Group 16 Research Summary

1.Title and Citation of the Paper

- **Title:** Towards Automated Continuous Security Compliance.
- **Authors:** Florian Angermeir; Jannik Fischbach; Fabiola Moyón; Daniel Méndez Fernández.
- **Year of Publication:** 2024.
- **Full Citation (IEEE style):**
  F. Angermeir, J. Fischbach, F. Moyón, and D. Méndez Fernández, "Towards Automated Continuous Security Compliance," *Proc. 18th ACM/IEEE Int. Symp. Empirical Software Engineering and Measurement (ESEM '24)*, Barcelona, Spain, Oct. 2024, pp. 440–446.

2) Objective and Research Question

- **Main objective:** The main objective of the research was to identify the practical challenges of Continuous Security Compliance (CSC) in Continuous software Engineering (CSE), and lay out a roadmap to help different industries (including highly regulated industries) in selecting the right automation tool to introduce automation into CSC in a problem driven way.
- **Research goals/ questions:** The authors laid out their goals for the research as below:
  - understand the challenges of adhering to security compliance regulations in continuous software engineering projects
  - understand requirements and constraints for automation in Continuous Security Compliance as suggested in literature and practice
  - analyze the potential and limitations of automation as treatment towards the identified challenges and its implications for manual involvement
  - develop and evaluate – along the previously determined potential and limitations – sensible solutions containing automation in industrial settings to treat respective challenges

3) Technique/Methodology

The technique they used for their research:

1. **Defined the term:** They first clarified what Continuous Security Compliance (CSC) means by doing an ad-hoc review of existing papers and by extending that definition to encompass its efforts in making Continuous software Engineering more efficient.
2. **Collected and verified challenges:** Next, they ran a tertiary literature study to gather CSC challenges reported in prior work and validate them. Afterwards, they aggregated the remaining unverified challenges into 12 new challenges.
3. **Identified challenges, root causes and requirements for automation:** Next, they carried out in depth interviews with CSE stakeholders targeting the root causes of the challenges,

their automation potential, and respective limitations and requirements for their automated treatments.

4. **Planned and carried out state of the art analysis and solution design:** Afterwards, they set up a design science roadmap with an industry partner to build and test automation in cycles: survey → interviews → solution design → real world (industrial) validation.
5. **Laid down benchmarks for treatment validation:** They planned to test their design based on 3 criteria:
   (1) the satisfaction of the requirements identified in step 3
   (2) the impact on Continuous Security Compliance, and
   (3) the value added by the treatments to CSE projects

Contribution to the field: It's the first research to define Continuous security compliance in terms of its impact on Continuous Software Engineering and to lay out a design science roadmap tailored to CSC. It's a clear upgrade over ad hoc approaches because it provides a practical, integrated method to plan and test CSC automation.

4) Datasets Used

- **Datasets:** The paper's evidence comes from a tertiary review of past studies, with plans for future industry studies.
- **Availability/Coverage:** The protocol and analyzed data are publicly available as supplementary materials. The coverage reflects CSC challenges in continuous software engineering as reported in prior research.

5) Results

- **Experiments conducted:** The paper doesn't do experiments. Instead, it presents a validated list of real-world challenges found in prior studies (grouped into clear categories with specific items), aggregates unvalidated challenged into 12 new challenges, lays out a design science roadmap tailored to CSC and plans to test automation solutions later with industry partners.
- **Key metrics:** Not applicable here. For future industry tests, the authors plan to measure impact on CSC and value added to CSE practices as well as if the requirements laid out by the organization have been met. But those results aren't available yet.
- **Summary vs. baselines:** There are no baselines to compare against. The main outcome is a design science roadmap to guide different industries incorporating automation in CSC.

6) Overall Findings

Main findings:

- A clearer definition of Continuous Security Compliance (CSC) that fits both continuous software engineering and real regulations.
- A validated, expanded list of CSC challenges, including new ones like the heavy effort of evidence generation and limits in pipelines/tools.

- A design science roadmap to build and test automation with industry teams and auditors as well as benchmarks to test these systems against.

Support for the objectives:

- These results answer the first 3 goals (definition, challenges, where automation can help) and set up how to accomplish the last goal (testing in real industry settings).

Limitations / future work:

- The actual automation solutions and quantitative evaluations are future work to be done with industry partners and assessed for auditor acceptance.

7) Insights and Critical Analysis

Insights / reflections:

- This paper is a solid starting point. It gives common terms, a clear map of the problems, and a practical plan to move from ideas to tests in real companies.
- The argument is backed by a literature review and an industry-linked roadmap. And the authors are open about limits (the ad-hoc review).

How to improve:

- Automation pipelines (e.g., evidence generation and control mapping) and report metrics like coverage, time to evidence, and auditor acceptance could be built.
- Specific data models could be provided for these purposes.

Contribution to our work:

- It shows us where automation is needed (evidence generation, pipeline integration, and handling tool findings).
- It shows us a design science path to build and test these solutions, which will give us a strong foundation on AI-enabled compliance research.

8) Relevance to our Research

- **Relevance:** Our topic is AI in Cybersecurity Auditing & Compliance Monitoring. This paper defines Continuous Security Compliance (CSC) and lists pain points that fit AI well like automating evidence collection, mapping controls to system artifacts, and sorting issues by importance.
- **Adaptable techniques/findings:** Although this paper doesn't pick specific AI models, it clearly shows where to apply AI and how to validate it using a design science approach with the help of surveys, interviews, pilot deployments, and auditor review. That could be helpful.
- **What we plan to contribute:**

- We plan to map the issues and gaps among manual compliance and auditing methods and how it could be mitigated with the help of AI.
- We plan to research the different automation tools, their potential, limitations, and use cases to help industries make better decisions regarding automation in CSC.