Technische Hochschule
Brandenburg
University of
Applied Sciences
Fachbereich
Wirtschaft

Challenges for a Global Pre-Employment Screening Process Rollout

Term Paper

Faculty of Economy

Technische Hochschule Brandenburg

Submitted by:

Hendrik Müller

4th Semester

Mentor: Prof. Dr. Heinz-Dieter Schmelling

Müller, Hendrik Master Security Management 5th Semester	Werastr. 54 88045 Friedrichshafen hendrik.mueller@th-brandenburg.de Matr.-No. 2020-2183 Due: 29.03.2019

Friedrichshafen, 29th March 2019

Content

Table of figures

List of tables

Acronyms

PES	Pre-Employment Screening

1 Preface

Corporations face a wide variety of potential threats that could cause harm to their employees or impact their business. Prominent in modern times are threats targeted at the IT infrastructure of businesses or physical threats for institutions that are located in crisis affected regions. Another important, but in some countries often negligent threat, is posed by the companies' own employees. Insiders or employees that want to harm the company could theoretically do so in any regard; be it physically harming employees, sabotaging equipment or processes, or stealing property. Theft of digital or intellectual property could be considered especially critical, because the scruples of employees might be lower than physically harming someone or physically sabotaging something. Especially corporations with a high focus on know-how and technology have to prevent potential theft of data or technology as that is crucial for their business operations and competition.

Preventing employees to harm the company is no easy task. There are, however, specific measures that can be taken to reduce the risk of harm from the own workforce. One of the measures that are already in great use by authorities all over the world is background checks of employees. This is to guarantee, that they have never before conducted any crimes or shown any signs of unusual behavior that could be seen as a foreshadowing of conducting misbehaviors or crimes in the future (Barrett, 2001).

The concept of background checks or "Pre-Employment Screenings" (PES) is nothing new and regionally more or less common. This paper does not want to critically deal with the concept of PES itself, but shall instead take a look at another, sometimes less obvious problem: the challenges of a global realization of a PES program. The basis of any security measure relays in a holistic approach to effectively reduce a risk. As such, internationally operating companies might be faced with the challenge to design measures that are working among all parts of the organization. These challenges are surely not a sole security related problem and also apply to other aspects of a company's organization. However, these generic challenges will not be the focus of this

paper and only be dealt with if important for the specific process described in this paper.

The following paper will take a look at what challenges a company faces when dealing with a globally targeted PES program. PES as a concept will quickly be explained by taking a best practice model as an example. This model will not be critically reviewed but rather explained to derive the critical points that could pose a problem when trying to implement such a process globally. The focus will then shift to the generic, global challenges. It should be mandatory that each company might face a variety of challenges that might be similar to other companies' challenges but also a variety of individual challenges. In this paper, the considered challenges shall focus solely on a generic level that can be expected from a PES process. The third part of the paper shall then show what impact these challenges have on the PES process. As no individual challenges will be taken into consideration, the results of this paper shall be a generic approach to implement PES on a global level without trying to be seen as an implementation guideline of any kind.

2 What is Pre-Employment Screening (PES)

Before taking a closer look at the challenges for implementing a global PES process, such a process shall first be described. As it is not the intention to critically review existing PES models or to create a new approach, an established model shall be introduced here that will serve as the basis for the following considerations.

2.1 Purpose of PES

PES is utilized to assess the honesty and integrity of future employees prior to their employment (Barrett, 2001). This shall guarantee that the applicant does not pose an elevated risk to the company due to possibly existing bad character traits or dishonesty. According to a German survey regarding information security, it is assumed that more than 70% of incidents resulting in know-how loss or information theft in German companies are initiated from an employee within the company (SiFo, 2010).

To mitigate this risk factor, employee checks or screenings can be chosen as one measure or control. These checks are regionally more common in for instance the US than in Europe. This is often a result of regulatory uncertainty, especially since these screenings might be seen as privacy invasive (Deloitte, 2012). They are nonetheless a control that is in the realm of possibilities and can serve a purpose. Specific national or supranational regulations may even require specific PES-like methods to be conducted depending on the field of profession. Examples could be the German Aviation Security Act, requiring that all personnel working in specific aviation security relevant areas to undergo a screening process (LuftSiG, 2005 & LuftSiSchulV, 2008). Or the compliance checks needed to comply with EU anti-terror regulations in order to avoid penalties connected to foreign trade activities or to receive specific certifications like the “Authorized Economic Operator” (Maier, Berens & Schweitzer, 2017).

