DNV CYBER

IT Security Product Certification in the Era of Automated Evidence Generation and AI-Assisted Evaluation

Jussipekka Leiwo, Ph.D.
Product Cyber Security Strategy Consultant

Why This Presentation?

AI-based evidence generation and validation is not coming. It is already here

The scale, diversification of the certifications required for global markets is overwhelming the conventional certification practices

Compliance validation tools shall be used by the evaluators and certifiers and by the developers throughout the SDL

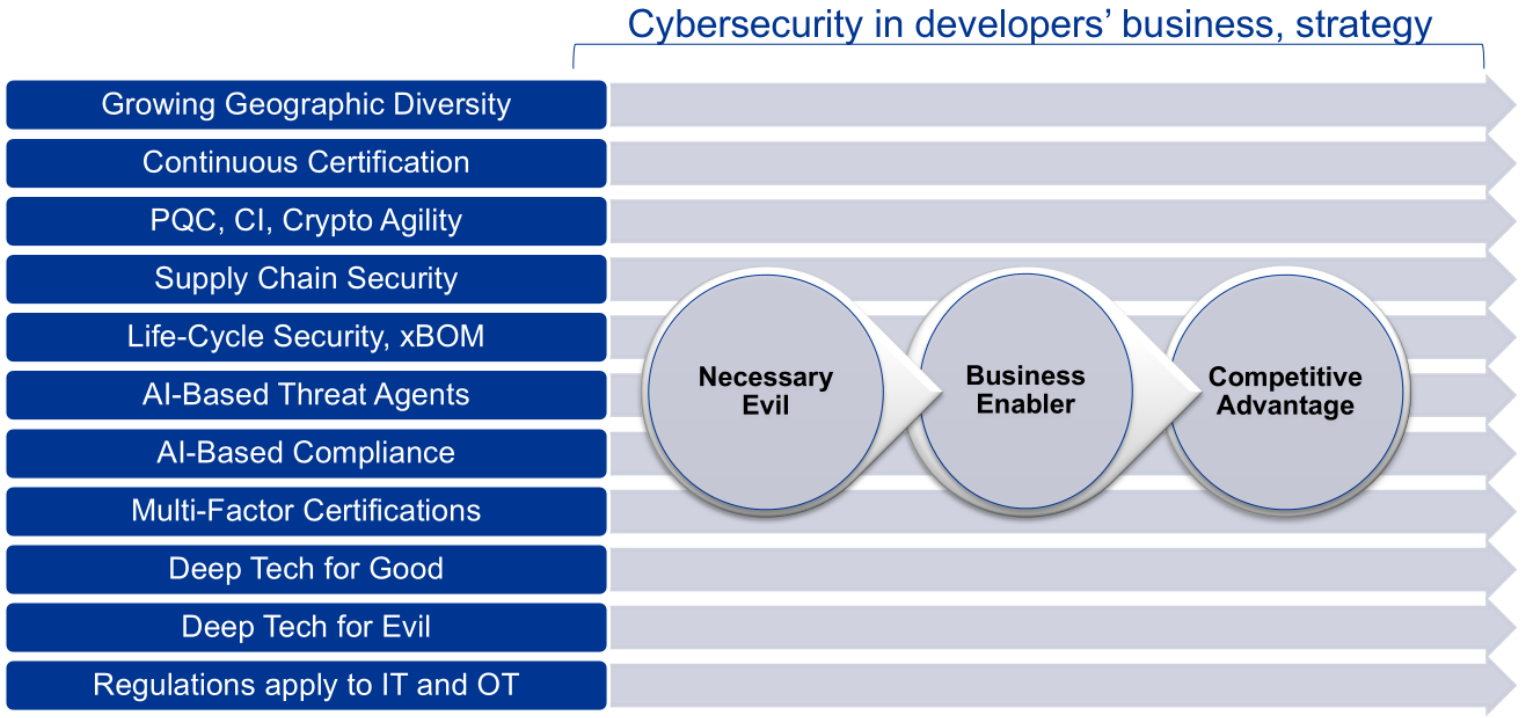
We shall use AI-based tools in accordance with AI-developed processes to evaluate and certify products developed and validated with AI assistance

What could possibly go wrong!

Let's consider the implications to the evaluation and certification processes and to the confidence in the results

DNV CYBER

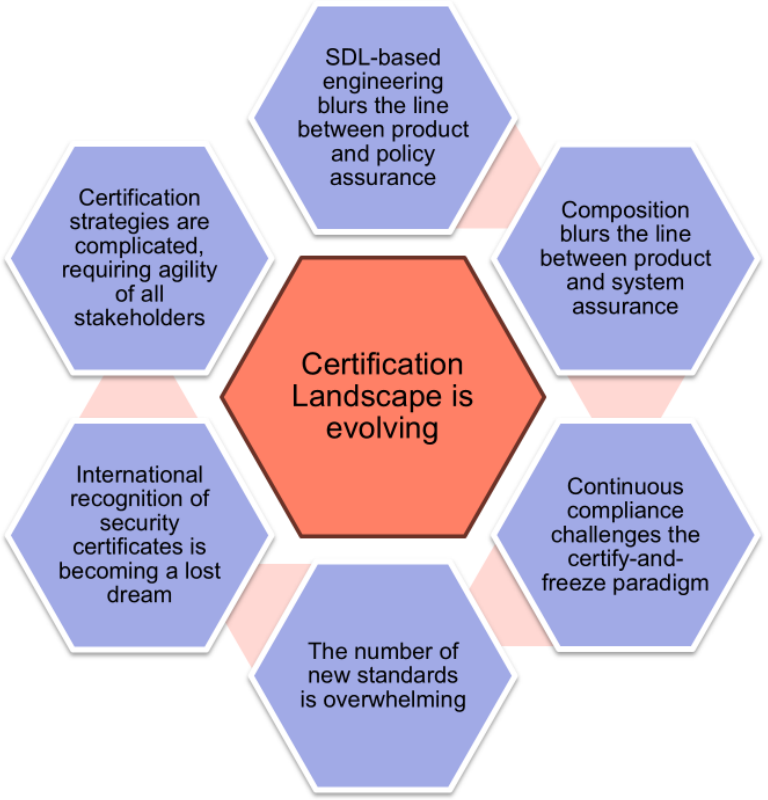
Complexifying Regulatory, Operational Environment



