VDA QMC

German Association of the Automotive Industry
Quality Management Center

Quality Management in the Automotive Industry

Product Compliance

Volume 2: Product Safety and Product Conformity

1st edition, November 2025
Online download document

Quality Management in the Automotive Industry

Product Compliance

Volume 2: Product Safety and Product Conformity

1st edition, November 2025
Verband der Automobilindustrie e. V. (VDA)

Imprint

ISSN 0943-9412

Verband der Automobilindustrie e. V. (VDA)
Quality Management Center (QMC)
Behrenstraße 35
10117 Berlin

Non-binding VDA recommendation

The German Association of the Automotive Industry (VDA) recommends that its members apply the following VDA volume when introducing and maintaining QM systems.

Disclaimer

This VDA volume reflects the technical procedures known at the time of its respective edition. The contents therefore represent the knowledge and views of the authors at the time of publication. Although the information has been prepared with the greatest possible care, no claim is made for factual accuracy, completeness, and/or timeliness; in particular, this publication cannot take into account the specific circumstances of individual cases. Use of the information is therefore at the reader's own responsibility. Applying the VDA recommendations does not relieve anyone of responsibility for their own actions; all act on their own responsibility.

Liability for the content and application of this VDA publication and for the persons involved in preparing the VDA recommendations is excluded.

Anyone who, when reading or applying these VDA recommendations, encounters inaccuracies or the possibility of misinterpretation is requested to inform the VDA immediately so that any deficiencies can be corrected.

Copyright Protection

Translations

The German document is the original. In the event of interpretive questions in other language versions, the German version shall be referred to as the original. This publication will also appear in other languages. The current version can be obtained from VDA QMC.

Gender Note

For reasons of readability, the masculine form is used for personal designations; however, the feminine form is always implied.

Contents

4

1 Introduction

The common goal of the VDA and its members is to continuously ensure the *compliance* of their *products* in a global market, while protecting people and the environment and preventing hazards. For the purposes of this recommendation, *Product Compliance* (*PC*) includes so-called *binding obligations*, i.e. all applicable legal obligations and obligations voluntarily entered into by the company.

Product Compliance is crucial for a company's business success and should therefore be ensured for the *products* provided. This refers to systems, hardware, software and/or services.

Products are becoming more and more complex, there is a growing number of statutory and regulatory requirements, and interdependencies in supply chains are increasing. In order to meet these requirements, companies need elements helping them to identify, monitor, control and minimize product-related risks. A *Product Compliance System* (*PCS*) is used for this purpose, which is intended to enable the organization to identify and minimize potential risks at an early stage. The detailed description can be found in the VDA Volume “Product Compliance - Volume 1: Product Compliance System”.

The *PCS* is based on the *Three Lines Model* and describes the governance function (*Second Line*), while this VDA volume describes the tasks of the operational departments (*First Line*) derived from the *PCS*. People who take on these tasks are called *Product Safety and Conformity Representatives* (*PSCR*). It is at the discretion of each company to delegate these tasks through appropriate processes to one or more individuals, functions, or roles within the organization.

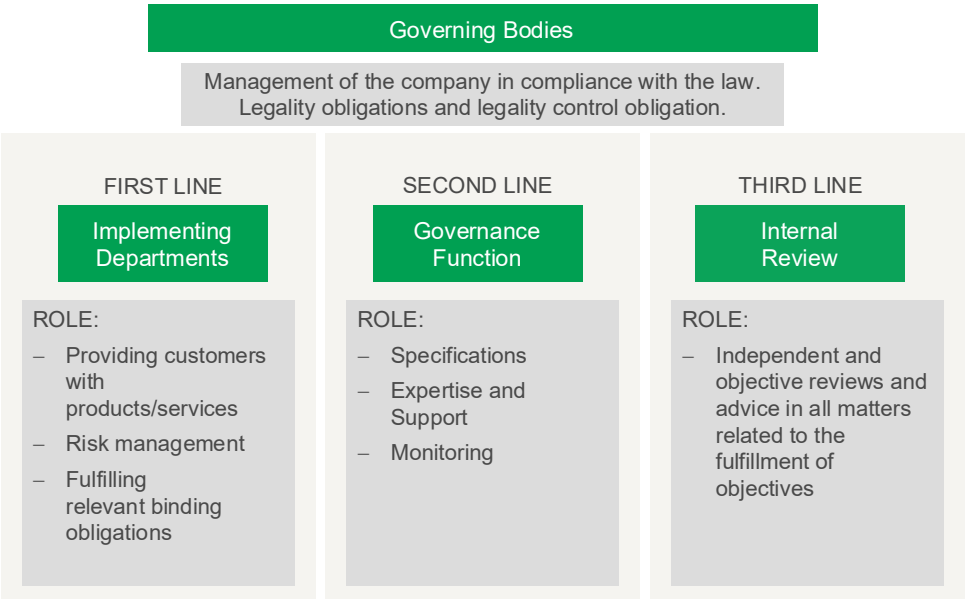

Figure 1-1: Three Lines Model based on the IIA

As part of the first line, the *PSCRs* are responsible for implementing the guidelines issued by the *second line* and company management.

The regulations presented in this volume do not have any bearing on quality assurance systems (such as DIN/EN ISO 9001 or IATF 16949). In particular, they do not serve to interpret or evaluate quality assurance or *QM systems*.

2 Fundamentals

2.1 Definition of Product Compliance

This volume replaces the earlier VDA Volume “Product Integrity”.

The term *Product Integrity* is replaced by the term *Product Compliance*.

Product Compliance means adhering to the *binding obligations* applicable to a company's *products* throughout the *product life cycle*, from innovation to end of use, including product recycling. A distinction is made between legally binding, supporting norms and standards and supplementary voluntary commitments (see VDA Volume "Product Compliance – Volume 1: Product Compliance System", 1st edition, November 2023, Chapter 2.3).

Product Compliance includes *product conformity* and *product safety*, as shown in the following diagram.

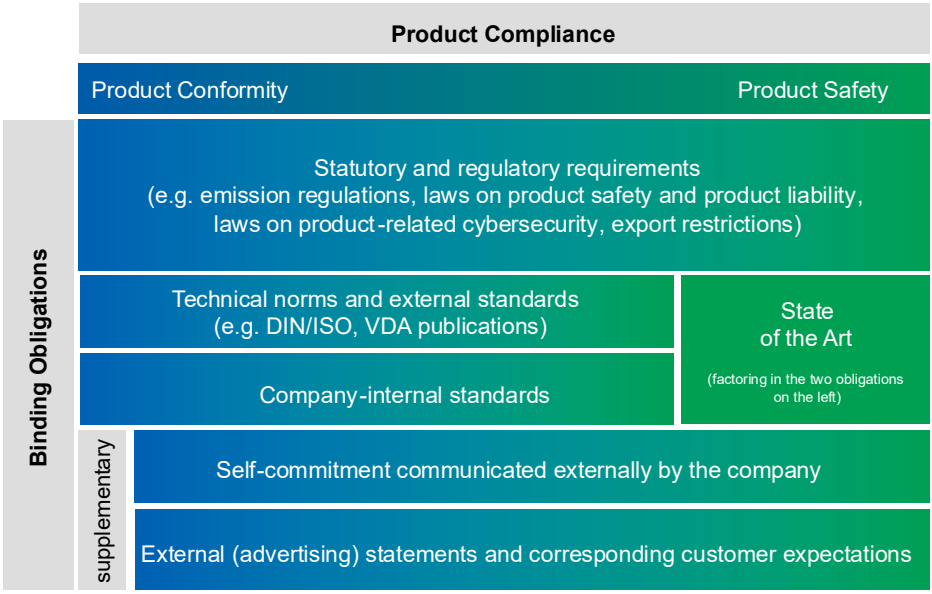

Figure 2-1: Definition of Product Compliance

Product compliance refers to the fulfillment of *binding obligations* necessary for *placing a product on the market*. The term *placer on the market* potentially includes all manufacturers within the supply chain. The term *product* encompasses complete vehicles, accessories, spare parts, software, or other items made available on the market.

In the supply chain, a distinction is made between suppliers (Tier-n) and vehicle manufacturers (OEM). In some cases, different responsibilities arise for these. The responsibilities for OEMs described in this volume may also affect suppliers if they offer their own *products* on the market.

Product safety also includes the fulfillment of the legitimate expectations of the users and other affected persons as well as expectations pertaining to safety and environment during intended and foreseeable use throughout the *product life cycle*. The state of the art must be observed.

Figure 2-2 provides an illustrative overview of legal and regulatory requirements as well as technical norms and standards. Since it is not always possible to clearly categorize requirements as pertaining to either *product safety* or p*roduct conformity*, a holistic view of *Product Compliance* is recommended. There are regulatory topics, such as cyber security, from which requirements can emerge both in terms of *product safety* and *product conformity*.

Other VDA volumes explain methods and processes that contribute to achieving *Product Compliance* (e.g., *Lessons Learned*, Product and Process Audits, Special Characteristics).

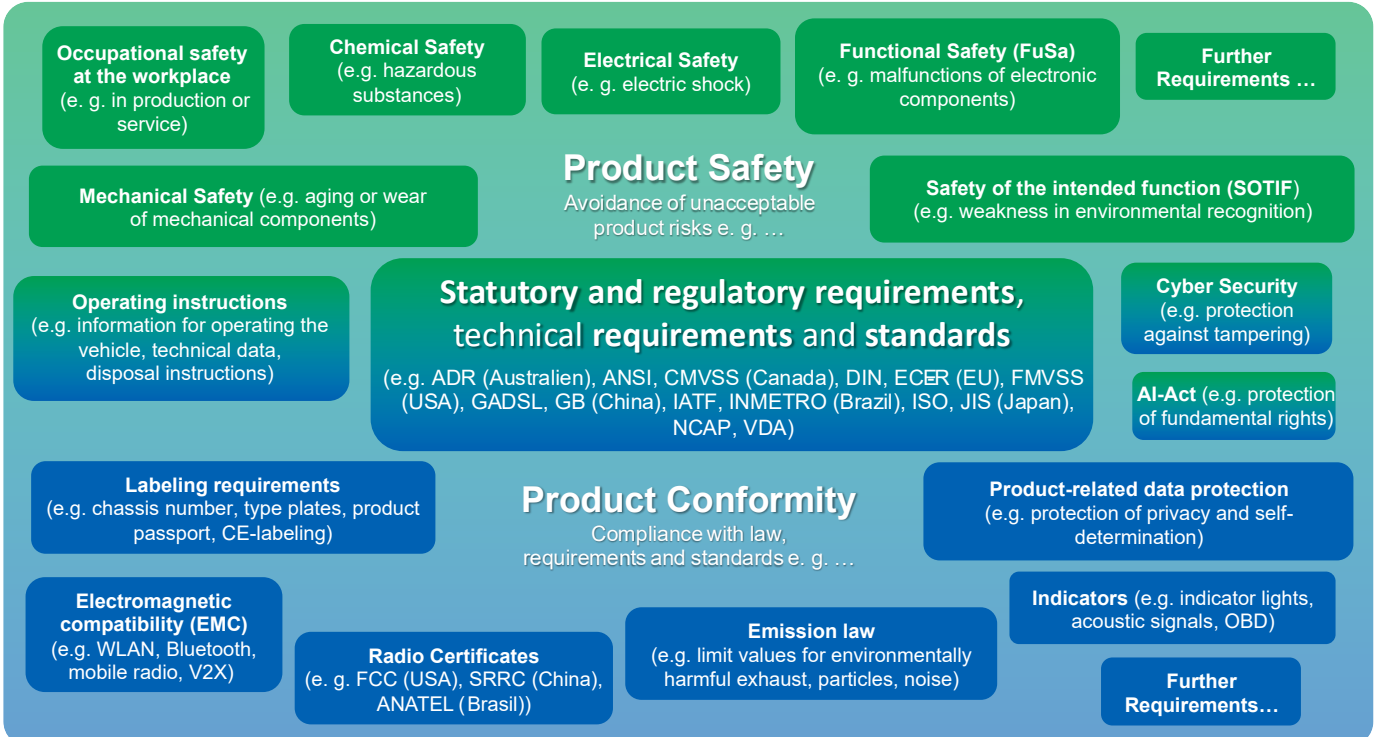

Figure 2-2: Exemplary overview of product safety and product conformity requirements

2.2 Role of the PSCR in the Organization

The *Product Compliance* of *products placed on the markets* is the responsibility of the company's *management bodies*. As a rule, this responsibility is not delegable. The associated tasks and powers can be assigned to operative departments. It is the duty of the *management bodies* to ensure, within the framework of their *legality control obligation*, that the company complies with the rules.