2.2 PES model (by Maier, Berens & Schweitzer)

To establish a common understanding on PES, a best practice model by Maier, Berens and Schweitzer (2017) shall firstly be explained. This model is characterized by a risk based approach that focuses on strategic goals and is considered compliant with the European data protection regulation. This allows for a greater flexibility when applying specific screening methods, as they can vary in form and depth as long as the strategic goal is met. The model itself also follows a set of principles that are seen as a baseline requirement. These include:

- Transparency
- Consent
- Fairness
- Adequacy (Maier, et al. 2017).

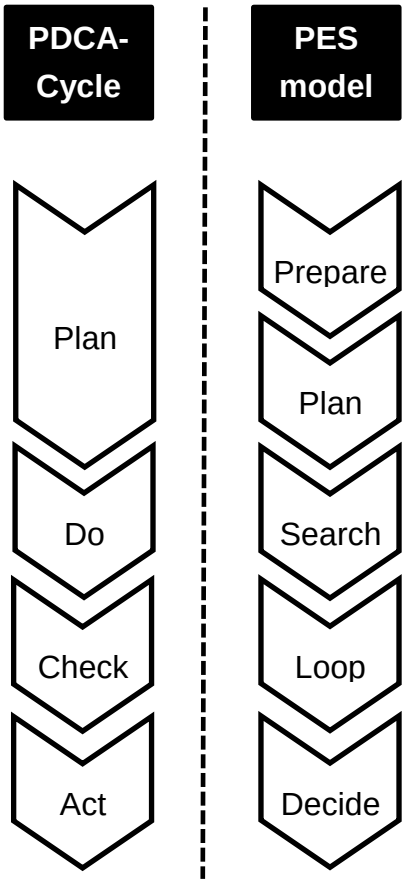

Figure 1: Overview PES model with comparison to PDCA-Cycle (created by the author on basis of Maier, et al. 2017).

These principles shall guarantee, that the PES process is transparent and known to the affected people, allows them to decline their participation in said process[1] and that the screening is limited to only the required and necessary depth, based on the associated and suspected, individual risk. Following these principles, the model is divided into five different phases. These phases could be considered an extended PDCA-Cycle (reference *FIGURE 1*).

Prepare: The first phase will define the companies policy on PES. It should answer the most important questions and determine possible exception processes. Depending on internal and external requirements, these policies can vary from company to company. Internal requirements take into account the individual risk management policy or philosophy of the company, its organizational goals, ethical values and its risk appetite. External requirements focus on the competitive environment of the company, regulatory requirements that may force the company to consider specific screening methods or the social environment. The resulting policy will be the framework by which PES will be implemented (Maier, et al. 2017).

Plan: The second step shall define the operational guideline by which PES will be conducted. Core of this step will be a risk profile of the individual position. The risk will determine the depth and scope of the screening. So called red flags will be defined, that are later relevant to indicate if a finding from the screening is relevant or not (Maier, et al. 2017).

Search: The third phase is the actual screening phase. Sources will be identified to acquire information from before actually gathering the information. Especially the previously defined red flags will be indicators for possible findings (Maier, et al. 2017).

Loop: The loop phase allows the applicants to justify possible findings. If red flags were found in the search phase, it does not necessarily indicate a dishonest applicant. This phase is supposed to separate

[1] According to the model chosen, participation shall always be voluntarily. As such, people that decline to participate in said screenings have the right to do so, but this might inevitably impact their application. In addition, the consent allows for a greater set of screenings to be conducted.

the false positives from actual dishonest applicants (Maier, et al. 2017).

Decide: Eventually, the last phase will result in a decision to hire or decline an applicant (Maier, et al. 2017).

Now, the actual screenings will be dependent on the associated risks of a position or function. To help determine the risk, Maier, et al. (2017) defined six attributes that need to be considered:

- Extremist attitude
- Problematic financial conditions
- Identity disguise
- False declarations
- Drug abuse
- Lack of integrity

Each of these attributes will be rated in regards to internal and external influences. Internal influences meaning company internal rules and regulations, risk appetite ethical values etc. External influences reference standing legal obligations, industry[2] or social influences. The rating itself could e.g. be based on a three level classification from low to medium to high. Now, the attributes itself would determine the kind of screening to be conducted (e.g. regarding problematic financial conditions, credit checks could be used), while the rating of the attribute could determine how intense the checks should be conducted. Eventually, you could end up with a little matrix that shows which attributes apply to the respective function / position on hand and how intense the checks need to be conducted. *TABLE 1* shows how a risk profile could look like for a specific position within the company.

