, memory, unpopulated Printed Circuit Boards (PCB), Operating System, Drivers, Utilities.

Note 2:
The EMVCo change management guidance should be taken into account when determining the **product configuration item** sets.

The **Vendor** shall identify and record in the Configuration Management Database (CMDB) the **Configuration Items** within the **Product** that have an impact on the compliance of the **Implementation** with the relevant **Technical Specifications**. Such **Configuration Items** comprise those from part A and B1 (these are **critical configuration items**).

The part of the **Product** to which a CI belongs shall be identified as an attribute of the CI and shall be recorded in the CMDB.

4.3.2 Configuration Items Relationship Identification

The **critical configuration items** shall be identified and recorded in the **Configuration Management System**. The hierarchy and relationships of the **critical configuration items** within a **Product** shall be documented in a tree structure called the **Product Configuration Tree**.

The **configuration items** identified in the **Product Configuration Tree** shall be traceable (including version or status etc.) to the configuration management tools used to manage and control the hardware and software configurations.

Note 1
The purpose of the **Product Configuration Tree** is to allow Mastercard to easily identify the differences of Implementation critical CIs between two **Products**.

Note 2
The **Product Configuration Tree** shall be consistent with the naming and numbering used in the configuration management system as well as on the **EMVCo L1 LoA**. The naming and numbering conventions defined as a requirement of this document shall be followed.

The **Product Configuration Tree** shall have the following structure.

The **Product Configuration Tree** shall contain two sub-trees:

- The A tree (also called Implementation **Configuration Tree**): tree structure presenting the CIs from part A of the **Product**, down to the lowest level of independent change. The root of the A tree shall be identified by the **Implementation identifier** (Implementation ID).
- The B1 tree: tree structure listing the CIs from part B1 of the **Product**.

Note 3
The configuration tree(s) listing the software CIs (for both part A and part B1) shall also show the associated CI version status. Software CIs are usually modules or libraries. This also applies if the software CIs are shown in a separate document.
Examples of version status are (but not limited to) checksum, hash code, release date.

The A and the B1 trees shall have the root of the **Product Configuration Tree** as a direct parent.

The Implementation **Configuration Tree** shall be composed of two sub-trees:

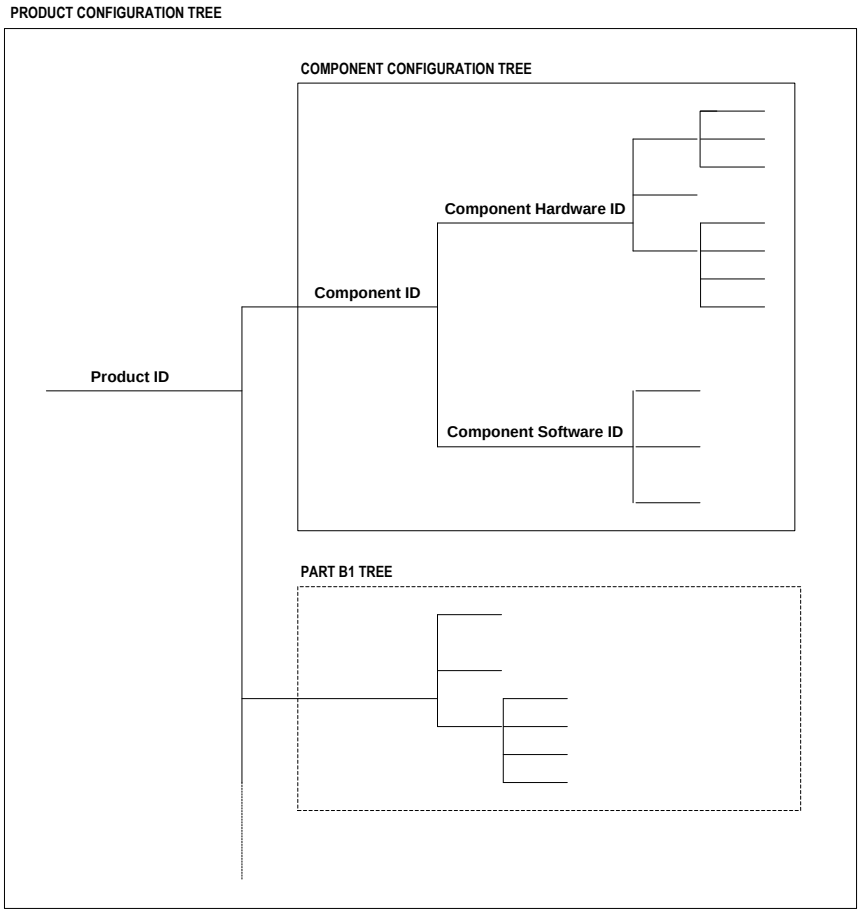
- **Implementation** hardware tree: tree structure listing the hardware CIs from part A of the **Product**.
- **Implementation** software tree: tree structure listing the software CIs from part A of the **Product**.

The root of the **Implementation** hardware and software tree shall be identified by the **identifiers** of the **Implementation** hardware (Implementation Hardware ID) and software (Implementation Software ID).

The root of the **Product Configuration Tree** is identified by the **Product** ID.

The **Product** ID, Implementation ID, Implementation Hardware ID and Implementation Software ID within the **Configuration Tree** shall be the ones declared in the **ICS** for **Terminal Type Approval Level 1** and reported on the EMVCo **Level 1 Letter of Approval** or implementation evolutions that have been validated by processes conforming to the TQM Requirements.

Figure 4-2 - Product Configuration Tree



Note 4
The **Product Configuration Tree** can also contain a B2 sub-tree. However, this sub-tree is not relevant from a TQM perspective.

Note 5
The definition of the level of breakdown for **Configuration Items** for the B1 tree is left to the **Vendor**. However, the **Vendor** shall be aware that an insufficient level of breakdown may not prove the limited impact of a change to Mastercard. Refer to the examples in "**Configuration Items**" Part B1 definition.

Note 6
The **Implementation** and **Product Configuration Trees** should preferably be directly generated from the **Configuration Management System**'s configuration management tools. However, any kind of documentation is accepted (a specifically created document, an organized set of print screens, etc.) Whichever form the product configuration tree takes it shall contain the product ID, implementation ID (IFM / PCD) and implementation (HW and SW) IDs as defined in this section.

Note 7
Any discrepancy from the declared hardware or software revision associated with Part A or B1 components and that found at audit shall be raised as a major nonconformity.

4.4 Configuration Information

Implementation and **Product configuration information** shall be developed, established and maintained throughout the **Product** life cycle.

The **Implementation configuration information** shall be managed separately from the **configuration information** of the **Product**.

4.4.1 Implementation Configuration Information

Implementation **Configuration Information** shall include (but is not limited to):

- **Implementation** Configuration Management Plan
- **Vendor**'s internal specifications for the **Implementation**, including:
    - **Implementation** Functionalities to be achieved including reference to the relevant **Technical Specifications** versions.
    - Hardware and software architecture of the **Implementation**
    - Parts list (see also Component Identification (Bill of Materials))
    - Source codes list (including version information)
    - Technical documentation of CIs (e.g. chipset, ASIC etc.) if any
    - Requirements for **Implementation CIs** implementation
        - Electrical schematics
        - Antenna layout
        - Drawings (**Implementation** layout)
    - Requirements for **Implementation** software development chain
    - Requirements for **Implementation** hardware integration (e.g. exploded diagram or assembly drawings)
    - Requirements for **Implementation** software integration (software loading process)
    - Requirements for **Implementation CIs** identification
        - Conventions to be used
        - **Implementation Configuration Tree**
    - Qualification methods to be used to check compliance of the **Implementation** with the relevant **Technical Specifications**
- **Vendor**'s internal specifications for the **Implementation interface**, including:
    - Requirements for power supply
    - Definition of the **Implementation** software **interface** (APIs, APDUs) with the rest of the Terminal (Level 2)
    - Requirements for antenna landing zone
    - Requirements for **Implementation** critical **CIs** (part B1) identification and conventions to be used
    - Hardware and software architecture of the **Implementation Interface**
    - Parts list (see also Component Identification (Bill of Materials))
    - Source codes list (including version information)
    - Guidelines for implementation of the **Implementation** within a **Product**
    - Qualification methods to be used to check the compliance of a **Product** with the **Implementation interface** specification.