If *PSCR*s are described below, this applies to persons designated as *PSCR*s by management. These *PSCR*s perform *PC*-related tasks defined by the *PCS* themselves or transfer them to other persons who act in a *PSCR role*. These individuals form the *PSCR network* with *PSCR* as the central interface. During implementation, existing organizational structures and terminology can be used, and activities and responsibilities can be integrated into them.

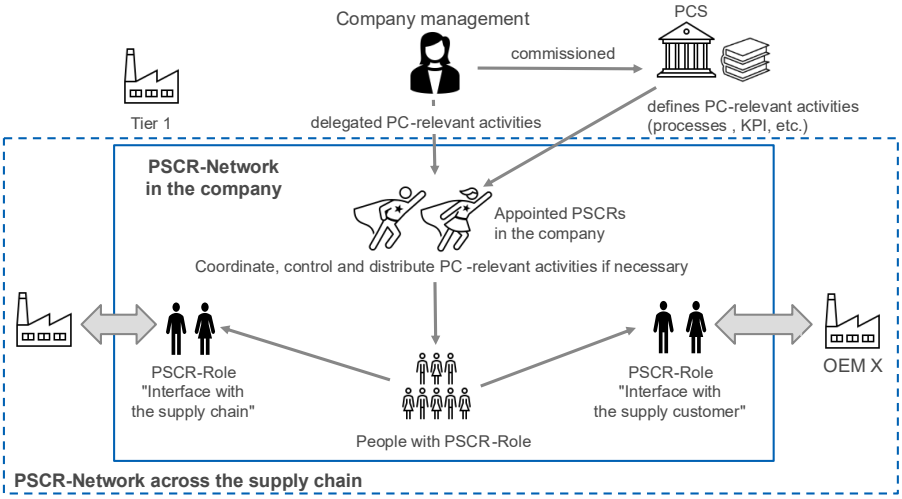

Figure 2-3: Schematic representation of a PSCR network in an enterprise using the example of a Tier 1 supplier (transferable to the entire supply chain)

3 Elements of Product Compliance

The following subsections describe the tasks of the *PSCR role* based on the seven elements of the *PCS* – regardless of the specific implementation in the company. An overview of the main *PSCR* tasks is provided in Figure 6-1.

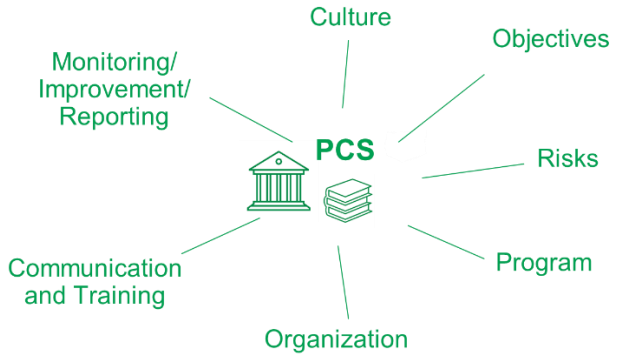

Figure 3-1: Seven elements of PCS

3.1 Culture

The *Product Compliance culture* (*PC culture*) anchored in the corporate values (see VDA Volume “Product Compliance – Volume 1: Product Compliance System”) must be integrated into daily processes through the *PSCR network* and communicated to all employees. The top priority is to prevent non-compliance in the *products*.

The *PC culture* serves as a guide for questions and decision-making. When conflicts arise between different objectives (e.g. deadlines, costs, *quality*), it is crucial to have a company culture in which employees are encouraged to openly address and resolve their concerns, including any *Product Compliance* issues. It is also important to reinforce and promote a positive error and *lessons-learned* culture as well as an awareness of *Product Compliance* requirements among all employees. All employees must be informed that early active intervention in the event of potential non-conformances is desirable and necessary and will never

result in any negative consequences for them personally.

In the interest of *Product Compliance,* the *PSCR network* calls for integrated, responsible and value-oriented practices in all areas. The people in the *PSCR* network should be role models for all employees.

The following are measures that are essential for a *PC culture* and that should support and further develop the individual *PSCR* and the *PSCR network* with their activities:

- through regular training, inform employees about the *Product Compliance* and the importance of *compliance*.
- ensure the implementation of the measures through the appropriate monitoring activities.
- communicate an open error culture and point out (anonymous) reporting system.

The *Product Compliance culture* thus forms the basis for all the following elements.

3.2 Objectives

Performance objectives and key figures are the basis for continuously measuring, controlling and improving the effectiveness of the implementation of the *First Line* requirements defined by the *PCS*. The defined *PC key performance indicators* (*PC KPIs*) support the transparent display and monitoring of the activities of the *PSCR network*.

They also form the basis for regular reporting and the determination of necessary actions. The overarching objectives and key figures are jointly defined by *First Line* and *Second Line* (see Chapter 3.7.1). The *First Line* periodically records the previously agreed *PC KPIs* in their area of responsibility and makes them available to the organization. The frequency of *PC* target review follows a risk-based approach and can be part of an annual management review.

The respective *PSCR role* is responsible for *Product Compliance* in its area and

collects and monitors the corresponding performance objectives and controls the definition and implementation of measures in the event of non-conformances.

3.3 Risks

Each *product* implicitly includes *Product Compliance risks* (*PC risks*). Therefore, *risk management* is imperative in order to identify, assess and manage *Product Compliance* issues on an ongoing basis in an appropriate and effective manner. A *PC culture* creates the basis for enabling employees to address identified *PC risks* openly and without fear.

The *PSCR role* is a point of contact for *Product Compliance* issues and should have the appropriate level of expertise to assess *PC risks*.

A central element of this competence is the understanding of cognitive biases – systematic errors of thought that unconsciously influence our perception and decisions. Our brain essentially uses two thinking strategies: fast, intuitive thinking (System 1) and slow, analytical thinking (System 2).[1]

System 1 works efficiently and avoids overloading the brain with too much unnecessary information. At the same time, fast thinking can lead to problematic hasty decisions, such as confirmation bias, in which only information that supports existing assumptions is considered. Another cognitive bias is the availability heuristic, in which decisions are made based on information that is particularly easy to retrieve or emotionally present – even if it is not statistically representative.

These and many other cognitive distortions cause some information to be overstated, while others are neglected. This leads to risks being misjudged. It is therefore essential for *PSCR* to be aware of these traps. This can be remedied by activating System 2 using methodically conducted risk analyses, viewing from different perspectives and targeted training on risk perception.

Therefore, *PSCR*s know and apply appropriate methods for the qualitative and/or

[1] See Daniel Kahneman, *Thinking, Fast and Slow*, 2011

quantitative assessment of *PC risks*. If possible, the implementation should follow recognized standards. This promotes acceptance of the result and makes it possible to compare *PC risks* with one another. At the same time, decisions with regard to countermeasures can often be made faster, more transparently and more precisely. The experience of the risk assessor is of enormous value.

*PSCR*s work according to the processes defined in the *PCS*. Depending on the time in the *product life cycle*, the role model in the company and the position in the supply chain, the tasks assigned to the *PSCR*s may be different. Systematic and timely identification, analysis and assessment of *PC risks* is always an integral part of the task portfolio and accompanies the entire *product life cycle*.

During product development and before the start of production, *PC requirements* are determined from the *binding obligations* and, if necessary, converted into product requirements (see Chapter 3.4.3). This is done either specifically for individual *products* or based on construction and function groups. The responsible *PSCR roles* ensure that this is fulfilled before *placing on the market*.

In the ongoing production process and after *placing on the market,* however, *PC risks* must be assessed and mitigated (see Chapters 3.4.4 and 3.4.5). If a non-conformance is reported, potential *product safety* or *conformity* non-conformances are first verified and presented objectively. The subsequent analyses cover all the findings and, depending on the subject, require cooperation between the relevant areas such as e.g., development, production, quality assurance, homologation and law. The affected parties in the supply chain must cooperate to the extent reasonable and necessary and are involved in the analyses as well as the assessment of the results accordingly. The *PC risk* assessment is performed based on these analyses. The final assessment of *PC risk* in the overall system is carried out by the overall system manufacturer. Suppliers should be appropriately informed of the outcome so that they can assess whether any actions are needed on their part, e.g. required reporting. In any case, the results must be carefully documented in order to ensure complete traceability. If a relevant *PC non-conformance* is identified in the risk assessment, the *PSCR*s usually lead to a decision on an appropriate measure. A defined decision-making body is convened for this purpose. The scope of the decision-making options depends on the role that each company plays in its business activities.

Examples of possible reactions to a *PC risk* in *products* already delivered to end customers (here: vehicle users) include:

- Offer to carry out a service task during the next workshop visit
- Offer to carry out an OTA-Software-Update (Update over the air)
- Service task with customer notification (timely appointment)
- Recall with *customer* notification

In any case, it must be checked whether there is a reporting obligation to an authority (see also Chapter 3.6.1.3).

All documents relevant to the decision must be kept in accordance with the process specified by the *PCS*. Where an appropriate risk mitigation measure is adopted, the *PSCR*s shall ensure its implementation. The implementation and effectiveness of the measures should be monitored by a sufficiently independent body.

Ultimately, the *PSCR*s manage *PC risks* consciously and thus make an important contribution to *Product Compliance*.

3.4 Program

Within the *PCS*, the term program refers to all activities and processes within the company that aim at achieving, maintaining and monitoring *Product Compliance*.

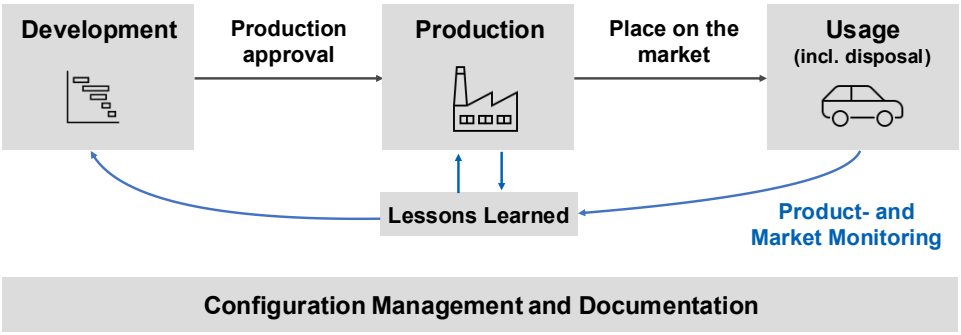

Figure 3-2: Product Compliance throughout the product life cycle

Throughout the *product life cycle* (see also VDA maturity model[2],) *PSCR*s should be included in processes in order to ensure and maintain *Product Compliance* according to their responsibilities and powers, depending on activity or specific events.