[2] Depending on the industry, competition and the threat of internal theft might be higher or lower, thus it needs to be taken into consideration as an external influence.

Table 1: Example risk profile for a specific position within the company (created by the author on the basis of Maier, et al. 2017).

Attribute	Severity	Intensity of screening
Extremist attitude	Low	No screening required
Problematic financial conditions	High	High
Identity disguise	Medium	Medium
False declarations	High	High
Drug abuse	Low	No screening required
Lack of integrity	Medium	Medium

Should a screening be required and eventually conducted for an attribute, there needs to be a method to distinguish when a finding is actually relevant and could lead to a negative impact for the applicant. Therefore, Maier, et al. (2017) proposes to define so called Red Flags. Red Flags are simply indicators that a risk in regards to the attribute is likely to exist. In other words, red flags are predefined thresholds for possible findings. To follow the core principles of the process, everything needs to be transparent. Therefore it needs to be defined in advance what kind of finding could lead to a negative impact for the applicant. If these red flags would not be defined prior to the screening, than the applicant would be at the mercy of whoever will be rating the screening findings.

3 Global challenges for a PES process

Looking at PES from a global perspective, a centralized approach means that the PES model shortly explained above needs to be rolled out in all parts of the company. This might show challenging due to various aspects that need to be taken into consideration. The most relevant aspects shall be mentioned in order to derive an approach that shall help to overcome these aspects and show possible solutions for implementing a global PES process.

3.1 Identify stakeholders

Among the company, there will be different stakeholders that need to be identified when considering introducing a PES process. These stakeholders could roughly be sorted into two groups. Stakeholders who would be impacted by the process and stakeholders who themselves require the process to be implemented. Without intending to provide a concluding list, the following stakeholders would most likely be of interest and potentially impacted by PES:

HR: Operational handling of PES and need to implement the process into their existing process landscape.

Labor law: Will be interested, that the process does not violate any standing laws and that the consequences of such a screening will be within allowed boundaries.

Data protection: Just like labor law, will be interested that no data protection violations exist.

Information security: Needed to help with the risk analysis by advising on which kind of information should be of concern and needs to be within the scope of PES.

Workers council: Will care a lot that employees (or future employees) will receive a fair and legal treatment during their application.

Now, this is already a very simplified list that shall simply serve as an example. Looking at a global rollout of such a process, much more stakeholders could be impacted. Local departments of the above mentioned organizational units might all have to be considered as well as stakeholders that may be specific to the individual company.

The second group of stakeholders might not seem as obvious at first. But some departments among the company might already be bound by specific regulations (see *SECTION 3.3*) to have a PES-like process in place. Identifying these demands will be crucial in order to avoid parallel processes later on by incorporating them into the scope of the PES process. This might also determine the kind of risks that do exist and the screening methods needed. A company from the pharma industry e.g. might require the screenings to focus much more on drug abuse than on other risk attributes.

3.2 Assessing already established procedures among the company

It is very likely, that a globally operating company already has some kind of PES-like processes implemented among some parts of the company. They may not always be classified as such and thus can be hard to identify. But be it based on regulatory requirements, insurance topics or local customs, some kind of background checks might already exist. These might not be centralized, but only apply to a specific part of the company. Even HR might differ from region to region and might already conduct some kind of background checks.

Identifying all these existing processes can be hard and requires to get in touch with the right people as the information is most likely not centrally available. But in order to implement a process that can be applied to all locations and one that can be centrally steered, it is important to know of these locally existing checks. Otherwise the new process might not fit in with the already existing processes and the results could hardly be anticipated. Economical loss could be only one of many possible impacts.

But not only the possible negative impact needs to be considered, but the existing processes might show what kind of checks or screenings should be considered to make sure that the new, global process considers all existing risks among the company.