- **Change control** records for the **Implementation** and **Implementation Interface**
    - **Change control** records for the **Implementation**
    - **Change control** records for the **Implementation Interface**
- Final testing of products and implementations, production result records
- Production acceptance and release records
- **Service** records for the **Implementation** and **Implementation Interface**
  (Records of all work carried out including, but not limited to: Component replacement, PCB swap, ECN application, re-loading the firmware / software that includes **Implementation** and **Implementation Interface** firmware / software)
- Final testing of products and implementations, service result records
- Service release records
- TQM documents:
    - Related TID and VOD questionnaires.
    - Implementation Conformance Statements (ICS)
    - **Letter of Approval** once obtained (Level 1)
    - EMVCo **TTA L1** Test Report including the ICS submitted for EMVCo **TTA L1**.

4.4.2 Product Configuration Information

Product Configuration Information shall include (but not limited to):

- **Product** Configuration Management Plan including Reference to the relevant **Implementation Configuration Information**
- **Product** specifications:
    - Hardware and software architecture of the **Product**
    - Diagram(s) depicting the **interfaces** between the **Implementation** and the **Product**
    - Antenna landing zone
    - **Implementation** power supply
    - Printed Circuit Boards layout
    - **Implementation** critical **CIs** identification (parts A and B1) and **Product Configuration Tree**
- Support documentation:
    - Guidelines for application software development
    - Manufacturing package
    - Guidelines for installation, software loading, use and maintenance
    - Maintenance package
- TQM documents:
    - **Product configuration audit** reports (See “Monitoring and measurement of **Product** Configuration”):
        - All functional **configuration audit** reports
        - All physical **configuration audit** reports
    - Proof of compliance continuity with the relevant **Technical Specifications**

4.5 Naming and Numbering Conventions

Unique naming and numbering conventions shall be established and documented that define methods for:

- Allocation of a unique **identifier** to each selected **Configuration Item**
- Allocation of a unique **identifier** to each selected **Configuration Information**
- Identification of **change control** information such as revision status
- Identification of the **Implementation ID**, **Implementation** hardware ID and **Implementation** software ID
- Identification of New **Implementation** Versions and Derived **Implementations**
- Identification of **Product** ID.

These conventions shall allow the unique identification of a **Configuration Item** to be traceable to its associated documentation (including the relevant EMVCo L1 LoA / LoAs) and vice-versa.

Note 1
Naming and numbering conventions can be specific to one **Implementation** or be common to all projects.

These conventions shall allow Mastercard and Mastercard customers (or their agents) to be certain that a **Product** is covered by a **TQM Label**.

Note 2
The **identifiers** could for example consist of a combination of fixed or variable alphanumeric characters. The fixed characters would be identical for all New **Implementation** Versions or Derived **Implementations**.

Another solution could be to structure the **identifiers** in the following manner:

ID = Name + V+v, where:

- v is incremented when the change leads to a change of ID without change of **Implementation** specification
- V is incremented when the change leads to a change of ID with change of **Implementation** specification
- Name is unchanged for New Versions or Derived **Implementations**.

4.6 Configuration Baselines

The **Vendor** shall establish and approve **item** configuration baselines, whenever needed in the **product** life cycle (see Configuration Management Plan.). These **item** configuration baselines shall record the **configuration information** of this **item** at the specific time or stage of its life cycle.

Change documentation shall be added to the **configuration information** in a baseline or a new baseline shall be established after each change (or batch of changes) have been approved for **release** into production.

In particular, a **Product** Configuration baseline shall be established, named/numbered and approved for each **release** of **Product configuration information**, including the one leading to the manufacturing of **DUT** submitted to Test Laboratories. The level of details to which the **Product** is defined in this baseline shall be compliant with the **Product Configuration Information** requirements.

Note: The level of detail to which an **item** is defined in a configuration baseline depends on the degree of control required at the related stage of the **item** life cycle.

4.7 Component Identification (Bill of Materials)

The **Vendor** shall state the specification of each component that will be used for manufacturing, including the component manufacturer and manufacturer's part number of the component (MPN) for each baseline, including the one leading to the manufacturing of **DUT** submitted to Test Laboratories.

The **Vendor** shall validate any proposed changes to component values or characteristics. (See **change control**)

Any change to a part A or B1 component shall have the relevant **change control** records including, where appropriate, the relevant validation reports to support the change.

4.8 Requirements for assessing alternative components

The **Vendor** shall validate any proposed change of **component manufacturer**. Any change to a part A or B1 component shall have the relevant **change control** records to support the change.

The **Vendor** shall validate any additional (alternative) components. Any additional (alternative) part A or B1 components shall have the relevant assessment (**change control**) records to support the addition to the Bill of Materials.

4.9 Change Control

After EMVCo **TTA L1** approval (EMVCo **L1 LoA**), all changes to the **critical configuration items** (Part A and Part B1) shall be controlled.

The process for controlling change shall be documented and shall include the following:

- Initiation, identification and documentation of the need for change
- Categorization of the change
- Evaluation of the consequences of the change
- Compliance with the **Technical specifications**
- Compliance with the **Vendor**'s internal specifications for the **Implementation**
- Compliance with the **Vendor**'s internal specifications for the **Implementation Interface**
- Approval of the change
- Implementation and verification of the change

The process definition shall define the associated responsibilities and forms to be used.

4.9.1 Initiation, Identification and Documentation of the need for change

Prior to submission for evaluation to the **Approval Authority**, all change proposals should be identified and documented.

Change proposals shall include at least the following information:

- The reason for the change
- A description of the proposed change
- **Configuration Item**(s) and related **configuration information** to be changed, including details of their title(s) and current revision status
- Details of other **Configuration Items** or **Configuration Information** that may be affected by the change.

4.9.2 Categorization of the Change

Any risk, arising from the change, on the following shall be identified and recorded:

- Noncompliance with the relevant **Technical Specifications**
- Noncompliance with the **Vendor**'s internal specifications for the **Implementation**
- Noncompliance with the **Vendor**'s internal specifications for **Implementation interface**

A change with one of these risks shall be categorized as an **Implementation** critical (Major) change.

Changes outside the risks above are Minor changes, unless the changes affect **Fit**, **Form** or **Function**, which then shall also be categorized as Major changes.

The categorization shall be recorded.

Note 1
The EMVCo change management guidance should be taken into account when determining the categorization for Major and Minor changes.

Note 2
If the categorization terms in the **change control** process do not include "Major" and "Minor" as described in this document, then there should be a description of how the terms in the **change control** process relate to the EMVCo and TQM categorization terms.

4.9.3 Evaluation of the Consequences of the Change

When a change is categorized as a Major change, its consequences shall be evaluated before acceptance of the change by the **Vendor**.

For this purpose, the **Vendor** shall assess the continuity of the compliance with the relevant **Technical Specifications**.

In the situation where the **Vendor** can demonstrate that the compliance with the relevant EMV Specification is maintained, the **Vendor** shall also evaluate the impact on:

- Compliance with **Vendor**'s internal specifications for the **Implementation**,
- Compliance with the **Vendor**'s internal specifications for **Implementation interface**

and shall assess the need for **Implementation Critical Configuration Items** re-identification.

The **Vendor** shall keep records of the change evaluation (See Control of Records).

4.9.4 Compliance with the Technical specifications

When assessing the continuity of compliance, the **Vendor** shall evaluate whether the changed design is still compliant with the relevant **Technical Specifications**.

There are three options:

- The proof of compliance requires testing of the relevant **Technical Specifications** functionality. In this case, an EMVCo **TTA L1** test session shall be performed by a **Test Laboratory**.
- The compliance can be proved by design (e.g. proof by assessment) which shall be recorded or through tests that do not include EMVCo **TTA L1** testing to verify the **Technical Specifications** functionality. In this case, the demonstration and the associated test reports (debug or formal tests), if any, shall be recorded (See Control of Records).
- The compliance cannot be proved. In this case, the change shall not be accepted.