The following chapters discuss *Product Compliance* over the *product life cycle* (see Figure 3-2). Product-related security issues that arise from the corresponding regulatory requirements, such as cyber security and theft protection, must also be taken into account.

3.4.1 Configuration Management

Comprehensive configuration management generally means controlling, managing and documenting changes in complex systems throughout the *product life cycle*.

This includes continuously steering and checking adjustments, corrections and additions. The respective system and all its components should always be clearly

[2] See VDA Volume *Maturity level assurance for new parts – Methods, measurement criteria, documentation*, 3rd, revised edition, June 2022.

defined, documented and traceable to the origins.

Configuration management is thus essential for a systematic, consistently transparent *product life cycle*. Even the smallest changes to the process or *product* can have far-reaching consequences. It is therefore necessary to establish responsibilities, e.g. release responsibilities, depending on the scope of the change either in the *PCS* or by the designated *PSCR*. Market-specific regulatory requirements must be observed [e.g. KBA (German federal authority for road traffic), Ministry of Industry and Information Technology (MIIT), China's State Administration for Market Regulation (SAMR)].

Examples of proper configuration management:

- version management (e.g. new update after design change)
- change management (e.g. ability to check when the *products* underwent a change)
- support for *product* or assembly or function group selection under *PC requirement* (traceability)
- build and release management (e.g. traceability of the software modifications)
- process changes/adjustments (e.g. documentation of utilized auxiliary substances and operating materials)

If questions affecting *Product Compliance* arise from the context of configuration management, the respective *PSCR role* should be consulted.

It is recommended that any evidence generated be documented and retained in accordance with the company-specific guidelines.

3.4.2 Documentation

Adequate documentation of all *PC*-related processes is essential. *PCS* provides a structured, end-to-end description of all relevant processes, including standardized forms. Integration into the company's internal storage system and protection against tampering with data and records by unauthorized persons must be taken into account.

The respective *PSCR role* ensures that a minimum duty of care is applied when preparing documents, in particular in connection with *PC*-relevant content, in order to ensure general traceability.

Minimum requirements related to *Product Compliance* include the following:

- neutral, fact-based data collection
- creation of meeting reports
- decisions must be documented in a comprehensible manner
- in-house rules for internal communication and external communication with government authorities and other supervisory bodies
- comprehensible documentation of changes related to *PC* such as adjustments, corrections and additions to *products* and/or manufacturing processes
- retention periods due to legal requirements and customer requirements must be taken into account (see also VDA Volume 1 – "Documented information and retention")

Once they are issued as a documented version, documents can no longer be modified. Changes to previous versions must be clearly indicated.

Open issues shall be tracked by the respective *PSCR role* and verifiably submitted for final assessment.

Documentation of the entire *PC* activities from the detection of a *PC non-conformance* to the elimination of the *PC non-conformance* have to be documented by the respective *PSCR role* (e.g. according to VDA Volume "8D – Problem Solving in 8 Disciplines").

Contents of the documentation must be defined taking into account internal and regulatory requirements and coordinated in the supply chain if necessary. In doing so, it is important to ensure that information and data management is consistent (traceability) in order to meet the requirements arising from regulations such as the digital product passport.

Documentation of *PC* activities can be integrated into the document management systems (DMS) already in place in the organization, provided that they meet the

above requirements. A dedicated document management system is not required.

3.4.3 Development

During the development phase the *PSCR role* ensures that responsibility for identifying and implementing *PC requirements* is defined according to the *PCS* processes. This includes determining the product requirements necessary to comply with the *binding obligation* and identifying appropriate sources for these requirements (see Figure 2-2). The *PSCR role* ensures the implementation of the *PC requirements* and initiates the decision-making-process on measures in the event of identified non-conformances.

The following description provides a basic guide to identifying and implementing *PC requirements* along the *product life cycle* (for further details, see practical example in Chapter 5.3).

Definition of product scope including *target sales markets*

The product scope definition includes the *product*, the proposed application, and the *target sales markets* in which the *product* will be sold. All phases of the *product life cycle* (e.g. manufacturing, operation, maintenance, recycling, scrapping) shall be taken into account. *Product Compliance* also extends to any necessary market-specific requirements for *products* and product descriptions, such as component markings and recycling and disposal requirements.

Identification of guidelines for development plans

These findings are then used to obtain the generally applicable *PC requirements* for the *product* (incl. its traceability) and, if necessary, the processes utilized. This includes *compliance* with all relevant *binding obligations* (see Figure 2-1). In this case, insights from previous projects (*lessons learned*) must also be taken into account (see Figure 3-2).

Translation of the guidelines into technical specifications (requirements)

and implementation

The analysis and interpretation of the *PC requirements* then leads to the creation of specific technical individual requirements for the *product* and the process and to their implementation.

Review/assessment of *compliance* with requirements in development

The verification of *compliance* with the derived technical requirements (project milestones) is intended to ensure that *Product Compliance* is being achieved in the development phase. This can also pertain to the approval of templates and pre-series stages. Product release also confirms *Product Compliance* with regulatory requirements (such as type approvals and other product certifications).

Documentation

Appropriate documentation and filing of the identified requirements with reference to the original source of the requirement is necessary in order to be able to demonstrate which *PC requirements* were valid at the time of *placing products on the market*.

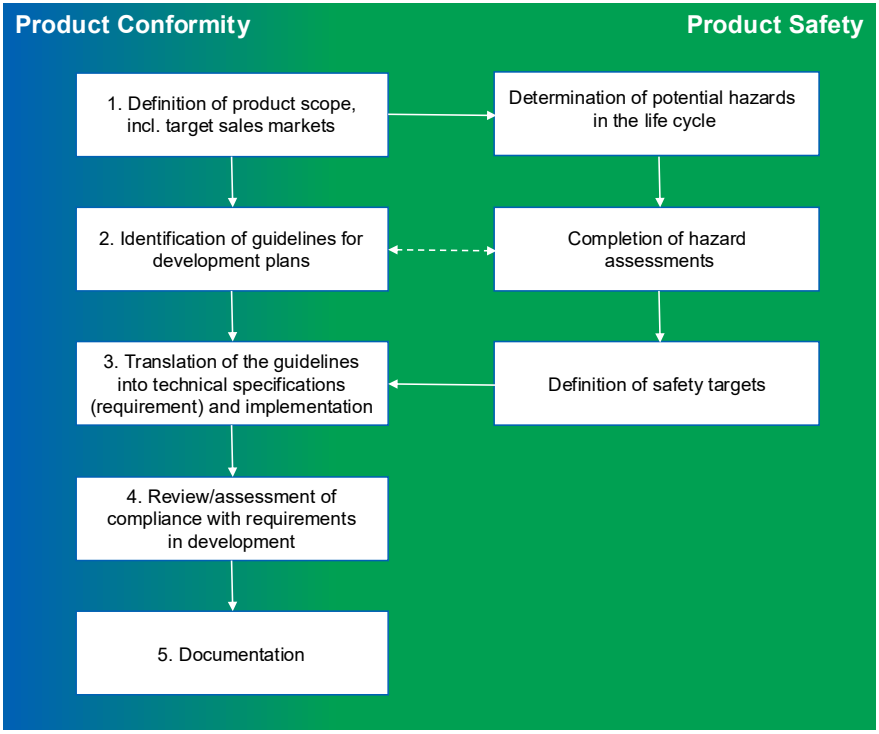

Figure 3-3: Procedure in development for determining and implementing PC requirements

Identifying potential hazards in the *product life cycle*

With regard to *product safety,* the potential hazards for each *product* or system in the *product life cycle* shall be systematically identified. This includes various categories of potential causes of danger, for example:

- intended and foreseeable use
- functional and non-functional non-conformances
- functional dependencies
- tampering

Completion of hazard assessments

For each identified potential hazard due to a non-conformance, a hazard assessment shall be performed for all relevant *product life cycle* phases. An established procedure is the derivation of ASILs (Automotive Safety Integrity Level) for functional non-conformances according to ISO 26262. Non-functional non-conformances can be considered, for example, according to ISO 12100. The risk assessment is carried out in a systematic and comprehensible manner. The affected suppliers in the supply chain contribute to this risk assessment with the necessary information on their own responsibility and assess potential risks limited to their area of responsibility. Appropriate account should be taken of interfaces and intended use.

Defining *safety objectives*

The identified relevant hazards result in *safety objectives.* These *safety objectives* shall be accompanied by an attribute that is traceable throughout the *product life cycle* (e.g. "Special characteristics with safety relevance"). In addition, where possible, *safety objectives* should be quantified, e.g. FTTI (Failure Tolerance Time) or maximum temperatures, in order to ensure sufficient risk mitigation or avoidance and to establish acceptance criteria for the final safety validation.The *safety objectives* are implemented in a risk-based manner using appropriate state-of-the-art methods (e.g. V-model, FMEA).

3.4.4 Production

The *PC requirements* relating to the manufacturing process are introduced in the production phase analogously to the design requirements in the development phase. Additional *PC requirements* may exist in the respective production area and corresponding measures may be required (e.g. installation documentation by means of QR code or acknowledgement by employees).

Within the scope of production process and product approval (see e.g. VDA Volume 2), *compliance* with production-related special characteristics (*product safety* and *product conformity*) is verified and documented at the start of

production (SOP). These will be verified and confirmed regularly during series operation. The frequency of this verification is determined on a risk basis and updated if necessary.

Examples:

- *PSCR* line walks for *product safety* assessment
- *CoP* inspections as conformity verification
- *Requalification test* in line with product monitoring to confirm the specified product characteristics
- Confirmation and documentation of *compliance* with *product safety* requirements at regular intervals, as described in the Chinese SAMR 75/76
- Review for potential *PC risks*, analyze and assess, and report on issues found during routine review at regular intervals

In advance, an escalation process for non-conformances must be defined within the *PCS* (including reaction plans, responsibilities and, if necessary, the involvement of experts). According to this process, various actions are prompted, escalating up to a block on delivery issued by the *PSCR*. The handling of non-conformities should be coordinated within the supply chain.

Note: In the context of Product Compliance, it is essential to perform product and process audits, e.g. as per VDA Volumes 6.3 and 6.5.

3.4.5 Usage

This chapter is limited devoted exclusively to the identification and assessment of product safety risks during the use phase, i.e. for *products* that will be *placed* or already have been *placed on the market*. The focus is on assessing risks in a transparent and traceable way. This is accomplished using a systematic procedure, unambiguous terminology, clear task delineation within the supply chain and easily comprehensible documentation.

There is no detailed discussion of the assessing of *PC risks* to other protected interests, such as the environment, animals, energy resources, property or commercial transactions. In assessing these other *PC risks*, it can be helpful to know the basic methodology for the assessment of risk to life and limb and to use that as a guide.

A *safety risk* is usually defined by the *severity of damage* (*injury severity*) and the associated probability of its occurrence. Risks with low *severity of damage* and low probability of occurrence are tolerated more readily than risks with high *severity of damage* and/or high probability of occurrence. Foreseeability (detectability) and controllability (containability) also play a role.