3.3 Different regulatory requirements – boundaries of PES

It is in the nature of PES that these measures and processes can be very intrusive and therefore need to be in accordance to a variety of different regulations. Specifically data privacy and labor law need to be considered in order to not violate any applicable law. As initially stated, the regulatory requirements for PES will not be looked at in detail here. That topic alone is rather extensive. However, the regulatory requirements are nonetheless an important factor when looking at PES. Without looking at the regulatory requirements of different countries in this paper, the important point to get across is that these different requirements exist and need to be considered when rolling out a global PES process. It is not sufficient to e.g. check the law in Germany and match the process to comply with the German regulation. Things that might be legal here might not be legal or merely not possible in other countries.

To make an example, with the consent of the applicant, it might be legal to conduct credit checks in Germany to determine if an applicant lives outside his financial boundaries. However, this check, even with the consent, might be illegal in other countries, or there might simply be no way to acquire that kind of data due to lack of institutions. Now, this fact needs to be considered to avoid situations where some applicants will have to undergo these checks, whereas others don’t although they applied for a similar position or function within the company; so obviously they should have a similar risk profile associated with them. And as initially stated fairness is one of the principles for a good PES implementation, so comparability should be given to keep it fair for the applicants.

3.4 Process control

Another challenge that arises is the control over the process itself. Implementing a central process worldwide requires a good infrastructure in place. Colleagues around the world need to be able to support this process. Otherwise it will be nearly impossible to account for it centrally. After all, a central process needs to be enforced and implemented by the same environmental conditions. It needs to be guaranteed, that the process generates the same results regardless of location. But in order to give this guarantee, experts would need to be in place that are all knowledgeable about the process

and who can support the implementation on site. Even the quality of the screenings itself needs to be assured in order to follow the process principles as defined by Maier, et al. (2017).

4 Standardized PES approach – Considerations

To overcome the challenges identified previously, a standardized approach seems to be needed. Only a standardized approach can assure that the process will be comparable among the company and that the mitigation levels are identical as it should be for a holistic approach. There might also be other approaches available so this shall be seen as only one approach to mitigate the existing challenges.

4.1 Define security levels

The first step to a standardized approach could be the implementation and definition of security levels. To make checks comparable among the company while still maintaining a risk based approach, defining a set of predefined background checks and associating them with different, elevated risks could be a viable approach. That means that instead of defining an individual risk matrix as shown by Maier, et al. (2017) a set of e.g. three different security levels could be defined. An example can be seen in *FIGURE 2*.

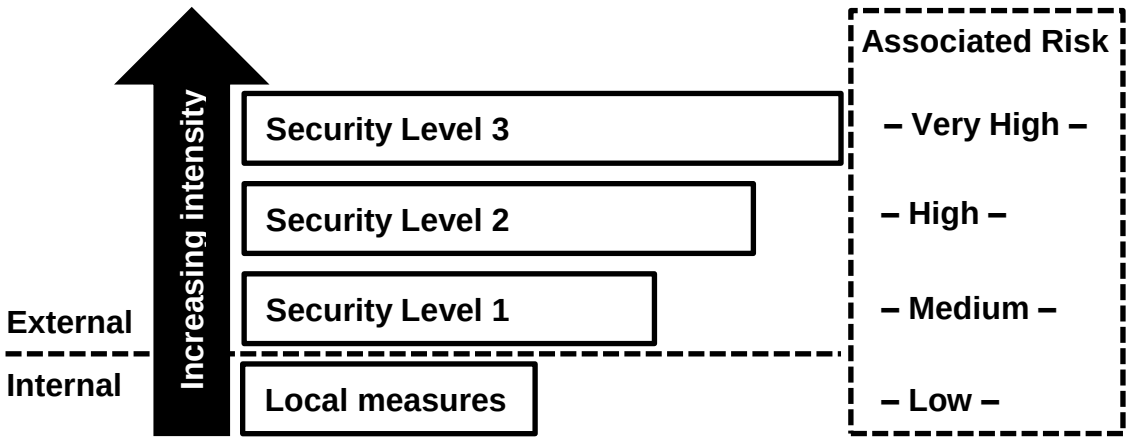

Figure 2: Security level structure (created by the author, 2019).

In order to account for possible local checks that might be conducted based on reasons other than security, those could still be done but they would be outside the actual PES scope. As seen in *FIGURE 2*, those checks could be subsumed under “local” checks that apply for low risk functions or positions only. Leaving this door open preserves the existing local customs while integrating them into the bigger picture. So these processes are to some degree also part of the new PES process. Obviously, this is only intended for risks below a specific threshold and anything that is actually security related and has an elevated risk associated should instead be integrated and considered into the actual security levels.