In the situation of a change of **Technical Specifications**, a new EMVCo L1 **LoA** is required to demonstrate compliance of the **Product** with the changed specification.

If there is a new EMVCo L1 LoA, then Mastercard shall be informed in order to carry out an assessment regarding continued L2 compliance. Please note that the assessment result may require additional regression testing.

Test Laboratories accredited by EMVCo can perform debug or formal EMVCo **TTA L1** tests:

- In Formal test sessions:
  - The complete set of tests are executed (e.g. analog & digital tests for contactless; mechanical, electrical and protocol tests for contact)
  - A detailed Test Report is issued.
- In debug test sessions:
  - The **Vendor** can request the execution of only a subset of the tests.
  - A lightweight Test Report is issued.

When the **Implementation** already has a **TQM Label**, results of debug test sessions performed in an accredited Laboratory are accepted by Mastercard. Their results are recognized because Mastercard is confident that:

- The change impact and the testing needs have been correctly evaluated
- The **configuration information** of the tested sample has been recorded
- The sample's configuration is uniquely identified
- The sample's identification supplied to the laboratory allows **traceability** to its **configuration information**

Without a **TQM label**, only formal test sessions are accepted.

Note 1 EMVCo **TTA L1** tests done internally by the **Vendor** may not be recognized by Mastercard as proof of compliance with **Technical Specifications**.

Note 2 The **configuration management** of L2 software is within the scope of TQM. The **configuration management** of L2 software shall not be assessed during a TID or VOD review but shall be within the scope of a TQM audit.

4.9.5 Compliance with the Vendor's internal specifications for the implementation

When assessing the continuity of compliance, the **Vendor** shall evaluate whether the modified **Implementation** still conforms to the **Vendor**'s specifications. **Fit**, **Form** and **Function** of any changed **item** of the **Implementation** shall be checked to ensure that it remains compliant with the **Vendor**'s specifications.

Note
A change of **component manufacturer** for a component is not a change of **Fit**, **Form** or **Function**. For example, replacing a capacitor by an equivalent from another **component manufacturer**.

There are two cases:

- The modified **Implementation** still conforms to the **Implementation** specifications. The modified **Implementation** is considered a New Version of the **Implementation**;
- The modified **Implementation** no longer conforms to the **Implementation** specifications. New specifications shall be created and the modified **Implementation** is considered a Derived **Implementation**.

The evaluation and its conclusion shall be recorded.

4.9.6 Compliance with the Vendor's internal specifications for the implementation interface

When assessing the continuity of compliance, the **Vendor** shall evaluate whether the **Product** with modified part B1 conforms to the **Vendor**'s **Implementation interface** specifications. **Fit**, **Form** and **Function** of the part B1 that includes the changed **item** shall be checked to ensure that it remains compliant with the **Implementation interface** specifications.

Note
A change of **component manufacturer** for a component is not a change of **Fit**, **Form** or **Function**. For example, replacing a capacitor by an equivalent from another **component manufacturer**.

There are two cases:

- The part B1 still conforms to the **Implementation interface** specifications. The **Product** is considered as a Derived **Product**;
- The part B1 does not conform to the **Implementation interface** specifications. The change is not acceptable unless a deficiency in the **Implementation interface** specifications can be identified.

The evaluation and its conclusion shall be recorded.

4.9.7 Re-identification of Configuration Items

The need to re-identify **Configuration Items** (assign a new **identifier**) depends on **Interchangeability** of the superseded and superseding **items**.

Assessing the need for re-identification prior to obtaining an EMVCo **TTA L1 LoA** is not necessary.

Interchangeability

Two **items** are considered interchangeable when:

- The **Fit**, **Form** and **Function** of the superseded and superseding **items** meet the **Product** specifications
- These previous criteria are met both ways (old in the new and vice-versa)
- These previous criteria are met with no special measures to the **item** or related **item** and in all applications (where used).

For instance, a resistor is interchangeable with an equivalent one from another **component manufacturer**.

The **Vendor** is responsible for the method used for **interchangeability** analysis. The **interchangeability** analysis shall be recorded (See Control of Records).

Re-identification

In the situation where two **items** are interchangeable, the superseding **item** does not need to be re-identified, if the **traceability** is achieved by another means. Otherwise the **item** shall be re-identified.

In the situation where a superseding **item** is not interchangeable with the superseded one, the superseding **item** shall be re-identified. The evaluation of **interchangeability** and the re-identification shall be pursued back up the **Configuration tree** until the **interchangeability** is re-achieved.

The re-identification analysis shall be recorded (See Control of Records).

Note: The re-identification back up the **Configuration tree** could lead to the re-identification of the **Implementation ID**, **Implementation** hardware ID or **Implementation** software ID.

4.9.8 Approval of Change

After a proposed change, has been evaluated, the **Approval Authority** shall review the evaluation and shall decide upon the approval of the change.

Prior to approval of a change, the **Approval Authority** shall verify that:

- The proposed change is necessary and the consequences would be acceptable
- The change has been properly documented and categorized
- The planned activities for the implementation of the change into **Product** and **Implementation Configuration Information** are satisfactory
- The planned activities for submission to Mastercard TQM process are satisfactory.

The approval shall be recorded (See Control of Records). Notice of the change shall be circulated to all relevant parties both within and outside the organization.

Note: Mastercard are a relevant party outside of a **Vendor**'s organization.

4.9.9 Implementation and Verification of Change

After implementation, compliance with the approved change shall be verified. This verification shall be recorded to allow **traceability** (See Control of Records).

The **Vendor** shall establish and maintain a documented process(es) which provides **traceability** of design changes to identifiable manufacturing dates, lots, or serial numbers. This shall enable the **Vendor** to identify and recall **Products** that are unfit to remain in service.

4.10 Remote software updates

Any remote software or firmware updates that include the reloading of any part A or part B1 software (or firmware) shall be verified by the **Vendor** on representative hardware, including the 'Minimum requirements for final testing of **Products** and **Implementations**' before the remote update is authorized.

Note: Remote software updates include over the air (OTA) updates as well as updates carried out in the field or via the Terminal Management System (TMS).

4.11 Product Configuration Status Accounting

4.11.1 Product Configuration Records

The **Vendor** shall perform **Product** configuration status recording activities throughout the life cycle of the **Product** in order to support and enable an efficient configuration management process.

The **Product** configuration records shall include details, when appropriate, of

- The **Product Configuration Information** (such as identification number, title, effective dates, revision status, change history and its inclusion in any baseline)
- The **Product**'s configuration (such as part numbers, **Product** design or build status)
- The status of **release** of new **Product Configuration Information**
- The processing of changes (change control records).

The evolving **Product Configuration Information** shall be recorded in a manner that identifies the cross-references and interrelationships necessary to provide the required reports to Mastercard at request.

4.11.2 Product Configuration Reports

When needed (at request) the **Vendor** shall be able to provide records such as:

- A list of **Products** for which baselines have been established
- A list of **Configuration Items** included in a specific configuration baseline
- A list of **Product Configuration Information** included in each specific configuration baseline

A list of configuration baselines containing a specific **Configuration Item** or a specific **Configuration Information**

- The current revision status and change history of a specific **Configuration Item** or a specific **Configuration Information**
- Status records on changes and **concessions**
- Details of the status of delivered and maintained **Products** concerning part and **traceability** numbers and their revision status

5 Manufacturing and Service

All manufacturing and **service** sites that are within the scope of the TQM approval shall hold one of the following:

- ISO 9001:2015 certification
- TL 9000 Release 6 certification
- IATF 16949:2016 certification

The certification scope shall cover all TQM activities that are carried out by the site or organisation.

Note: This certification shall be accredited by a National Accreditation Body that is a signatory to the IAF MoU (http://www.iaf.nu//articles/IAF_MEMBERS_SIGNATORIES/4)
This requirement also applies to any sub-contract **manufacturer** (**Supplier**) used by the **Vendor** (see Supplier Management).

5.1 Manufacturing (Vendor responsibilities)

5.1.1 Manufacturing control

The **Vendor** shall plan and carry out manufacturing under controlled conditions and are responsible for ensuring that the manufacturer meets their responsibilities under the TQM requirements.