Based on the results of the risk assessment, it needs to be checked whether there is any duty to notify authorities and take action. The decision-making processes and organizational structures necessary for this are defined by the *PCS* and described in Chapter 3.5 Organization.

Interface description in the supply chain

General responsibility for the final risk assessment of the vehicle system and the potentially required actions lies with the OEM as the vehicle manufacturer. The vehicle manufacturer involves the suppliers in the risk assessment at the vehicle level to the extent necessary. The affected suppliers contribute to this risk assessment by independently providing the necessary information and assess the *PC non-conformance* within their area of responsibility, appropriately taking into account interfaces and intended use. The aim is to incorporate all relevant findings from the analysis processes of the partners involved. For one thing, this creates a shared, consistent image (preventing misunderstandings) and, for another, it ensures the completeness and accuracy of the risk assessment. This requires a flow of information in the supply chain, including the respective *PSCR role* (see Figure 3-4)

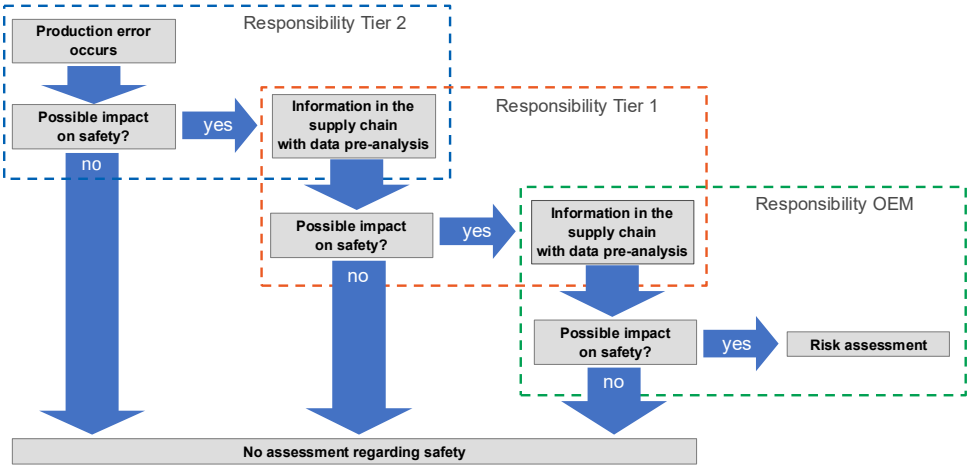

Figure 3-4: Example of information flow in case of a potentially safety-related PC non-conformance

This principle applies equally to other conceivable times and places where a *PC non-conformity* is detected.

Description of the *error systematics* and the *relevant event chains*

First, we need to understand the *error systematics*. We'll start by looking over the entire sequence of all individual steps from the potential *PC non-conformance* to the effect in the overall vehicle system. To create the *error systematics*, we need to consider the following aspects, fleshing them out as necessary:

- Non-conformance of the *product* with the specification (e.g. specification, drawing)
- Effect of *PC non-conformance* in the overall vehicle system
- Detectability of *PC non-conformance*, such as warning light, abnormal noise, odor

The *error systematics* is then expanded to include the interaction with external influencing factors in order to determine the *relevant event chains*. The following

elements are assessed here, among others:

- relevant situations, for example traffic situation, climatic conditions
- controllability by vehicle users, road users or third parties
- potential *injury severity* for vehicle users, road users or third parties

There may be several *relevant event chains*, each of which must be assessed separately. The potentially affected operational and situational states must be taken into account. Operating states include, for example, charging, parking, reversing, driving while using driver assistance systems, etc. Situations include, for example, highway driving, turning, traffic accident, etc. Figure 3-5 shows an example of the effect when the vehicle is moving or when it is stationary.

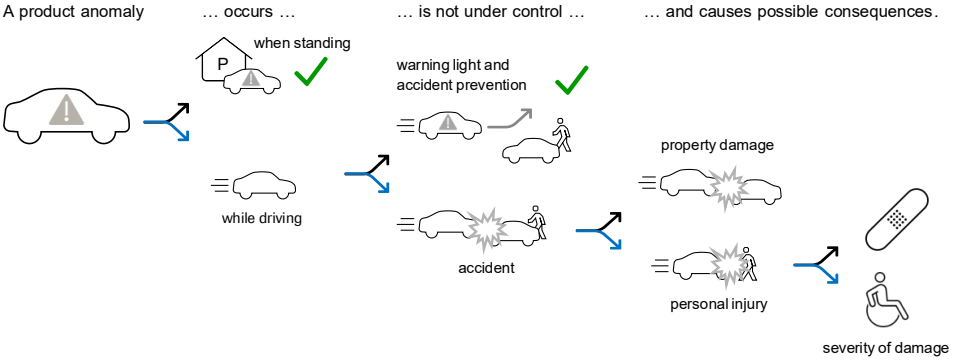

Figure 3-5: Example of a relevant event chain

The *relevant event chains* are used to check which input information is required for an assessment. Missing information may need to be obtained or developed (e.g. test series, forecasts, evaluation of field data).

Types of risk assessments

Typically, we would start with an initial risk estimation. This provides an initial indication of the level of risk and the urgency of any risk-mitigating measures.

Depending on the outcome, more in-depth analysis and a more detailed risk assessment may be required. This can be carried out either qualitatively, quantitatively or in a mixed form (partially quantitatively). A reassessment is required when new knowledge is acquired.

Possible forms of risk assessment are described below, taking into account the essential elements of a risk assessment, such as *severity of damage*, likelihood of occurrence, detectability and controllability.

a) Initial risk estimation

The initial risk assessment is an ad hoc evaluation of the risk by experts based on the information available at that time.

Possible results:

- need for (immediate) action yes/no
- further analysis needed

b) Qualitative or semi-quantitative risk assessment

The qualitative risk assessment is a detailed continuation of the risk estimation. It does not use any numerical values but is instead based exclusively on the qualitative description of the probability of occurrence and the *severity of the damage*. Pre-defined scales allow for systematic and consistent classification (see Figure 3-6.

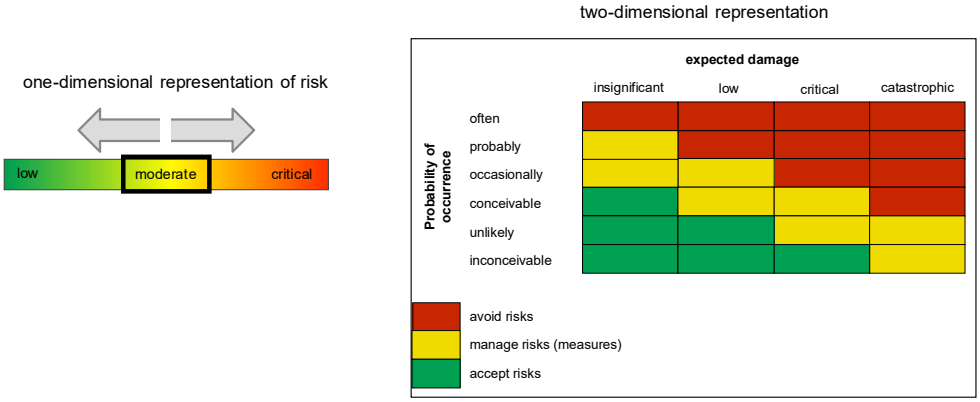

Figure 3-6: Examples of scales

The qualitative assessment is one possible method. It can be used, for example, in case of insufficient data availability or a weak database with the goal of producing more of a visually compelling representation of the potential risk.

If reliable figures are available for some aspects, these can be used for a semi-quantitative assessment. This makes the result more concrete, since at least part of the overall probability is calculated.

Possible results:

- Risk level (e.g. low, moderate, critical)
- comparability of multiple scenarios and/or actions
- further analysis needed

c) Quantitative risk assessment

The quantitative risk assessment is based on strong data or expert estimations. Its result is a calculation of risk. This is done by quantifying the individual steps of the *relevant event chain* and multiplying the factors by one another. The result represents the overall probability of the *relevant chain* of events occurring and thus the risk to *a* vehicle from the potentially affected volume (*individual risk*).

The *individual risk* can be used to calculate the *risk of the total population* according to the potentially affected volume. The frequency of occurrence of the *relevant event chain* can thus be estimated on the premise that the input data are sufficiently reliable and precise. In statistics, this is referred to as the expected value.

Possible results:

- probability of occurrence of the *relevant event chain*
- risk level (e.g. low, medium, high, serious)
- comparability of multiple scenarios and/or actions
- further analysis needed

Review

A risk assessment is a recursive process. The utilized information and data should always be thoroughly examined according to the two-person rule and updated with any new findings.

a) Data sources

The risk assessment is done using different data sources. Valuable sources include publicly accessible accident and registration statistics, recall databases from authorities or research institutes, as well as our own statistical analyses such as failure rates, results from test series, etc. They need to be evaluated with regard to *quality*. The guiding questions in Chapter 4.4.5 are very helpful in this process.

b) Reliability

Every individual step in the risk assessment should be evaluated for reliability in order to determine whether the risk assessment is strong overall. This includes the exact source and/or origin of the individual pieces of information/data. For information that is initially unreliable, such as estimates, an attempt can be made to increase reliability by carrying out more in-depth analyses.

Here are some examples of varying data reliability according to data origin (in order of increasing reliability from top to bottom):

- estimates
- similar studies that are not directly transferable to the chain of events to be assessed (possible use of a correction factor)
- representative statistics or studies
- test series, analyses and calculations which can be applied to the chain of events being assessed

c) Sensitivity analysis

The sensitivity analysis shows how reliable the risk assessment is, taking into account appropriate variances of the input information. Statistical methods such as confidence interval procedures or Monte Carlo simulations can be helpful for this.

d) Plausibility check

In order to further increase the load-bearing capacity of the risk assessment, the input information should be made plausible. This could be a comparison with field data, replacement part turnover or a comparison with other subjects.

Examples of official guidelines for risk assessment

- The SAGA (Safety Gate Risk Assessment; formerly RAPEX) is set out in Annex 2 to the Commission Delegated Regulation supplementing Regulation (EU) 2023/988. This guideline essentially advises grading the *severity of the damage* and classifying the risk, in combination with the probability, into four risk levels (serious, high, medium or low) using a table
- PRISM (Product Safety Risk Assessment Methodology) is published by the Office for Product Safety & Standards in the UK. This method is based on the RAPEX method and supplements it, for example, with a preliminary initial estimate (“risk triage”) preceding the risk assessment

and other factors that impact the decision on how to handle the risk (“risk evaluation”), e.g. the number of *products* and the consideration of the relative risk for *products* developed for protection.

- "Safety of motor vehicle product – Guidelines for risk assessment and risk control" GB/T 34402-2017 is a standard in China that combines the *severity of damage* with its probability in two stages: First comes the initial estimate. In the second step, it is corrected as necessary according to certain criteria. The standard allows for both a qualitative and a quantitative estimation of the factors. The risk is classed in five levels (high, relatively high, medium, relatively low and low). Instructions are described in accordance with the risk level

3.5 Organization

3.5.1 Internal Organization

The implementation of a *PCS* requires that appropriate organizational and procedural structures be established, documented and approved by Management. These structures define *PC*-related roles and responsibilities along the *Three Lines Model* (see VDA Volume "Product Compliance – Volume 1: Product Compliance System").