Now, for each security level, a set of screenings should be defined; screening methods that each intend to focus on one of the risk attributes as defined above by Maier, et al. (2017). The higher the security level, the higher the risk and therefore the more intense should the screenings be.

Table 2: Screening methods per Security Level (created by the author, 2019).

Security Level	Screening Method	Risk Attributes
Local Measures	Undefined	• Undefined
Security Level 1	Compliance checks	• Extremist attitude • Lack of integrity
	Educational achievements	• False declarations
	Past employments	• False declarations
	Address validation	• Identity disguise
Security Level 2	Credit checks	• Problematic financial con.
	Reference checks	• False declarations • Lack of integrity
	Media search	• Extremist attitudes • Drug abuse
Security Level 3	Self-Employment	• Lack of integrity
	Equity investments	• Lack of integrity • Problematic financial con.
	Network visualization	• Lack of integrity
	Political connections	• Extremist attitude • Lack of integrity
	Reputation assessment	• Lack of integrity
	Criminal record	• Extremist attitude • Lack of integrity • Drug abuse

TABLE 2 shows one example how the screenings could be arranged within the security level structure. The higher the risk (or security level) the more intense and the more diverse the screenings could become. While the screenings focus on some basic verification checks for medium risks, they could become much more diverse and intense for higher risks. In the example above, the screenings focus mainly on risk attributes such as false declaration and identity disguise for medium risks. For high and very high risks, the checks focus more and more on lack of integrity problematic financial conditions and extremist attitudes. It should be noted that in the example above it is assumed, that each security level incorporates the lower level. That means that a security level 2 would automatically include all security level 1 checks.

This approach appears to be in conflict with the individual risk based approach by Maier, et al. (2017). But it is a needed tradeoff to convert a pure risk based consideration to a more pragmatic and more economic approach. Defining a risk profile for each individual position or applicant could be cumbersome; at least when trying to conduct the actual screenings. The missing standardization would require a very individualized operational handling that would result in higher costs and a missing comparability. Only with this tradeoff can a standardized and comparable process be guaranteed. Eventually, the security levels would be consistent among the company and regardless where the screening has been conducted, employees with the same security level would have gone through the same screenings.

To further support the standardized approach and to also mitigate the challenge of process control it should be considered if the PES process itself can be outsourced. Specialized companies could conduct the actual screenings which might be more cost effective and due to their networks they could make sure to support a worldwide rollout as their peers could make sure that the local handling of the PES process fits the desired process description. Overcoming this challenge within the company could proof difficult. As shown in *FIGURE 2* the screenings could be split into internal and external screenings. As already mentioned, the local screening measures might be part of the PES process itself, but they are not part of the standardized security levels. As such, these checks could still be conducted internally without impacting their current implementation among the locations. Only the standardized security levels could be outsourced for the mentioned benefits.

4.2 Define job profiles

After defining the security levels, it needs to be determined which position or function requires which screening. This would be the substitute to the defined risk profiles by Maier, et al. (2017). Taking the internal and external influences into consideration, the main functions and positions within the company should be pre-rated with a respective security level. This can be done centrally (as far as possible) once for each function and position. Eventually, when a vacancy becomes available it would already state the needed security level and a candidate would have to comply with these requirements during the hiring process.

To define the job profiles, a check-list could be established, helping to identify the criticality of a function or position based on different characteristics. The method shown by Maier, et al. (2017) could be used to assess the risk, in addition to company specific considerations (responsibility of the position, general risk appetite, risk exposure, etc.). The check-list could also be used to allow each department to rate new positions they might tender and allow them to "generate" the needed security level themselves.

4.3 Role of security in PES

Ideally, PES should be a process integrated into the HR process landscape and handled solely by HR. It should be just another step needed when applying for a position. *FIGURE 3* shows how this process could be integrated into the existing recruitment and hiring process. The dark process steps show the two additional PES related process steps. Overall, PES can be integrated quite nicely into the existing HR process landscape.

Figure 3: Example of integration of PES into the existing recruitment and hiring process (created by the author, 2019).