Manufacturing activities include (but are not limited to):

- Component purchase.
- Control of nonconforming product.
- Control of changes.
- PCB assembly.
- **Module** and **Product** assembly.
- Software / Firmware loading.
- Functional testing.
- Built **configuration** verification.

Controlled conditions shall include, as applicable:

- The availability of information that describes the characteristics of the **Product.**
- The availability and suitability of work instructions, as necessary.
- The use of **suitable equipment.**
- The availability and use of monitoring and measuring devices.
- The implementation of monitoring and measurement.
- The implementation of **release** and delivery activities.

The **Vendor** shall ensure that the controls apply to any internal manufacturing as well as to any manufacturing sub-contracted to a **Supplier**.

5.1.2 Validation of processes for manufacturing

5.1.2.1 Controls for producing and controlling production process and assembly documentation

The **Vendor** shall ensure that the **manufacturing sites** or organizations have appropriate process instructions in place. Any variation to manufacturing processes shall be approved and validated by the **Vendor**.

5.1.2.2 Controls for producing and controlling automated manufacturing processes

The **Vendor** shall ensure that an **Automated Manufacturing Process** is appropriate for the task being performed.

Any variation or change to an **Automated Manufacturing Process** shall be approved and validated by the **Vendor**.

A **Vendor** shall be able to demonstrate that the software that is installed in each component has its revision validated.

The **Vendor** shall be able to demonstrate that effective measures are in place to ensure that the software installed in a component at manufacture cannot be modified after manufacture.

5.1.2.3 Product Acceptance Plan

The **Vendor** shall document and implement a **Product** Acceptance Plan that defines **Vendor**'s acceptance for **production**.

Product acceptance shall apply to each **manufacturing site** or organization and shall be effective upon completion of the **manufacturing qualification process** for the product.

If sampling of the manufactured batches or lots is allowed by the **Vendor**, the sampling criteria and the acceptable quality level (AQL) shall be defined by the **Vendor**.

The **Product** Acceptance Plan shall include verification of the built **Product configuration** with its **Product configuration information**.

Evidence of conformity with the acceptance criteria shall be maintained (see Control of Records). Records shall indicate the person authorizing the **release** of the **Product**.

Note 1
The "verification of the built Product configuration with its Product configuration information" should, as a minimum, for each unit selected for verification, include hardware build (e.g. PCBA), software / firmware version and the status of the functional tests (final test) carried out during assembly.

Note 2
If the "verification of the built Product configuration with its Product configuration information" is achieved (partially or fully) by automatic means, how this is achieved should be described in the product acceptance plan.

5.1.2.4 Manufacturing monitoring

Manufacturing monitoring shall include ongoing and scheduled inspections, including **Product configuration** and **configuration** processes verification demonstrating the consistency of each **Product** to its **Product Configuration Information**.

The **Vendor** shall make sure that quality variance is effectively analyzed by the **manufacturing sites** and organizations as well as ensuring that corrective actions are made to remedy any deviations.

5.1.3 Control of Nonconforming Product

The **Vendor** shall ensure that **Product** which does not conform to its **Product configuration information** is identified and controlled to prevent its unintended use or delivery.

The controls and related responsibilities and authorities for dealing with nonconforming **Product** shall be defined in a documented procedure.

The **Vendor** shall deal with nonconforming **Product** in one or more of the following ways:

- By taking action to eliminate the detected nonconformity
- Evaluate the need for action to eliminate the cause(s) of the nonconformity, in order that it does not recur or occur elsewhere
- By taking action to preclude its original intended use or application.
- By authorizing its use, **release** or acceptance under concession by a relevant authority
- Make changes to the **configuration management system**, if necessary.

Records of the nature of nonconformities and any subsequent actions taken, including concessions obtained and identifies the authority deciding the action shall be maintained (see Control of Records).

When nonconforming Product is corrected, it shall be subject to re-verification to demonstrate conformity to the requirements.

When nonconforming Product is detected after delivery or use has started, the Vendor shall take appropriate action for the effects, or potential effects of the nonconformity.

5.1.4 Minimum requirements for final testing of Products and Implementations

Products (components) shall be verified and tested at the final production stage, this testing shall verify the physical performance of every **Product** or **Implementation** manufactured.

The testing shall be performed on a physical test bench or tool with traceable test equipment or using uniquely identified and controlled contact or contactless cards as references. The **Vendor** shall ensure yearly (unless another period is justified) calibration and verification of the test bench or tool or reference cards used to perform this final test.

For **IFM**'s, as a minimum, card operation procedures "Activation", "Reset", "Information exchange" and "Deactivation" shall be performed with a representation of an integrated circuit card.

Using **PCD** reference cards only:

For **PCD**'s, as a minimum, PCD to PICC communication shall be established at 0cm as well as at 4cm using communication signal interface Type A and at 0cm as well as at 4cm using communication signal interface Type B.

If the terminal's functional test specifies the card type for the test, the PCD to PICC communication should be robust enough to reject an incorrectly presented card. (E.g. a Type B card is presented during the Type A test will not return a pass result)

Distances of greater than 4cm may be substituted for the 4cm tests.

Using a combination of RF field strength measurement and **PCD** reference cards:

If the radio frequency field strength is verified during the final testing of **products,** then the following criteria apply:

- The RF field strength measurement is required for one position at a height of 4cm.
- If the measurement is carried out without modulation (carrier only) then the EMVCo PCD analogue radio frequency field strength limits apply, PCD field strength (V_{OV}).
- If the measurement is carried out with modulation (i.e. the modulation cannot be turned off in production) then the **Vendor** shall define and document appropriate minimum and maximum PCD analogue radio frequency field strength limits, PCD field strength (V_{OV}) for both Type A and Type B modulations.
- The RF field strength measurement can be measured at a height greater than 4cm. In this case the **Vendor** shall define appropriate minimum and maximum PCD analogue radio frequency field strength limits, PCD field strength (V_{OV}), taking in to account the requirements for carrier only measurements or measurements with modulation.
- If RF field strength measurements are carried out and the method does not conform with the requirements above, the method used shall be documented and include detailed information explaining how the method used correlates with the EMVCo RF field strength measurement method.

If the radio frequency field strength is verified during the final testing then, as a minimum, PCD to PICC communication shall also be established at two distances (0cm and 4cm) using communication signal interface Type A and Type B. (e.g. Type A at 4cm and Type B at 0cm or vice versa).

Distances of greater than 4cm may be substituted for the 4cm tests.

As a reminder, the **Vendor** shall perform EMVCo **TTA L1** and L2 tests at Mastercard's discretion at an accredited laboratory as requested by Mastercard.

5.2 Manufacturing (Manufacturer responsibilities)

This section details the responsibilities of the **manufacturing site** or organisation.

5.2.1 General responsibilities

The **Manufacturer** shall plan and carry out production under controlled conditions.

Controlled conditions include, but are not limited to:

- Implementation of contract and agreement (quality and **configuration management**) requirements.
- Standards and procedures to be followed.
- Deliverables exchanged between the different entities.
- Responsibilities and authorities to provide and/or receive deliverables.
- Common reviews to be conducted.
- Review and acknowledgement of purchase orders.
- Control of customer documents, data and equipment.
- Communication procedures are defined.

- The availability of information that describes the characteristics of the **Product.**
- The availability and suitability of work instructions, as necessary.
- The use of suitable equipment.
- The availability and use of monitoring and measuring devices.
- The implementation of monitoring and measurement.
- The implementation of **release** and delivery activities.

5.2.2 Control of documents and records

In addition to the ISO 9001 requirements for documented information, the **manufacturing site** or organization shall ensure that:

- All documentation supplied by the **Vendor** is controlled, including when documentation is updated.
- If the final production test as well as the production acceptance and release records are not supplied to the Vendor, the minimum TQM record retention time applies. (See record control)

5.2.3 Internal audit

In addition to the ISO 9001 requirements, the **manufacturing site** or organization shall ensure that the implementation of the **Vendor**'s requirements are checked where appropriate during the internal audits.