The *PSCR roles* is anchored in the *First Line* and can be split up between multiple people. It is not necessary for everyone in this *PSCR network* to have the title “*PSCR*”.

Delegation of *PC* tasks requires that the tasks, competencies and responsibilities be defined and documented, e.g. by means of a *RACI chart* or within the framework of existing organizational and role structures.

The employees to whom these roles have been assigned and who are therefore involved in *PC*-relevant processes must be adequately qualified and trained.

The contact person(s) for *PC*-relevant facts must be designated and known within the company and the supply chain. This facilitates the speedy exchange of information in the event that a product warning is needed and ensures that all employees have a contact person available for *Product Compliance*-related questions.

In case of staffing changes, the role must be reassigned as quickly as possible by the person responsible for delegating it. Until it is reassigned, responsibility for the role goes back to the delegating person.

When delegating the role, be sure that the tasks are assigned to persons whose position in the company hierarchy gives them adequate decision-making powers.

The requirements for internal delegation can also be applied to an external delegation, e.g. when contracting a service provider. The *legality control obligation* remains entirely with the *management bodies* of the *customer* (contracting company).

For various in-house roles and committees (e.g. management, quality control),

there may be duties to provide information or reports to external bodies (e.g. government authorities). The *PSCR role* has either an executive or supportive function, depending on the structure defined in the company:

- Identification of affected *products* and markets
- Integration of relevant internal technical bodies
- Finding and providing requested information
- Planning, tracking and documentation of resulting action plan
- Creation and timely provision of notifications and reports to authorities

The necessary committees and participants in relation to *PC*-relevant facts are determined by *PCS*.

The specific tasks, rights and duties of the *PSCR role* in conjunction with duties to inform and report should be implemented according to the delegation principles described above.

3.5.2 Outsourcing

PC-related activities can be outsourced to suitable suppliers/service providers. Such assignments are subject to the delegation principles set out in Chapter 3.5.1. The contracted suppliers/service providers must be selected systematically in order to ensure their suitability for the assigned tasks and the *customer*-specific requirements, e.g. based on

- proof of an effective *quality management system* at the supplier/service provider company
- proof of systematic competence management at the supplier/service provider company
- Proof of adequate resources (e.g. appropriate tools, staff, databases, etc.) to handle the assigned tasks
- proof of the supplier’s/service provider’s suitability based on corresponding reference projects in the past

The details of the assignment must be specified in interface agreements between the *customer* and the supplier/service provider. For example:

- *PC requirements* for the scope of supply/service
- Type, scope and timing of expected information/working materials (e.g. hardware, software, access permissions, digital access, etc.) or work results both on the part of the *customer* and on the part of the supplier/service provider
- Triggers/limit values in case of *PC non-conformances*
- Definition of responsibilities, incl. communication and escalation paths

3.6 Communication and Training

3.6.1 Communication

3.6.1.1 General communication guidelines

For all *PC*-related communication, the following must be observed:

- All matters must be described completely, clearly and unambiguously
- The information (documents, incl. emails) should only be distributed to the persons specifically involved with the *PC*-relevant facts.
- The language and representations must be kept clear, comprehensible and matter-of-fact. In particular, it should be free of emotions, colloquialisms, slang and sarcasm. Keep in mind that, despite confidentiality, the stored documents are liable to be disclosed widely outside the company (e.g. e-Discovery).
- As a rule, only facts and fact-based assessments should be documented. If, in an exceptional case, we start with assumptions or hypotheses, these assumptions or hypotheses, along with any interpretations derived from them, must be clearly identified as such in the documentation. Opinions or interpretations must be immediately checked and followed up with facts (e.g. refrain from prematurely assuming that a potential safety non-conformity will pose a risk to life and limb)
- There may be cases where the effect of an issue cannot be assessed in full (e.g. delivery of components for a complete system whose behavior can only be assessed by the system manufacturer). In such cases, formulations pre-empting a final evaluation at the complete system level should be avoided.
- Every problem description should be accompanied by a solution or a description of solution-finding activities
- Are facts formulated in a confusing way, or if assertions are based on incorrect or no longer defensible assumptions, a clarifying statement should be sent out in order to document the latest status of the discussion

The *PSCR*'s responsibilities include raising awareness of the content and language of *PC*-related issues.

3.6.1.2 Internal communication

Internal communication is based on processes and specifications that ensure internal exchange with involved employees or organizational units. In addition, the internal communication processes promote open, goal-oriented and efficient exchange on *PC*-relevant facts, especially regarding *PC non-conformances*.

Upon detection of a *PC non-conformance*, immediate notification must follow within the process defined in the company. A previously defined consistent notification process must be observed for this purpose. In order to ensure smooth communication, the interfaces in the supply chain should be defined in advance if possible and made known to the relevant contact persons in the company.

Internal communication tasks of the *PSCR*:

- responsible for the planning, organization, application/approval and implementation of cross-departmental communication activities.
- communication of *PC*-related non-conformances, e.g. with development, production, sales and distribution, quality assurance
- ensuring the effectiveness of internal communication of *PC*-relevant facts through systematic and procedural structures including early warnings

3.6.1.3 Flow of information within the supply chain

The implementation of *PC* measures is in the interest of all process partners in the supply chain.

The responsible *PSCR role* coordinates the necessary communication with the respective external stakeholders (authorities, contractual partners, press, etc.) in accordance with the company's internal guidelines and with the involvement of the respective internal departments (law, communication, etc.). Country-specific regulations, technical conditions, locally applicable laws must be taken into

account on a case-by-case basis.

As soon as a *PC non-conformance* is detected as part of the product monitoring process, this information is to be forwarded immediately to the impacted interface partners in the supply chain for further risk analysis. In the case of a reportable non-conformance, the report is usually made to the authority by the OEM. The reason for this is that the impact of a possible non-conformance with regard to a risk analysis on a component can only be comprehensively and appropriately assessed in the overall system (vehicle). However, if the supplier has its own reporting obligations, it may also have to report the non-conformance independently to the authorities. This should be done with the involvement of the affected OEMs.

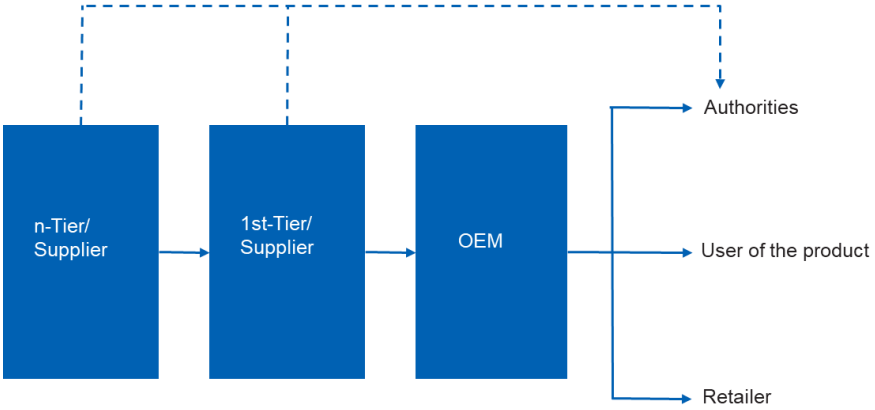

Figure 3-7: Schematic example of a notification process

An example of the reporting process for China is shown in Figure 3-8.This notification process can also be applied to the n tier in analogous form. This tier always notifies its respective superordinate supplier. Similar procedures are defined in other countries. Specific local circumstances must be taken into account (e.g. NHTSA Tier 1 duty to report in case of *PC non-conformance* affecting multiple OEMs).

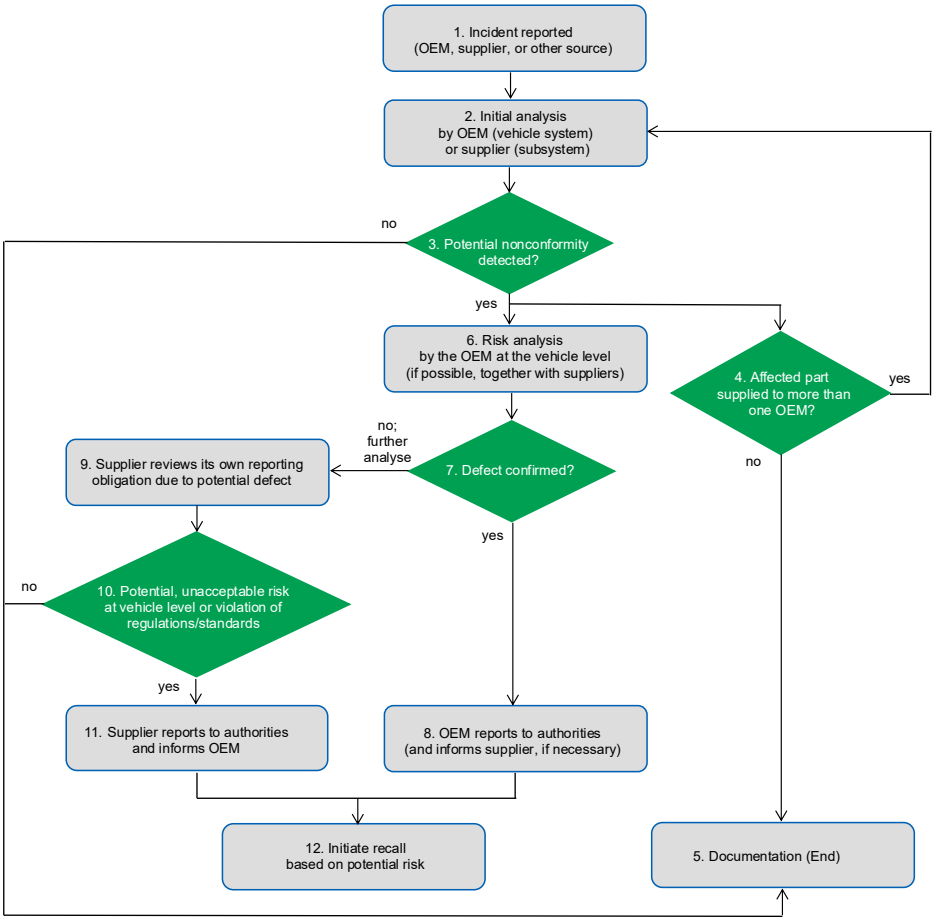

Figure 3-8: Notification process example from the German-Chinese working group Product Safety as part of the collaboration of BMWi and AQSIQ of 2017

Table 3-1: Explanation of the example reporting procedure in Figure 3-8

Step	Authorities	OEM	Supplier	Note
1		R	R	Potential process initiated by: • Tests or validation • Analysis of field complaints • Information through the press or social media
2		R / S	R / S	Initial analysis can be carried out as follows: • Overall vehicle system (OEM) • Subsystem (OEM or supplier)
3		R / S	R / S	Verification of potential *product safety* deviations or non-conformities during the initial analysis.
4		I	R	If the supplier supplies the same or equivalent parts to more than one OEM, the initial analysis has to be carried out at each OEM. Due to the influence of the non-conformance on the different systems, the analysis result may be different.
5		R	S	All relevant information is documented and the process is completed.
6		R	S	The OEM will perform a risk assessment for the verified non-conformance. This assessment is carried out at the overall vehicle level. Suppliers provide support with the individual subsystems if necessary.
7		R	S	*PC non-conformances* relevant to safety or conformity are determined based on the risk assessment.
8		R	(I)	If a potential risk cannot be ruled out, the OEM must report it to the authorities and, if affected, to its supplier.
9			R	If the joint assessment by the OEM and the supplier does not result in a notification to the authorities by the OEM, the supplier has to review its own reporting obligation to the authorities.
10			R	The supplier shall check whether the incident in connection with its product leads to safety or conformity-relevant *PC non-conformances* or inadmissible risks to persons or property.
11	I	I	R	In case of *PC non-conformance* relevant to safety or conformity, the supplier notifies the authorities and informs the OEM.
12	R	R	S	Recall measures are taken according to instructions by authorities.