Security should have little to no stakes in the operational handling of PES. Security should instead be responsible for the PES process itself and make sure that the standardization is implemented in a meaningful and logical way. In addition, they might be seen as consultants to support other

departments regarding the rating of positions and functions where needed although the responsibility would remain with the individual departments. This approach will require that the actual screening is conducted by an external service provider. HR itself could not conduct the screenings, nor could security take over this for a big, multinational company.

Something that also needs to be taken into consideration is an exception process. A simple black or white approach might not be realistic as it is likely that situations will emerge where the screening itself might result in red flags, but in the following loop phase, the applicant might be able to give good explanations. Or the applicant might be unable to disproof some of the findings, yet the department would still like to hire him due to little or no alternatives available. This means the risk treatment becomes a risk acceptance. At this stage, the security department should be consulted in order to give advice on possible mitigating measures that do allow hiring an applicant that poses an elevated risk. These measures need to be chosen on a case by case basis. In the end, however, the department would have to acknowledge the risk and be held accountable for it.

5 Conclusion

PES as a security measure seems to be more and more in the focus of companies as the threat from the inside becomes more aware. In the end, PES is just another possible measure available to cope with the existing risks in order to try and mitigate those risks. However, since PES is targeting the employees or applicants directly it is an especially sensitive topic that requires more sensitivity than other measures. Similar to other security measures, PES can also not guarantee complete security. It can merely reduce the existing risks, but it cannot prevent employees from becoming a threat after years of working for the company. Given that complete security cannot be guaranteed, it needs to be determined if the price (i.e. “privacy intrusion”) is worth the actual results.

Should it be decided to implement PES on a global level, then a few considerations need to be made. Best practice approaches for PES do exist, but the challenge will be implementing those in an effective way. Decentralized approaches appear less desired as the workforce would be treated differently although the underlying risk will be the same nonetheless. Therefore, a central, standardized approach seems needed. Only then can the process be part of a harmonized, holistic concept.

But a standardized approach also means that a pure risk based concept might not be feasible as it will be nearly impossible to effectively and economically roll this out among all parts of the company. Compromises need to be made in favor of cost efficiency and comparability. Eventually, a process could be generated that could be easily outsourced to further streamline the screenings itself. Specialized service providers could guarantee not only data privacy compliant handling, but also that the standard will be enforced in all parts of the world.

However, the standardization might lead to that specific screenings cannot be conducted because they are not possible all around the world. Now, a decision needs to be made whether or not these screenings are only conducted in some countries or if these screenings are left out fully. Should they

be partially conducted, then the standard might no longer be comparable. But if they are left out fully, then the screening process itself might no longer be as effective as it should be and might have to be questioned. To follow up on this, it might be very interesting to focus on the screening methods itself in order to identify all possible screenings available (for all the risk attributes) to then evaluate how many of them are enforceable on a global level.

Bibliography

Barrett, P. (2001). Pre-Employment Integrity Testing: Current Methods, Problems, and Solutions. *British Computer Society: Information Security Specialist Group March 29th-30th, 2001, Milton Hill, Oxford*.

Deloitte (2012). Risikominimierung bei der Personalauswahl. [Studie]. Momentaufnahme zur Lage von Unternehmen in Deutschland.

Luftsicherheitsgesetz [LuftSiG]: Luftsicherheitsgesetz (LuftSiG) vom 11. Januar 2005 (BGBl. I S. 78). Zuletzt geändert durch Artikel 1 des Gesetzes vom 23. Februar 2017 (BGBl. I S. 298).

Luftsicherheits-Schulungsverordnung [LuftSiSchulV]: Luftsicherheits-Schulungsverordnung (LuftSiSchulV) vom 2. April 2008 (BGBl. I S. 647). Zuletzt geändert durch Artikel 182 des Gesetzes vom 29. März 2017 (BGBl. I S. 626).

Maier, B., Berens, H. & Schweitzer, A. (2017). Pre-Employment-Screening. *Ein risikobasierter Praxisleitfaden zur Bewerberüberprüfung im Personalauswahlverfahren.* Boorberg Verlag.

Sicherheitsforum [SiFo] (2010). Know-how-Schutz in Baden-Württemberg [Studie]. SiFo-Studie 2009/10.

Statutory Declaration

I hereby declare, that I produced the following paper on my own using no other but the mentioned literature and resources and that this work has not been submitted to any other examination office in identical or similar form.

Friedrichshafen, 29.03.2019

Place, Date

Signature

(Hendrik Müller)