5.2.4 Control of changes

In addition to the ISO 9001 requirements, the **manufacturing site** or organization shall ensure that:

- Changes notified by the **Vendor** are checked, acknowledged, implemented and the implementation is verified.
- Any variation to manufacturing processes shall be approved and validated by the **Vendor**.
- Any variation or change to an **Automated Manufacturing Process** shall be approved and validated by the **Vendor**.

5.2.5 Monitoring and measurement

In addition to the ISO 9001 requirements, the **manufacturing site** or organization shall ensure that:

- Inspection activities are carried out at appropriate points during the manufacturing including any additional instructions by the **Vendor**. Any nonconforming product shall be controlled.
- Quality variance during the manufacturing activities is effectively analyzed as well as ensuring that corrective or preventive actions are made to remedy any deviations.

5.2.6 Control of Nonconforming Product

Any **product** which does not conform to its **product configuration information** or inspection criteria is identified and controlled to prevent its unintended use or delivery. The controls and related responsibilities and authorities for dealing with nonconforming product shall be defined and documented.

Nonconforming product shall be dealt with by one or more of the following ways:

- By taking action to identify the nonconforming product.
- By taking action to separate the nonconforming product.
- By taking action to eliminate the detected nonconformity.
- Evaluate the need for action to eliminate the cause(s) of the nonconformity, in order that it does not recur or occur elsewhere.
- Make changes to the processes or **management system**, if necessary.

5.2.7 Purchasing

If the **Vendor** has authorized the purchasing of part A or part B1 components the **supplier** management requirements apply.

The **Vendor** shall validate requests for alternative components as well as alternate **component manufacturers** not listed on the bill of materials (BOM) or the **Vendor**'s approved vendor list (AVL).

If the **Vendor** has authorized sub-contracted activities within the scope of TQM, the **supplier** management requirements apply.

The **Vendor** shall have sight of all documentation required by the **supplier** management clauses.

5.2.8 Competence

In addition to the ISO 9001 requirements, the **manufacturing site** or organization shall ensure that all personnel are competent to any **Vendor** specific requirements. (e.g. assembly work instructions, software loading procedures, functional test procedures, product acceptance requirements etc.)

Appropriate documented information for competence shall be retained.

5.2.9 Complaints, nonconformity and corrective action

Any complaints or customer reported issues that require investigation, any nonconformities and any corrective actions shall be dealt with in accordance with the ISO 9001 requirements for nonconformity and corrective action.

Records of issues reported by the **Vendor** shall record the **Vendor**'s acceptance of the issue evaluation and any corrective actions.

5.2.10 Manufacturing control

5.2.10.1 Components and Parts control

Purchased components or parts shall be inspected and verified before storage and use in manufacturing.

Inspection should include, but is not limited to: damage, manufacturer name, manufacture location / origin, part numbers, manufacturing date code, logos, font etc.

Components or parts provided by the **Vendor** shall be checked to ensure that it is complete and correct against the **Vendor**'s documentation. These parts shall be stored appropriately to ensure no unauthorised components or parts are used.

Rejected components or parts (with unresolved issues or awaiting return) shall be clearly marked and separated so that they cannot be used in manufacturing.

The kitting process shall ensure that the correct components or parts are used in manufacturing.

5.2.10.2 Equipment control

Equipment shall be controlled, suitable for use and have the appropriate parameters calibrated or verified, with those parameters recorded on a certificate or in a report. These parameters shall be confirmed by the **manufacturing site** or organization that they cover the use of the equipment, before the equipment is put into use or returned into use. This includes **Vendor** supplied equipment.

Note
Parameters are individual data points. A range or specification does not provide enough detail to confirm that the equipment is suitable for use.

Monitoring and measuring devices (equipment) shall be available for use where necessary in the manufacturing facilities.

5.2.10.3 Controls for producing and controlling automated manufacturing processes

The **Vendor** shall ensure that automated manufacturing processes are appropriate for the task being performed. Any variation or change to an **Automated Manufacturing Process** shall be validated and approved by the **Vendor**.

The **manufacturing site** or organization shall make the appropriate documentation and records available to the **Vendor** to support this activity.

5.2.10.4 Controls for producing and controlling production process and assembly documentation

The **Vendor** shall ensure that the **manufacturer**(s) have appropriate process instructions in place. Any variation to manufacturing processes shall be validated and approved by the **Vendor**.

The **manufacturing site** or organization shall make the appropriate documentation and records available to the **Vendor** to support this activity.

5.2.10.5 Final production testing of Products and Implementations

The **Vendor** shall supply the appropriate equipment (if necessary) and instructions for carrying out the Minimum requirements for final testing of **Products** and **Implementations**.

5.2.10.6 Acceptance of production

The **Vendor** shall supply the **Product** Acceptance Plan detailing the criteria to be met to accept **production**. The **product** acceptance plan may be carried out as part of the final inspection or outgoing quality control (OQC) activities.

Product shall not be **released** until the **product** acceptance criteria have been met. The acceptance criteria result and the release authorization for each production batch or lot shall be recorded. The record shall include the name of the person authorizing the release.

5.3 Post manufacturing service provisions (Vendor responsibilities)

5.3.1 Repair levels

The following repair levels are defined for the purposes of managing **service** and repair activities for TQM.

Repair level 1

- Replacement of external parts.
- ECO implementation (external parts, client application updates, key reloading).

Repair level 2

- The **terminal** is opened.
- No soldering activities are carried out.
- Replacement of mechanical parts, pluggable **modules**, housing parts (including any **items** containing part A or B1 components).
- PCB swap (including PCB's containing part A or B1 components).
- ECO implementation (mechanical parts, pluggable **modules**, housing parts).

Repair level 3

- The **terminal** is opened
- Replacement of any part, including:
    - PCB swap (including PCB's containing part A or B1 components).
    - Soldering activities can be carried out (including replacement of part A or B1 components).
- Personalization.
- ECO implementation (All parts including part A and B1 **configuration items**).

5.3.2 Service site categorization

Repair levels 2 and 3 are within the scope of TQM and these **service** sites are category 2 **suppliers** (See supplier management) as determined by the following criteria:

All **service** sites and organizations (that can carry out Repair levels 2 and 3) shall be declared on the VOD along with their region and activity level (percentage of the total repairs in a year, globally and percentage of the total repairs in a year for the region the site is located).

5.3.2.1 Service regions and activity definition

These shall either be up to the three most active **service** sites or if **service** activities are carried out worldwide, the most active site in each region, whichever is greater.

The regions are defined as:

- EMEA – Europe, Middle East and Africa.
- NAR – North American Region (USA, Canada, Mexico, Greenland).
- LAR – Latin American Region (Central America, South America and the Caribbean).
- APAC – Asia and Pacific.

'Most active' is defined as:

- Three most active sites: percentage of the total repairs in a year
- Most active site in each region: percentage of the total repairs in a year for the region the site is located

The **Service suppliers** that meet the requirements above shall be listed in the relevant sections of the VOD.

5.3.3 Service site controls

The **Vendor** shall plan and carry out service under controlled conditions and are responsible for ensuring that the service department, facility or organization meets their responsibilities under the TQM requirements.

5.3.3.1 Validation of processes for service provision

The **Vendor** shall validate any processes for **service** provision.

Validation shall demonstrate the ability of these processes not to alter the conformity of the **Product** to the relevant **Technical Specifications**.

Processes include but are not limited to receiving and screening checks, repair, ECO application, software loading, functional testing, as well as repair records and reporting activities.

The **Vendor** shall ensure that the processes of the **Service** Provider prevent the use of non-approved **Implementations**.

The **Vendor** shall ensure that any servicing activity cannot change the revision of software of the serviced **Product** or component, unless specifically authorized by the design authority.

Vendors shall have a robust process in place for post manufacturing activities including those at **service** or repair centers to ensure that the integrity of the hardware and software will not be compromised. In particular, the **Vendor** shall prevent the use of non-approved combinations of **PCD** hardware and **PCD** software or of **IFM** hardware and **IFM** software.

The **Vendor** shall establish arrangements for these processes including, as applicable:

- Defined criteria for review and approval of the processes.
- Approval of equipment and qualification of personnel.
- Use of specific methods and procedures (including applying ECO's during repair).
- Requirements for records and reports (see Control of Records and **Product** Configuration Status Accounting).
- Revalidation.