R – Responsible, S – Support, I – Information

The figures and process descriptions in this chapter refer to the status at the time of publication of this volume. The distributor of the respective *product* must independently find out about the country-specific notification obligations and periods.

3.6.2 Product Compliance Training

Employees of an organization must be continuously sensitized through regular briefings on *Product Compliance*. An appropriate training plan for the different roles and target groups of an organization is usually provided by the *Second Line*. The responsibility for conducting the training is defined in the *PCS* and can be carried out either by the *Second Line* or the *First Line*, depending on the content.

These training courses not only serve to qualify the *PSCR roles*, but also include, for example, awareness training for members of management or methodology training for specialist staff.

The *PSCR* define standards and tools, promote exchange with all relevant stakeholders in the company's business units and communicate regularly on the company's *Product Compliance* training program. The *PSCR* ensures that the holders of the *PSCR roles* are qualified according to the specifications. At least one formally trained *PSCR* should exist in each company. VDA QMC and its licensing partners offer training courses based on this VDA volume. The *PSCR*s may issue training certificates for the training of internal employees, which are recognized within the supply chain of the VDA members.

A regular review of the training content by the *PSCR* is useful in order to incorporate acquired knowledge, e.g. from the *lessons learned* process.

3.7 Monitoring/Improvement/Reporting

The purpose of monitoring and improvement is the regular and event-oriented assessment of the adequacy and effectiveness of the *PCS*. The aim is to systematically identify and reduce or prevent potential *PC risks* and possible rule violations in good time.

Information from existing systems such as the *quality management system* (*QM system*), the *PCS* and the whistleblower system can be used to identify non-conformances. Information from *First Line* committees can also provide valuable information. Networking these systems is therefore recommended. The reporting structures existing in these systems can also be usefully used for *PC*-related facts.

Identified non-conformities and potential improvements are analyzed, and suitable corrective/improvement actions are developed and implemented. These help to continuously improve *PC*.

3.7.1 Continuous Monitoring and Improvement

Lessons learned

If a *PC non-conformance* is detected, continuous improvement must occur. This *lessons learned* process must be ensured by the *PCSR role* throughout the *product life cycle* as part of due diligence obligations.

Note: General principles of the Lessons Learned Process are described in detail in the VDA Volume "Lessons Learned"[3].

[3] See Association of the Automotive Industry (VDA), *Lessons Learned – Definition of "Lessons Learned" in the Automotive Industry. Process description, application tips, and practical examples*, 1st edition, November 2018.

Figure 3-9: Lessons Learned Process (source: VDA Volume "Lessons Learned")

Monitoring *PC KPIs*

To continuously monitor and evaluate the effectiveness of *Product Compliance*, the *PCS* (*Second Line*) defines and periodically monitors company-specific *PC key performance indicators* (so-called *PC KPIs*). The respective *PSCR role* records these *PC KPIs* and reports to the *Second Line*.

PC key performance indicators can include:

- training rate of employees of an organizational unit
- staff fluctuation for *PC*-related tasks
- number and trend of *PC* non-conformances detected during the development phase in the course of *PC* audits
- number and trend of observed non-conformances e.g. in *CoP* activities, line walks or audits
- number and trend of *PC*-relevant field complaints

After evaluation of the *PC key performance indicators* by the *Second Line,* in case of non-conformances, the respective *PSCR role* should derive appropriate measures together with relevant specialist departments.

3.7.2 Product Monitoring and Market Observation

Product monitoring

Companies have a duty to monitor *products*, which must be ensured by *PC* activities. Product monitoring can generally be divided into a passive (reactive) and an active (preventive) part. Passive product monitoring refers to the gathering of information about product complaints in the field, such as *customer* complaints, warranty procedures or inquiries by authorities. Active product

monitoring includes, for example, a targeted analysis of possible non-conformities in the production or inspection process, the demand for spare parts or media research of comparable *products*.

Product observation may reveal a possible *PC non-conformance*. This non-conformity must be introduced into the *PC* process by the *PSCR role*, so that it can be assessed and so that improvements and actions can be developed. The scope of the obligations regarding product monitoring may vary for those involved in the supply chain. In particular, the product monitoring obligation for OEMs relates to the complete vehicle and, for suppliers, generally only to the delivered *product*.

Market observation

In the course of market observations, changes in consumer demands or consumer habits but also changes in the behavior of competitors are observed. Market observations depend on the possibility of tracking or monitoring on the market and cannot be conducted for all *products*.

For example, changes in consumer habits, the company combining its own *product* with third-party *products* (e.g. accessories and vehicle retrofits) or new technologies may lead to a change in the perception of safety among *consumers* or the general public.

Significant improvements in *product safety* through the implementation of new findings in the market can raise the state of the art for the competition. The expectation of consumers to participate in this improvement can lead to a new, justified safety expectation (example: functional quality of active/passive safety systems).

The *PSCR role* reports and monitors the findings from the market observation according to the processes defined in the *PCS*, so that *PC requirements* for the future *product* strategy can be derived from this.

3.7.3 Observation of Regulatory Requirements

Each individually manufactured *product* must comply with the regulatory requirements applicable in the jurisdictions of the *target sales markets* where the *product* is *placed on the market*.

In addition to product and market observation (see Chapter 3.7.2), this requires regular observation of new or modified regulations, whose influence on the *products* has to be evaluated and for which corrective action may need to be introduced.

The following points must be taken into account:

- For each individual *product placed on the market*, it should be possible to trace which regulatory requirements it meets.
- A collection (e.g. database, register) of all applicable regulations for all affected jurisdictions enables the responsible *PSCR role to* identify new or amended regulatory requirements for a specific *product*.
- The collection of regulations must be systematically and continuously updated with new and amended regulations.
- For the development of new *products* or changes to existing *products*, the applicable regulations are identified, and the product- and jurisdiction-specific regulatory requirements are determined.
- During the production phase of a *product*, the *PSCR role* in charge ensures continuous monitoring of the applicable regulatory requirements. In case of new or modified regulations, it is checked whether the production of the affected *products* can continue unchanged or whether it can continue subject to a change or recertification.
  The *placing on the market* of non-compliant *products* must be prevented by appropriate processes.

It is recommended that, in addition to the applicable regulations, the applicable non-mandatory norms and standards that are necessary in order to comply with the state of the art also be monitored similarly.

In today's complex regulatory landscape, effective regulatory monitoring is vital to maintaining *Product Compliance*.

3.7.4 Reporting

The *PSCR*s report regularly to the *management bodies* on *Product Compliance*-relevant facts, such as content, processes, audit results and improvement

measures. Clearly defined reporting and escalation channels are essential to ensuring that all relevant information is forwarded promptly and correctly.

The *PCS* defines escalation criteria, reporting limits, reporting frequencies, and reporting channels for *PC non-conformities*. The *PSCRs* ensure effective implementation within the *PSCR network*.

Reporting frequencies should be defined on a risk basis and reviewed at appropriately regular intervals. For example, a rapid escalation should take place in the event of serious non-conformances, whereas reviews of the effectiveness of the *PCS* or reports on *PC*-relevant facts can take place at regular intervals, e.g. monthly or quarterly.

As part of its governance function, the *Second Line* reports on the effectiveness of the *PCS* to the responsible persons, bodies or committees and receives information from the *PSCR network* (e.g. *PC KPIs* and audits).

4 Guiding questions

These key questions are designed to help address *Product Compliance* and can help identify and structure important aspects.

Reality is often more complex than default guiding questions. Sometimes it is necessary to shift focus or develop new questions in order to better understand the situation. It may be that a question is not relevant or that a particular situation raises other questions that are not included in the guiding questions.

This is a non-exhaustive list of sample questions that are not rigid and complement the guiding questions from the VDA Volume "Product Compliance – Volume 1: Product Compliance System". The main questions there are primarily aimed at the procedural design of the *PCS* and the questions from this volume are aimed at aspects of operational implementation.

Each company should examine these questions for itself and supplement them if necessary.

4.1 Culture

- Does the company convey to all employees – regardless of their function and also in daily processes – that *Product Compliance* is a joint responsibility?
- Are the *PSCR network* and its activities sufficiently known and accessible as a role model and bearer of the *PC culture*?
- Is there a clearly expressed positive error and *lesson-learned* culture that employees can express concerns about *PC non-conformances* without fear of negative consequences?
- Are employees involved in *PC*-related facts supported by the *PSCR network,* and can they act appropriately independently of commercial interests?

4.2 Objectives

- Have suitable, possibly department-specific *PC key performance indicators* (for specialist departments, for product areas, etc.) and target values been defined for all aspects of the *PCS* and communicated to employees?
- Are *PC KPIs* regularly collected, monitored, and reported by the PSCR network?
- Are *PC KPIs* reviewed for effectiveness and relevance? Are non-conformances analyzed, and are corresponding measures derived and implemented?

4.3 Risks

- Is the *PSCR* actively involved in risk management for *PC risks* throughout the entire *product life cycle*?
- Are structured risk analysis methods used, e.g., to minimize the influence of cognitive biases?
- Are the identified *PC risks* substantiated with appropriate measures, and are they checked with due diligence for implementation and effectiveness?
- Do communication structures exist in the event of *product safety* or *conformity* non-conformances (e.g. to OEMs, suppliers, authorities)?

4.4 Program

4.4.1 Configuration management

- Are product configurations and their components clearly identifiable?
- Are *PC requirements* (e.g. traceability) taken into account in version/change management (e.g. new revision status in the event of design changes or process changes)?
- Is resulting evidence documented and retained according to company-specific policies?

4.4.2 Documentation

- Is adequate, standardized, structured documentation of *PC*-related processes ensured?
- Is the traceability of the *PC*-relevant facts guaranteed, e.g., by means of a database?
- Are the relevant documents stored in the appropriate document storage system provided for this purpose?

4.4.3 Development

- Is the information necessary in order to conduct a hazard analysis available (e.g. product description, product limits, *target sales markets*, environmental conditions, use in dual-use applications, application areas, non-conformities in similar [predecessor] *products*)?
- Are *PC requirements* (all *binding obligations* including legitimate safety expectations of the general public) determined and their implementation ensured during the product development and before the start of production (SOP)?
- Is a systematic procedure used for hazard identification and assessment?
- Are all relevant life cycle phases (e.g. maintenance, decommissioning) of the analyzed *product* factored into the hazard analysis?
- Are all the relevant potential hazard causes accounted for in the hazard analysis (e.g., intended and predictable use, functional and non-functional failures, functional dependencies, tampering)?
- Based on a risk analysis, were appropriate product safety requirements derived (including comprehensible acceptance criteria) and countermeasures specified?
- Are all product safety requirements clearly marked and thus identifiable in the overall requirement process?
- Are there any other product safety requirements to be taken into account from the state of the art?
- Can proof of implementation (e.g. technical drawing, test result) be provided for each product safety requirement?