5.3.3.2 Service Audits

The **Vendor** shall audit all repair level 2 and repair level 3 service facilities and organisations every 12 months unless another period can be justified. The justification shall be clear and robust. The analysis and conclusion of the justification shall be recorded with the supporting records and / or data.

The **Vendor**'s audit records shall provide evidence that the Post manufacturing service provisions (Service facility responsibilities) have been met.

5.3.3.3 Authorised repairs carried out by the customer

The **Vendor** shall control any authorized repairs by the customer in the same way as an independent **service** site or organization.

5.3.3.4 Post service product release

If a critical component (part A or B1 components or PCB assemblies containing part A or B1 components) has been changed or the software (or firmware) reloaded, then the Minimum requirements for final testing of **Products** and **Implementations** shall be applied before the **products** are **released**.

5.4 Post manufacturing service provisions (Service facility responsibilities)

This section details the responsibilities of the **service** facility or organization.

5.4.1 General responsibilities

The service facility or organization shall plan and carry out **service** / repair under controlled conditions.

Controlled conditions include, but are not limited to:

- Implementation of contract and agreement (quality and **configuration management**) requirements.
- Standards and procedures to be followed.
- Deliverables exchanged between the different entities.
- Responsibilities and authorities to provide and/or receive deliverables.
- Common reviews to be conducted.
- Control of customer documents, data and equipment.
- Communication procedures are defined.

- The availability of information that describes the characteristics of the **Product.**
- The availability and suitability of work instructions, as necessary.
- The use of suitable equipment.
- The availability and use of monitoring and measuring devices.
- The implementation of monitoring and measurement.
- The implementation of **release** and delivery activities.

5.4.2 Control of documents and records

In addition to the ISO 9001 requirements for documented information, the **service** site or organization shall ensure that:

- All documentation supplied by the **Vendor** is controlled, including when the documentation is updated
- If the service records, final test and service release records are not supplied to the Vendor, the minimum TQM record retention time applies. (See record control)

5.4.3 Internal audit

In addition to the ISO 9001 requirements, the **service** site or organization shall ensure that the implementation of the **Vendor**'s requirements are checked where appropriate during the internal audits.

5.4.4 Control of changes

In addition to the ISO 9001 requirements, the **service** site or organization shall ensure that:

- Changes notified by the **Vendor** are checked, acknowledged, implemented and the implementation is verified.
- Any variation to **service** or repair processes shall be validated and approved by the **Vendor**.

5.4.5 Purchasing

If the **Vendor** has authorized the purchasing part A or part B1 components the **supplier** management requirements apply.

The **Vendor** shall validate requests for alternative components as well as alternate **component manufacturers** not listed on the bill of materials (BOM) or the **Vendor**'s approved vendor list (AVL).

The **Vendor** shall have sight of all documentation required by the **supplier** management requirement.

5.4.6 Competence

In addition to the ISO 9001 requirements, the **service** site or organization shall ensure that all personnel are competent to any **Vendor** specific requirements. (e.g. disassembly / assembly work instructions, software loading procedures, functional test procedures etc.)

Appropriate documented information for competence shall be retained.

5.4.7 Complaints, non-conformity and corrective action

Any complaints, customer reported issues that require investigation, nonconformities and corrective actions shall be dealt with in accordance with the ISO 9001 requirements for nonconformity and corrective action.

Records of issues reported by the **Vendor** shall record the **Vendor**'s acceptance of the issue evaluation and any corrective actions.

5.4.8 Service control

5.4.8.1 Returned products, components and parts control

Purchased components or parts (including PCB assemblies) shall be inspected and verified before storage and use in the **service** activities.

Inspection should include, but is not limited to: damage, manufacturer name, manufacture location / origin, part numbers, manufacturing date code, logos, font etc.

Components or parts (includes PCB assemblies) sent as a 'kit' by the **Vendor** shall be checked to ensure that it is complete and correct against the **Vendor**'s documentation. Kit parts shall be stored appropriately to ensure no unauthorized components or parts are used.

Rejected components or parts (with unresolved issues or awaiting return) shall be clearly marked and separated so that they cannot be used in the **service** activities.

The **service** and repair processes shall ensure that the correct components or parts are used.

Returned **product** shall be clearly marked and stored in accordance with the **Vendor**'s instructions whilst awaiting investigation and repair.

5.4.8.2 Equipment control

Equipment shall be controlled, suitable for use and have the appropriate parameters calibrated or verified with those parameters recorded on a certificate or in a report. These parameters shall be confirmed by the service site or organization that they cover the use of the equipment, before the equipment is put into use or returned into use. This includes **Vendor** supplied equipment.

Note
Parameters are individual data points. A range or specification does not provide enough detail to confirm that the equipment is suitable for use.

Monitoring and measuring devices (equipment) shall be available for use, as appropriate, at each repair station.

5.4.8.3 Controls for producing and controlling service processes

The **Vendor** shall ensure that the **service** sites and organizations have appropriate process instructions in place. Any variation to the **service** processes shall be approved and validated by the **Vendor**.

The service site shall make the appropriate documentation and records available to the **Vendor** to support this activity.

5.4.8.4 Post service product release

If a critical component (part A or B1 components or PCB assemblies containing part A or B1 components) have been changed or the software reloaded, then the Minimum requirements for final testing of **Products** and **Implementations** shall be applied before the **products** are **released**.

The **Vendor** shall supply the appropriate equipment (if necessary) and instructions for carrying out the Minimum requirements for final testing of **Products** and **Implementations**.

The repaired **product** shall not be **released** until all records required by the **Vendor** are complete and the Minimum requirements for final testing of **Products** and **Implementations** have been met.

6 Measurement, Analysis and Improvement

This chapter defines requirements for the implementation of processes for measurement, analysis and improvement of the **product** design processes including **configuration management**.

6.1 General requirements

The **Vendor** shall plan and implement the monitoring, measurement, analysis and improvement processes needed to:

- Demonstrate conformity of the **Product** configuration
- Ensure conformity of the **product** design process including **configuration management**
- Continually improve the effectiveness of the **product** design process.

This shall include determination of applicable methods and the extent of their use.

6.2 Interoperability Issues

The **Vendor** shall record any interoperability issue regarding a **Product** by one of its customers, by a subsequent purchaser of the **Product**, or any other involved entity (e.g. Mastercard).

These records shall describe clearly the problems encountered, their causes and corrective actions taken (see Control of Records).

Note:
Interoperability issues include reported bugs.

6.3 Internal audit

New **Vendors** shall complete all internal audits prior to the first audit by Mastercard.

The **Vendor** shall conduct internal audits at planned intervals to ensure that (where applicable) the management responsibility, operation, **product** design, **configuration management**, manufacturing and **service** as well as the measurement, analysis and improvement activities , meet the requirements of this document.

All of the requirements in this document shall be covered, where applicable, at least once every 12 months.

The following shall be defined in a documented procedure:

1. The audit criteria, scope, frequency and audit methods
2. Selection of auditors
3. The responsibilities and requirements for planning and conducting audits
4. Results of the audits are reported to the relevant management
5. Retain documented information as evidence of the implementation of the audit programme and the audit results
6. Follow-up activities shall include the verification of the actions taken and the reporting of verification results

Internal audits shall include a follow up of previous audit results.

The internal audit reports shall, as a minimum, include:

- Date of the audit
- Auditor(s)
- Auditee(s) [e.g. Names, Department or functional area etc.]
- Record which clauses of the TQM requirements were covered in the audit.
- Assessment of previous audit results
- Processes and records examined
- All comments, issues, improvement opportunities and nonconformities found

The conduct of audits shall ensure objectivity as well as impartiality of the audit process. Auditors shall not audit their own work.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes.

Note See ISO 19011:2018 for guidance.

6.4 Monitoring and measurement of configuration processes

The **Vendor** shall apply suitable methods for monitoring and where applicable, measurement of the **Configuration Management System** processes.

These methods shall demonstrate the ability of the processes to achieve planned results. When planned results are not achieved, corrective action shall be taken, as appropriate, to ensure conformity of the **Product** configuration.