4.4.4 Production

- Are all the process steps in production that are relevant for securing the *binding obligations* identified and thus marked as prioritized?
- Have safeguarding measures been defined for the prioritized process steps after risk assessment and implemented on the production line?
- Are action limits and *PC KPIs* defined in order to monitor and control the process sequence and the process result?
- Are process sequences and tests described (e.g. cycle, content) in order to regularly check *compliance* with production-related special characteristics during the series process?
- Is there a coordinated and communicated process and schedule for *PSCR* line walks or audits, and are these carried out accordingly?
- Are all *PC*-related production data identified and categorized accordingly, and are rules defined for their documentation and retention?
- Is it ensured that all employees in production are sufficiently trained and sensitized to execute *PC*-relevant processes?
- Are changes to the *product* and manufacturing process checked for *PC* relevance, documented and communicated?
- Are all *CoP* tests defined, performed and documented to demonstrate *product conformity*?
- Is there a described response plan after identification of *PC*-relevant *product* or manufacturing process non-conformances?
- Is process monitoring and *compliance* reporting implemented, and is *Product Compliance* verified at regular intervals?

4.4.5 Usage

- Are there known different methods for systematic risk assessment when *PC non-conformance* is detected?
- Are the persons carrying out the risk assessment sufficiently independent of the decision-makers?
- Are the *error systematics*, the influencing factors and the *relevant event chains* described in as much detail as possible with all relevant aspects and in order?

- Are all relevant analyses, including those of the partners involved, taken into account in the risk assessment?
- Is the nature of the risk assessment proportionate to the subject and the timing?
- Is the risk assessment documented transparently and comprehensibly, and has any source information been provided?
- Do the terms and definitions used reflect the facts clearly and appropriately in a risk assessment?
- Is the outcome of the risk assessment presented in a clear and comprehensible way?
- Is there a clear recommendation for action for the decision?
- Has a decision been reached, and does this result in official reporting obligations or compulsory actions?

In addition to the key questions, the following supplemental questions also provide guidance for evaluating safety-related *PC non-conformances*:

- Can the *PC non-conformance* pose a threat to life and limb?
- Does the error occur under certain conditions or situations, such as weather conditions, operating conditions or traffic situation?
- Is there a systematic or random (sporadic) error?
- Are further studies necessary to obtain a sufficiently reliable database (e.g. time-lapse test, sufficient sample size)?
- Are the data sources recognized and up-to-date, and are the resulting statistics representative of the use case?
- Is the reference size correctly accounted for?
  (Example: If the accident probability should be assessed as the result of tire damage, then the number of accidents due to tire damage is divided by the number of known incidents of tire damage with and without accident.)
- Are all the influence factors considered just once?
  (Example: If statistics on accidents due to tire damage refer to vehicles with and without tire pressure monitoring systems, the factor “tire pressure monitoring system present” may not be included in the risk

assessment. Factors used in the calculation must be independent of each other.)

- Could this be a false correlation?
- Is there a time delay until the error occurs (aging mechanisms, seasonal cycles, etc.)?
- Has the probability of occurrence been determined taking into account the manner of use?
- Are protective mechanisms (e.g. pressure relief valve, shielding plate) or risk mitigating measures (e.g. automatic shutdown, emergency operation) or warnings (e.g. stickers, warning lamps, acoustic or optical signals) effective?
- Has it been established to what extent and under what circumstances the risk can be controlled?
- Is it a *product*/feature designed for protection?
- Is a *product*/function for particularly vulnerable groups (e.g., children) affected?
- Is there a difference in risk compared to the approved *product* or comparable *products*?
- Is a large number of people affected, or is a particularly devastating effect expected?
- In particular, are fatal accidents, serious property damage or environmental damage realistically possible?
- Has there been any customer feedback regarding the use of the *product* that indicates a risk to life and limb?
- Is the period of observation sufficiently long to allow for expected effects to have already occurred (e.g. aging effects)?
- Have any accidents (incidents involving personal injury) occurred that were attributable to a product defect?
- Are there any findings from the risk assessments during the development and production phases that could be relevant?
- Are there similar *products*/applications/models that could also be affected?
- Are the experts involved sufficiently experienced, informative and questioning?

- Could it make sense to consult an external consultant, for example, because a specific expertise is required or a second (independent) opinion promises new insights?

4.5 Organization

4.5.1 Internal Organization

- Are adequate organizational and procedural structures established, documented and approved by management?
- Are qualified employees defined for the relevant roles and responsibilities in relation to *Product Compliance*?
- Does the organization support, manage and monitor the activities of all relevant entities (as defined by the scope) in identifying and managing *PC risks*?
- Is it ensured that the *PSCR network* is integrated into the overall organization (information on current topics, decision processes on *PC risks*, new *products*)?
- Are the escalation paths for *PC non-conformances*, if necessary up to management, known, and are they used?
- Is it determined who communicates with external bodies (authorities, press, etc.)?
- Are there any known contacts for *PC*-relevant facts in the company and supply chain?

4.5.2 Outsourcing

- Is there evidence of the suitability of the supplier/service provider (e.g. effective QMS, resources, reference projects)?
- Are there any interface agreements, e.g. on information to be provided or on dealing with *PC non-conformances*?
- Are escalation paths agreed upon in case of *PC non-conformance* or significant risks?

4.6 Communication and Training

4.6.1 Communication

- Is it explained how the relevant *Product Compliance* topics are communicated to the relevant employees/production/departments/suppliers?
- Is it explained how to communicate *Product Compliance* issues to promote awareness and transparency within the organization?
- Do the employees responsible know the sources of information relevant to them, and do they have the necessary access to them?
- Is accessibility ensured (anonymous) for critical topics? (e.g. *compliance* hotline).
- Are current *PC*-relevant facts communicated within the organization with the goal of increasing understanding of *Product Compliance*?

4.6.2 Product Compliance Training

- Is there an adequate process in place for planning, preparing, conducting and rolling out *Product Compliance* trainings?
- Has the need for further education/training for the aforementioned employees been analyzed, and have the training contents been provided to the relevant employees (according to target group, risk and need)?
- Have suitable training courses been conducted, and has adequate participant feedback been obtained in order to evaluate it for continuous improvement (e.g. through test questions, Q&A sessions, collection of participant assessments)?
- Is there a training plan agreed with the *PSCR*s to sensitize the employees (e.g. development, production, management) to their specific *PC* tasks?
- Are internal training courses conducted by VDA-certified *PSCR*s (or is the content of role-based training agreed with them,) and are training certificates created?

- Are repetition cycles defined for specific target groups and integrated into the training plan?

4.7 Monitoring/Improvement/Reporting

4.7.1 Continuous Monitoring and Improvement

- Are *PSCR*s integrated into the *lessons learned* process in the event of *PC non-conformances*?
- Are the *PC KPIs* defined in the *PCS* recorded and reported according to the specifications?
- Are improvement potentials for *PC* activities identified and implemented based on the defined *PC KPIs*?
- Are the *PSCR*s involved in the assessment of the implementation and effectiveness of the *Product Compliance* elements and derived measures by the *Second Line*?

4.7.2 Product Monitoring and Market Observation

- Is systematic product and market monitoring ensured?
- Are findings from *PC non-conformances* in current and new *products* systematically taken into account and documented in *PC requirements* (*lessons learned*)?

4.7.3 Observation of Regulatory Requirements

- Are the market-specific regulatory requirements known and evaluated, interpreted and implemented for the *product*?
- Are currently valid versions of the regulations/specifications observed throughout the *product life cycle*?

4.7.4 Reporting

- Are the reporting formats, including the recipients and the frequency of distribution of *PC*-related facts, defined and known within the organization?
- Are the escalation criteria defined by *PCS* known and is their implementation ensured within the *PSCR network*?

5 Practical Examples

5.1 Practical Example of a decision-making Body of a medium-sized Company

The following section uses an example from a medium-sized company to illustrate how to deal with *PC non-conformances*. The company management has delegated this decision-making process to a committee. The delegation was defined and documented in a *PCS*.

The decision-making body comprises the following functions:

- *Quality*
- Production
- *Product safety*
- *Product conformity*
- Product development
- Sales
- Customer service
- Legal
- Communication

The job description of the affected employees has been expanded accordingly. Substitution rules are established for all participants. Members and their alternates shall be technically and personally qualified to assess potential *PC non-conformances* and shall be equipped with the necessary resources, capacities and powers to perform their duties.

The participation of the respective functions is appropriately controlled according to the topic.

The committee will only be able to make decisions if all necessary competences are represented. This is determined by the chair at the beginning of each meeting. The chairmanship is defined and in this example is led by the designated *PSCR* representing the *Quality* Division. The *PCS* stipulates that decisions in the committee must be unanimous. If no unanimous agreement is reached, the decision will be escalated to corporate management.

The decision-making body meets as needed. The agenda items will be discussed and decided on the basis of a presentation that presents the full facts of the case. Meeting minutes must be prepared for every meeting. The minutes shall be filed centrally by the Chair of the panel.

All documents required for this process are defined as standardized forms and stored centrally. The storage of data in terms of retention period, tampering protection and access rights is regulated internally within the company.

The internal reporting process is defined in the *PCS* and is known to all employees involved. The external notification process is defined for the supply chain and communication is standardized.

As part of an annual briefing on the topic of *Product Compliance*, the committee members and their deputies are continuously sensitized. The effectiveness of the committee is monitored annually in internal audits by the *Third Line*.

5.2 Practical Example of a Risk Assessment Process and the corresponding Reporting Channel

The risk assessment process and the reporting route in the supply chain are illustrated below using a case study. In particular, the role of the *PSCR* of Tier 1 is described. As part of its business activities, As part of its business activities Tier 1 supplies the identical liquid container to two different OEMs, hereinafter referred to as OEM A and OEM B.

During their regular field observations, OEM A receives leaky fluid containers and hands them over to Tier 1 for a detailed analysis.

The initial assessment of OEM A indicates a potential safety relevance. Therefore, the *PSCR*s of Tier 1 are consulted.

In the course of their analyses, the *PSCR*s determined the use of a non-conforming starting material (granulate) for the production of the component.

The *PSCR*s verify the results of their detailed analysis with their *PSCR network* and the necessary experts and compiles the following information:

- What starting material is inappropriately used?
- Why did this use take place (cause)?
- Which production period and which volume are affected?
- Has the error already been corrected?
    - If so, by means of what measure?
    - If not, which measure corrects the error, and when does it take effect?
- Is a stock adjustment necessary?
- Are other parties in the supply chain affected?

The *PSCR*s evaluate the effect of using the wrong starting material on the component. Ultimately, the incorrectly manufactured components are temperature-resistant only up to a low value. This has an effect on the durability of the component during vehicle operation. As a result, these components do not meet the originally defined specification. A potential safety relevance in case of a premature failure cannot be excluded.

Within the scope of their assigned authority, the *PSCR*s order a delivery block and a stock adjustment.

The *PSCR*s inform both OEMs about the facts for evaluating the component non-conformance in the respective vehicle system environment. Unlike OEM A, OEM B determines in the course of their fault sequence analyses in the vehicle that no safety hazard can occur due to the non-critical installation situation. OEM B transfers the issue to its regular fault rectification process.

At OEM A, the case is presented to the decision-making committee with all the available findings. The decision-making committee determines the next steps. In the case study, OEM A prepares the steps for a safety recall and informs the relevant authorities.

As the identical container was provided by both OEMs in one market for which Tier 1 has a reporting obligation, the *PSCR*s report to the competent authority within the deadline.