6.5 Monitoring and measurement of Product Configuration

The **Vendor** shall monitor and measure the characteristics of the **Product** to verify that configuration requirements for the **Product** have been met. This shall be carried out at appropriate stages of the **Product** life cycle process in accordance with the planned arrangements of the configuration plan.

Configuration audits shall be performed in accordance with documented processes to determine whether a **Product** conforms to its requirements and **Product configuration information**.

Two types of **Product configuration audits** shall be performed in compliance with the planned arrangements:

- A functional **configuration audit**; this is a formal examination to verify that a **Configuration Item** has achieved the functional and performance characteristics specified in its **Product configuration information**;
- A physical **configuration audit**; this is a formal examination to verify that a **Configuration Item** has achieved the physical characteristics specified in its **Product configuration information**.

Configuration or product release records shall be verified that they did not proceed until the planned arrangements (see Configuration Management Planning) were satisfactorily completed and that an appropriate person authorized the release.

6.6 Analysis of data

The **Vendor** shall determine, collect and analyze appropriate data to demonstrate the suitability and effectiveness of the **Management System**, specifically addressing the requirements of **configuration management** and to evaluate where continual improvement can be made. This shall include data generated as a result of monitoring and measurement and from other relevant sources.
The analysis of data shall provide information relating to:

- The compliance with TQM requirements
- Conformity to **Product configuration management** requirements (see Product Design)
- Characteristics and trends of **configuration management** processes including opportunities for preventive action
- Characteristics and trends of **Products** including opportunities for preventive action
- **Suppliers**

Note:
Characteristics and trends of **Products** can include nonconforming **product** data.

6.7 Continual improvement

The **Vendor** shall continually improve the effectiveness of their **Management Systems**, specifically including **configuration management** through the use of the Configuration Management policy, Configuration Management objectives, audit results, analysis of data, corrective and preventive actions and management review.

6.8 Feedback Process on TQM Compliance

For any **Product**, the **Vendor** shall implement a feedback process whose objective shall be to regularly capitalize on information collected on similar projects, on information received from any 3rd party **suppliers**, on feedback from customers or any other reliable source for TQM compliance of current and future projects of the same nature.

Appendices

Appendix 1 - Acronyms

The following acronyms are used in this document:

Abbreviation	Description
AQL	Acceptable Quality Level
CI	**Configuration Item**
CMDB	Configuration Management Database
CMS	**Configuration Management System**
DUT	**Device Under Test**
ICC	Integrated Circuit Card
IFM	**Interface Module**
ISO	International Organization for Standardization
LoA	**Letter of Approval**
ODM	**Original Design Manufacturer**
OEM	**Original Equipment Manufacturer**
PCD	**Proximity Coupling Device**
PICC	Proximity Integrated Circuit Card
SMT	Surface Mount Technology
TID	Type Identification Description
TTA L1	EMVCo **Terminal** Type Approval Level 1
TQM	**Terminal** Quality Management
TVTP	**Terminal Vendor** Testing Process
VOD	**Vendor** Organization Description

Appendix 2 - Terminology

The following terminology is used in this document:

Agent: An Agent for electronic components is an intermediary company that does not hold component stock. If any components are stored, they are not for general sale. The intermediary company can also be another company belonging to the same group as the Vendor, Design, Manufacturer or Service company. Agents will usually place orders with electronic component **Distributors** or **component manufacturer**s on behalf of their customers. Agents can also be called a Broker.

Approval Authority: Person or group of persons assigned responsibility and authority to make decisions regarding the configuration. The Approval Authority can also be called the Dispositioning Authority or **Change Control** Board (CCB). [ISO 10007:2017]

Automated Manufacturing Process: Any process completed by a computer or a machine. Examples include SMT assembly, software loading programs, final production test software etc.

Change Control: Element of Configuration Management comprising the evaluation, coordination, approval and implementation of changes to **Configuration Items** after formal approval of their **Configuration Information**. The change may also be rejected after evaluation.

Component Manufacturer: A company that manufactures electronic components under their own name and /or under brand names.

Concession: A concession is a permission to use or **release** a **product** that does not conform to specified requirements within specified limits for an agreed time or quantity of that **product**. A concession does not affect the configuration baseline. Some organizations use terms such as “waivers” or “deviations” instead of “concession”.

Configuration: Functional and physical characteristics of a **product**, as defined in technical documents and achieved in the **product**.

Configuration Audit: Element of Configuration Management consisting of the verification that a **Configuration Item** conforms to its **Configuration Information**.

Configuration Identification: Element of Configuration Management consisting of selecting the **Configuration Items** for a **product**, assigning unique **identifiers** to them and recording their functional and physical characteristics in technical documentation (**Configuration Information**).

Configuration Information: Requirements for **product** design, realization, verification, operation and support. **Product** configuration information comprises both **product** definition and **product** operational information. [ISO 10007:2017]

Configuration Item (CI): Entity within a Configuration that satisfies an end use function. [ISO 10007:2017].

Configuration Item Baseline: Approved **Configuration Information** that establishes the characteristics of an **item** at a specific time in the **item**’s life cycle and that serves as reference for activities throughout the life cycle of the **item**.

Configuration Management: Coordinated activities to direct and control Configuration. [ISO 10007:2017]

Configuration Management System: Systems, processes and tools used to control and manage **configuration items** and **configuration information**.

Configuration Status Reporting: Element of Configuration Management consisting of formalized recording and reporting of information needed to manage a configuration efficiently. This information consists of approved **Product Configuration Information**, the status of proposed changes to the configuration and the implementation status of approved changes. [ISO 10007:2017]

Configuration Tree: Document showing the hierarchical path from an **item** down to selected lower level CIs constituting this **item**. The **Implementation** configuration tree identifies the Implementation - ID down to the Implementation hardware ID and Implementation software ID declared in the **Letter of Approval** for **Terminal** Type Approval Level 1 and down to their lower level **configuration items**.

Critical Configuration Items: PCD / **IFM** Part A and B1 components as defined in the 'Configurations **Items**' section.

Distributor: An electronic component distributor supplies components from multiple **Component Manufacturers** from their own stock (warehouse) and supply multiple electronic equipment manufacturers. Distributors can also be known by other names such as resellers, retailers, stockists etc.

Device Under Test (DUT): Product that was manufactured and submitted for testing to EMVCo **TTA L1** (includes debug testing prior to the formal TTA run).

Fit: The ability of an **item** to physically interface, or interconnect with, or become an integral part of another **item**.

Form: The defined configuration of an **item** including the geometrically measured configuration, density and weight or other visual parameters which uniquely characterize an **item**, component or assembly. For software, form denotes the language, language level and media.

Function: The action or actions which an **item** is designed to perform.

Identifier (ID): Identifying number which uniquely identifies an **item** (part number) or a document.

Interface Module (IFM): Implementation of the **Technical Specifications** for Contact **Terminal** Level 1.

Intermediary company: An intermediary company is a company the **Vendor** has an agreement with to facilitate services covered by the TQM requirements. The intermediary company has the agreement with the company supplying the services covered by the TQM requirements (e.g. a **Vendor** uses an intermediary company in Hong Kong to gain access to a manufacturing company in China). As long as the intermediary company does not perform any work that can affect product configuration, then the intermediary company need not hold ISO 9001 certification (or equivalent).

Implementation: Means the combination of hardware and software sub-sets of the **product** implementing the **Technical Specifications**. It is also called Part A in this document.

Implementation's environment (or Part B1): Component(s) of the **Product** that are not part of the Implementation but interface with the Implementation (for example used by or connected to the Implementation) or have a direct impact on the behavior of the Implementation.

Interchangeability: Two **item**s of a **product** are interchangeable when:

- the **Fit**, **Form** and **Function** of the superseded and superseding **item**s meet the **product** specifications, these previous criteria are met both way (old in the new and vice-versa) and
- these previous criteria are met with no special measures to the **item** or related **item** and in all applications (where used).

Interface: The functional and physical characteristics required to exist at a common boundary. Within an organization, a relationship among two or more entities in which the entities share, provide, or exchange data. Interfaces are not **items** but relationships between them.

Item: Non-specific term used to denote any **product**, including systems, subsystems, assemblies, sub-assemblies, units, sets, accessories, components, computer programs, computer software or parts.

Letter of Approval (LoA): See "**Terminal** Type Approval Level 1 Letter of Approval".

Management System: A set of interrelated or interacting elements of an organisation to establish policies, objectives and processes to achieve those objectives.

Manufacturer: Entity responsible of the manufacturing of the **product** and / or a **module**. The Manufacturer can be a **Supplier** or a **Vendor** entity.

Manufacturing qualification process: This is a **Vendor** process to define the pre-production steps and checks required in order for the **Vendor** to approve the start of **production** for a **product** or **module**.

Manufacturing site: A manufacturing site or organisation (which includes a Vendor manufacturing department) may be a **Vendor** or **supplier** entity. Manufacturing activities included in TQM (but not limited to) are PCB assembly, Component and **Product** assembly, Software loading, Functional testing, Production acceptance.

Module: IFM or PCD devices embedding Contact, Contactless or both payment technologies. A Module may also be referred to as a Component [See TQM/GEN/T01].

Original Design Manufacturer (ODM): An ODM is a company that designs and builds a **product** or **module** to its own specifications.

Original Equipment Manufacturer (OEM): An OEM is a company that designs and builds a **product** or **module** to another company's specifications.

Proximity Coupling Device (PCD): Implementation of the **Technical Specifications** for Contactless **Terminal** Level 1.

Product: Device embedding the **Implementation** and the **Implementation Environment**. It can be either a **terminal** or a standalone card reader.

Production: The period after pre-production when components, modules, products etc. are produced (usually for customers).

Release: Distribution of **Configuration Information** from one entity to another.

Sample: Product picked out of manufacturing for testing.

SMART: A way of defining objectives that can contribute to the clarity and success of the objective. SMART stands for Specific, Measurable, Achievable, Relevant, Time-bound.

Statement of Compliance: Document issued by Mastercard via the Assessment Body and renewed annually, which lists the Labels issued to the **Vendor**.

Service: Any post manufacturing activity where software loading or PCB changes containing part A or part B1 **configuration items** occur as well as any part A or part B1 component replacement. Service can also be called (but not limited to) repair, refurbishment, return market authorisation (RMA) etc.

Supplier: Entity having an agreement with the **Vendor** (or a Vendor's Supplier) for the design, development, manufacture, maintenance, **service**, repair, modification or supply of **items** or components.

Supply Chain: The sequence of entities and processes involved in the production and distribution of **items** in order to manufacture, supply and repair **products**.

Technical Specifications: Document defining the specifications against which an **implementation** is tested and approved for EMVCo **TTA L1**.

Terminal: Device used at the point of transaction to perform a financial transaction and incorporating the host communication. It may also include other interfaces and **Implementations** or be connected to other devices (Card Readers) containing needed **Implementations**.

Test Laboratory: A facility accredited by EMVCo for performing **TTA L1** or **TTA L2** tests and / or by Mastercard for performing Mastercard L2 tests.

Test Report: Report documenting the results of tested representative samples during formal or debug TTA L1 testing session by an accredited Test Laboratory.

Terminal Type Approval Level 1 Process (EMVCo **TTA L1 Process):** Process used by EMVCo to verify and acknowledge that an **Implementation** within a **Product** is compliant with the relevant **Technical Specifications**.

Terminal Type Approval Level 1 Letter of Approval (EMVCo **TTA L1 LoA):** Written acknowledgement by EMVCo that the **TTA L1** Test results for **Vendor**'s **Implementation** are in sufficient conformance with the relevant **Technical Specifications**.

Terminal Type Approval Level 1 Test (TTA L1 Test): Set of tests established by EMVCo to determine whether an **Implementation** meets the requirements of the related **Technical Specifications**.

Terminal Type Approval Level 2 Test (TTA L2 Test): Set of tests established by EMVCo (EMVCo L2 contact type approval) & Mastercard (Mastercard L2 Contactless Approval) to determine whether an **Implementation** meets the requirements of the related **Technical Specifications**.

TQM Label: Formal recognition from Mastercard that **Products**:
(1) which embed a specific **Implementation** which has been granted an EMVCo **TTA L1 LoA**,
(2) designed by the owner of this **LoA**
(3) and produced in specified **manufacturing sites**, are compliant with TQM requirements [TQM/GEN/T02].

See also: SoC (**Statement of Compliance**)

Traceability: Ability to trace the history, application or location of that which is under consideration.

Vendor: Entity responsible for the design, development and production of **Products** or **Modules**.
In cases where the design is sub-contracted (in full or in part) to another entity, although the **Vendor** is ultimately responsible for the requirement, "**Vendor**" can be read as "design authority".
The Vendor is the entity requesting **TQM Label** for an **Implementation**. If this request is accepted, the Vendor is the owner of the **TQM Label**.

Appendix 3 - Technology-specific Terminology and Information

Contact Terminal Level 1

Implementation Name: **Interface Module** or **IFM**

Definition: Virtual or abstract **Implementation** that contains the necessary hardware and software to power the ICC and to support communication between the **Product** and the Integrated Circuit Card (ICC) up to the transport layer, as specified in the Technical Specifications.

Contactless Terminal Level 1

Implementation Name: **Proximity Coupling Device** or **PCD**

Definition: Peripheral **Implementation** of the **Product**, that uses inductive coupling to provide power to a Proximity Integrated Circuit Card (PICC) and also to control the data exchange with the PICC, up to the transport layer (included), as specified in the **Technical Specifications**.

Appendix 4 - Guide to the required VOD supporting documents

The following is a guide to the documents required to support the VOD assessment.

ISO 9001 Certificate (for each applicable site and organisation; e.g. Vendor, design, manufacturing and service sites)
Configuration Management Policy
Management review procedure / agenda / report template (as appropriate)
Document and Record Control Procedure
- Including baseline and configuration information retention time

Naming and Numbering Conventions
Internal Audit Procedure

Product design process(es), including:
- Processes for managing configuration
- Sequence and interaction of the design and configuration management processes
- Product life cycle model including baseline and product configuration status recording activities

Change Control Process
Change control forms (e.g. ECR / ECN)

Implementation configuration management plan template

Manufacturing qualification process
Supplier management process, including:
- Managing an IFM or PCD OEM supplier [if applicable]
- Managing external services (HW or software design) [if applicable]
- Managing manufacturing suppliers
- Managing suppliers for software loading and / or final testing (if separate from the manufacturing location)
- Managing part A and B1 component suppliers (even if a supplier purchases A and B1 parts [e.g. a manufacturing supplier])
- Managing the purchasing (controls) of part A and B1 components
- Managing repair / service suppliers

Service control process, including:
- Validation of the processes for service provision

Monitoring, measurement, analysis and improvement process(es)
Configuration audits process
Nonconforming product procedure

Note:
The content of mandatory processes may be in documents of different titles (e.g. Configuration Management Manual, Quality Manual etc.). If this is the case, please provide these documents, noting the relevant paragraphs of the document that relate to the VOD question.

Appendix 5 - Guide to the required TID supporting documents

The following is a guide to the documents required to support the TID assessment.

Implementation (IFM or PCD) configuration management plan

Hardware block diagram
Hardware configuration tree
Circuit diagram (Schematic)
Bill of materials (including manufacturer name and MPN for Part A and part B1 components)
All hardware change documentation since the L1 LoA (E.g. ECR, ECN and supporting documentation)
All software change documentation since the L1 LoA (E.g. ECR, ECN and supporting documentation)
PCB Layouts
Antenna details (*PCD only*)
Hardware integration rules (e.g. exploded diagram or assembly drawings)

Software block diagram
Software configuration tree
List of Part A and Part B1 software modules (including versions or release date and time)
Software integration rules (software / firmware loading process)

Product acceptance plan
Product acceptance record (template or representative record)

EMVCo L1 LoA

For a terminal:
Clear photographs of the exterior of each terminal embedding the **IFM** or **PCD**.

For a module:
Clear photographs of the exterior of each module (**IFM** and / or **PCD** as appropriate).