The responsible *PSCR role* informs the respective next contact person in the supply chain about the facts and the corresponding result (see Figure 2-3 and Figure 3-4).

The *PSCR*s ensure that all relevant information is communicated, documented and stored in accordance with the company guidelines defined in the *PCS*.

The *PSCR*s check the effectiveness of the measure introduced with the *PSCR network* and report the facts to the *lessons learned* process.

5.3 Practical Example for the Determination and Implementation of a PC Requirement without Security Reference

The process for determining and implementing the *PC requirement* for an electronic control unit label is explained below using a case study.

Together with their *PSCR network* and the necessary experts, the *PSCR*s identify the *PC requirements* on the basis of the product scope, paying special attention to the regulatory requirements in the relevant *target sales markets*, and derive the Technical Specifications from this. No safety-relevant aspects for the label were identified during the risk assessment.

Technical specifications

- Label content: Product name, serial number, manufacturer, CE mark, recycling symbol
- Dimension and color
- Label material: Weather-resistant and temperature-resistant plastic label
- Attachment: Permanently adhered to housing surface and position on the housing defined based on assembly drawing
- Visibility: When installed, the label must be easy to read
- During the production process, it must be checked whether the drawing specifications are met, i.e. the correct label is applied in the correct position without damage

Review

After a prototype has been created, the person with the responsible *PSCR role* checks the label for *compliance* with the technical specifications. This includes the check for completeness of the information, the position on the housing, the results of the climate test and adhesive test as well as the readability in the installed state.

If the *PC requirement* is met, the label is released for series production by the *PSCR*. If non-conformances are identified, another check and *PC* approval by the *PSCR* will be carried out after implementation of the defined measures.

Documentation

Compliance with the individual technical specifications for confirming the *PC requirements* is recorded in the release document and stored in the document storage system in accordance with the specifications defined in the *PCS*.

5.4 Practical Example – Delegation Letter

Location/Department/Division/Division
of the company ***xxx*** hereby appoints
name of delegate
effective as of ***date*** (DD.MM.YYYY)
to the PSCR of the production plant/site ***yyy***

He/she is responsible for all Product Compliance (PC) issues from the date of designation.

Within the scope of this function, he/she has the following powers:

- Blocking of products or stopping of production processes in case of PC non-conformances
- Verification of compliance with PC-relevant regulations
- Process implementation for systematic risk identification in the context of Product Compliance
- Coordination and control of measures to minimize risks for identified PC risks

In this capacity, he/she has the following duties:

- Ensure line checks in production according to PC requirements
- Initiation and implementation of CoP sample checks, initiation of measures in the event of non-conformances, coordination and reporting to authorities
- Assist training managers in identifying training needs and train affected employees on key aspects of Product Compliance
- Regularly report to senior management on Product Compliance status

Functionally, he/she reports to the site managers.

6 Overview of PSCR Tasks

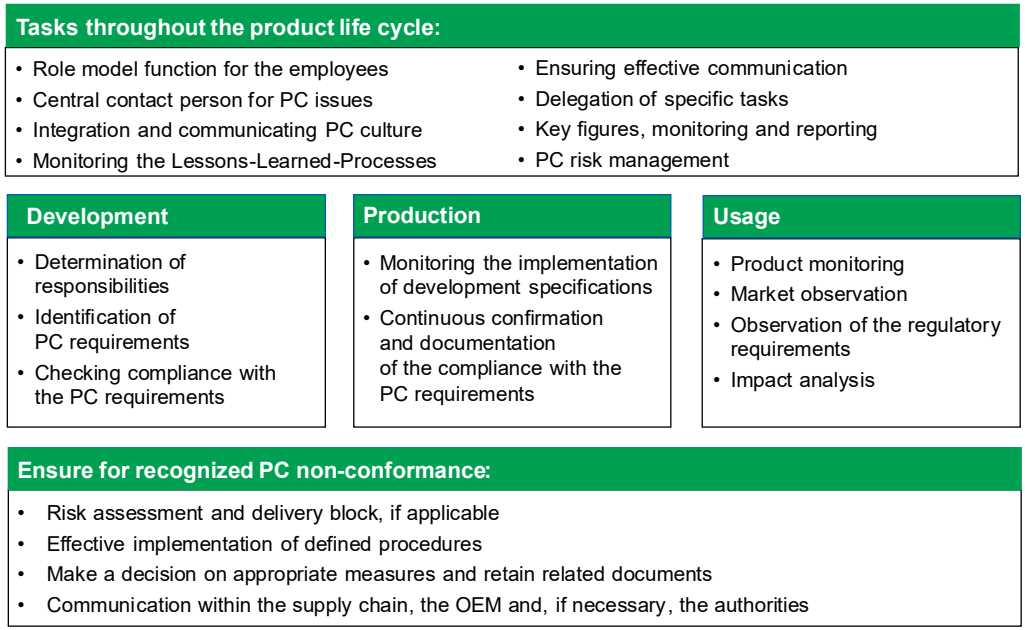

Figure 6-1: Overview of PSCR tasks

7 Glossary

Term	Definition
B2B business	Business relationship between companies (business-to-business)
B2C business	Business relationship between companies and end consumers (business-to-consumer)
Binding obligations **(related to *Product Compliance*)**	Legal and regulatory requirements relevant to a company's *products* that it must meet, and other product requirements (e.g., from internal and external norms and standards) that it chooses to meet.
Compliance	*Compliance* with all business-relevant laws, rules and regulations as well as self-imposed internal guidelines.
Conformity of Production **(*CoP*)**	Proof of conformity of the manufactured *products* with the approved (homologated) *product*.
Customer	"Organization or person receiving a *product*." (from DIN EN ISO 9000:2005). The *customer* is the recipient of a scope of delivery, no matter at what level of the supply chain. In *B2B business*, the last *customer* in the supply chain is the OEM and not the end customer of the vehicle; in *B2C business*, it is the end customer.
Error systematics	Causality between the cause of the error, the error and the misbehavior of *systematic errors*.
First Line	Operational departments: Provision of

	products/services to *customers*, management of risks, *compliance* with relevant *binding obligations*.
Individual risk	Multiplication of the factors of the individual steps of the *relevant event chain*. It thus represents the risk to a vehicle from the potentially affected volume.
Legality control obligation	The legality obligation constitutes the core of the statutory due diligence obligations regarding the management of a business. According to this, dutiful action includes both the *management bodies*' own *compliance* with the rules and – as an independent *legality control obligation* – the care for compliant conduct in the company.
Management body	Management of the company in *compliance* with the law. Legality obligation and *legality control obligation*.
Placing on the market	Placing *products* on a market.
Product	Material good (hardware or software) or a service that is the result of a production process.
Product Compliance (***PC***)	Fulfillment of product-related *binding obligations* throughout the *product life cycle*. *Product conformity* and *product safety* are parts of *Product Compliance*.
Product Compliance culture (***PC culture***)	A *Product Compliance culture* describes the common understanding of values and practices utilized in an organization in order to ensure *Product Compliance* throughout the *product life cycle*. It is characterized by responsible behavior, exemplary leadership

	and the systematic integration of *PC requirements* in all product-related processes.
Product Compliance key performance indicators (PC KPIs)	Key figures for transparent presentation and continuous monitoring of *Product Compliance* activities.
***Product Compliance non-conformance* (*PC non-conformance*)**	Failure to meet a *PC requirement*.
***Product Compliance requirement* (*PC requirement*)**	A *PC requirement* is a requirement on the *product* that results from the *binding obligations*. It forms the basis for the development, manufacture and distribution and use of compliant *products* and must be systematically identified, evaluated and integrated into company processes.
***Product Compliance risk* (*PC risk*)**	A *Product Compliance risk* is a potential or actual non-conformance from *binding obligations* that may occur along the *product life cycle* and jeopardizes *product conformity* or *product safety*. It requires systematic identification, evaluation and control through appropriate control measures to prevent legal and economic damage, as well as reputational damage to the company.
***Product Compliance System* (*PCS*)**	Company-wide, structured approach intended to ensure *Product Compliance*.
Product conformity	*Product conformity* means at least *compliance* with specific regulatory requirements necessary for the *product placed on the market*.

***Product Integrity* (*PI*)**	This term was used in the VDA Volume "*Product Integrity*" and referred to the fulfillment of *product conformity* and *product safety* requirements. The term *Product Integrity* is replaced by the term *Product Compliance*.
Product life cycle	Phases of development and use of a *product* up to its final disposal.
Product safety	*Product safety* also extends beyond *product conformity* to include meeting the legitimate safety expectations of users, other affected persons, and with regard to environmental risks during intended and foreseeable use throughout the entire *product life cycle*. The state of the art must be observed.
***Product safety and conformity representatives* (*PSCR*)**	Individuals nominated by corporate management to whom *PC* activities are delegated. The designated *PSCRs* coordinate and control the *PC* activities (*PSCR roles*). If necessary, these can be distributed to other people.
PSCR network	All persons who carry out *PC* activities, i.e. all designated *PSCRs* and all those assigned a *PSCR roles*. Depending on the context, this can mean the network in the company or the interfaces in the supply chain.
PSCR role	Delegated *PC* activity.
RACI chart	Accountability overview: - **R**esponsible - **A**ccountable - **C**onsulted - **I**nformed

Relevant event chain	Basic structure of risk assessment. Describes the required events in individual steps (error occurrence, relevant situation, possible hazard prevention and damage effect in the event of uncontrollability) which, together with their probabilities of occurrence, serve to determine a degree of risk.
Requalification test	In accordance with the production control plans, all *products* must be subjected to a complete dimensional inspection and functional testing, taking into account the *customer*'s requirements regarding the material, the function and the frequency. The results must be available for assessment by the *customer*.
Risk of the total population	Expected value as the mathematical product of the factors *individual risk* and total population.
Safety objective	The result of a risk assessment. This is a specific requirement that defines the measures to be taken to protect vehicle users from possible hazards and to reduce or avoid risks.
Safety risk	Risk of a *product* deviating from the specifications and resulting in possible effects on safety. It is usually defined by the *severity of damage* and the associated probability of its occurrence.
Second Line	Governance function: Guidelines, expertise and support, monitoring.
Severity of damage (***severity of injury***)	An estimate of the extent of damage that one or more persons may suffer in a potentially hazardous situation.

Target sales market	*Target sales markets* are the geographical, regulatory and economic areas in which a *product* is to be sold. They significantly determine the applicable *PC requirements* and are an integral part of the product scope.
Third Line	Internal audit and active review and advice on all issues relating to the achievement of objectives.
Three Lines Model	Describe effective structures and processes within organizations for *Product Compliance*. The division is into *management bodies*, *First Line*, *Second Line* and *Third Line*.

The terms of all VDA volumes are listed in a free online glossary in German, English and other languages:

https://vda-qmc-learning.de/module/glossar/

Quality Management in the Automotive Industry

The latest VDA publications on quality management in the automotive industry (QAI) can be found online at http://www.vda-qmc.de.

You may also order via this homepage.

Reference:

Verband der Automobilindustrie e. V. (VDA)
Quality Management Center (QMC)
Behrenstraße 35, 10117 Berlin
Phone +49 (0) 30 – 8978 42-235
Fax +49 (0) 30 – 8978 42-605
Email: info@vda-qmc.de, Website: www.vda-qmc.de

VDA QMC

Verband der Automobilindustrie
Qualitäts-Management-Center