3 DNV ©

DNV CYBER

Giving Away the Plot Early



- Compliance validation must be brought to the early stages of the SDL
- Evaluation and certification processes must become agile, continuous
- Evaluators, certifiers must ensure that the tools used in the validation of compliance function correctly
- Classic machine learning, tools based on test automation are not sufficient to meet the challenges

4 DNV ©

DNV CYBER

Example: CyberNEMO, CertifAI.

Funded by the European Union

https://www.dnv.com/research/future-of-digital-assurance/cybernemo/

Using AI in Risk Management for AI-Supported IoT-Edge-Cloud Environments: When AI monitors AI in Critical Infrastructure

Building on the NEMO (Next Generation Meta Operating System) project, the CyberNEMO project strengthens end-to-end cybersecurity and trust across IoT-Edge-Cloud environments (often called the computing continuum). This EU-funded research initiative brings together DNV and 22 partner organizations to advance cybersecurity resilience, risk preparedness, situational awareness, threat detection, and mitigation for critical infrastructure and its supply chains.

https://www.dnv.com/research/future-of-digital-assurance/certifai/

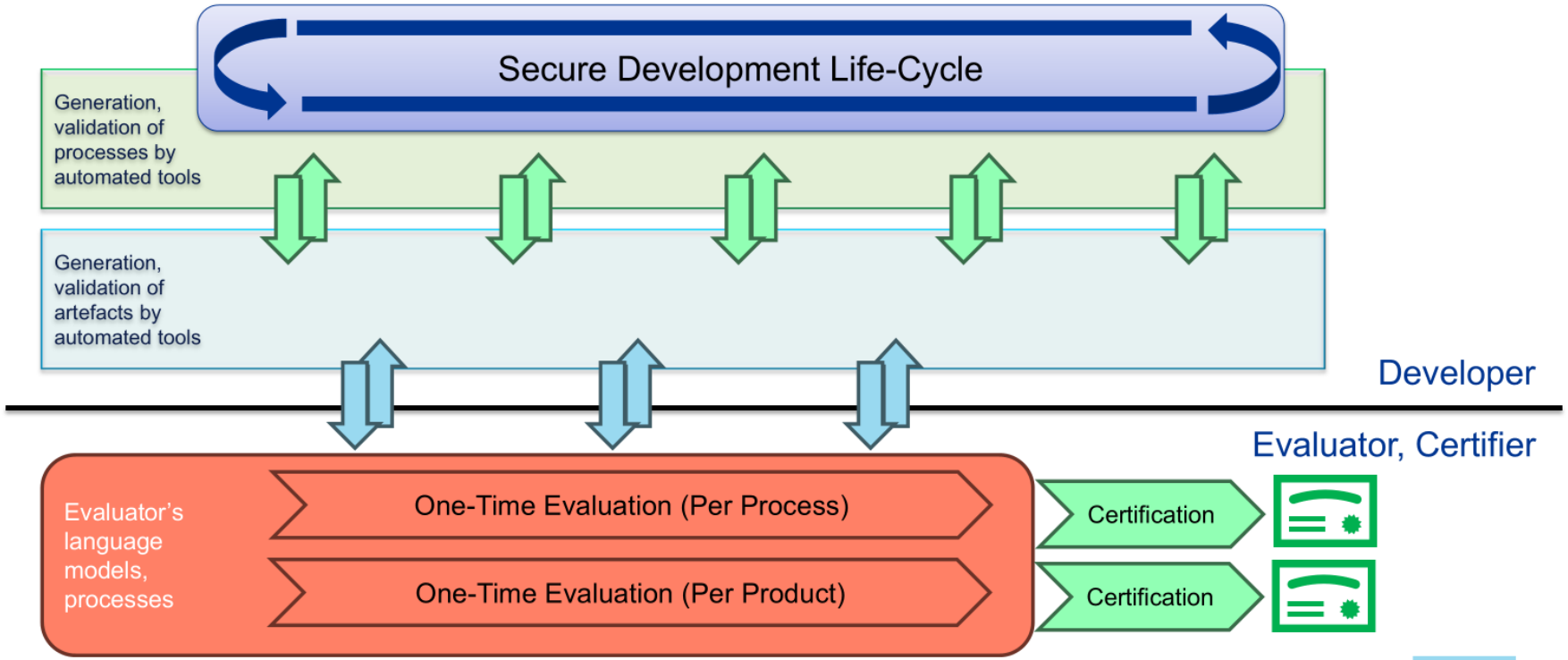
Enabling Continuous AI-Empowered Certification for a Secure Digital Future

This EU-funded research project brings together DNV and 11 partner organizations. The aim of the project is to investigate and develop AI-empowered approaches to the certification of information and communication technology (ICT) systems, driven by emerging EU cybersecurity legislation.

5 DNV ©

DNV CYBER

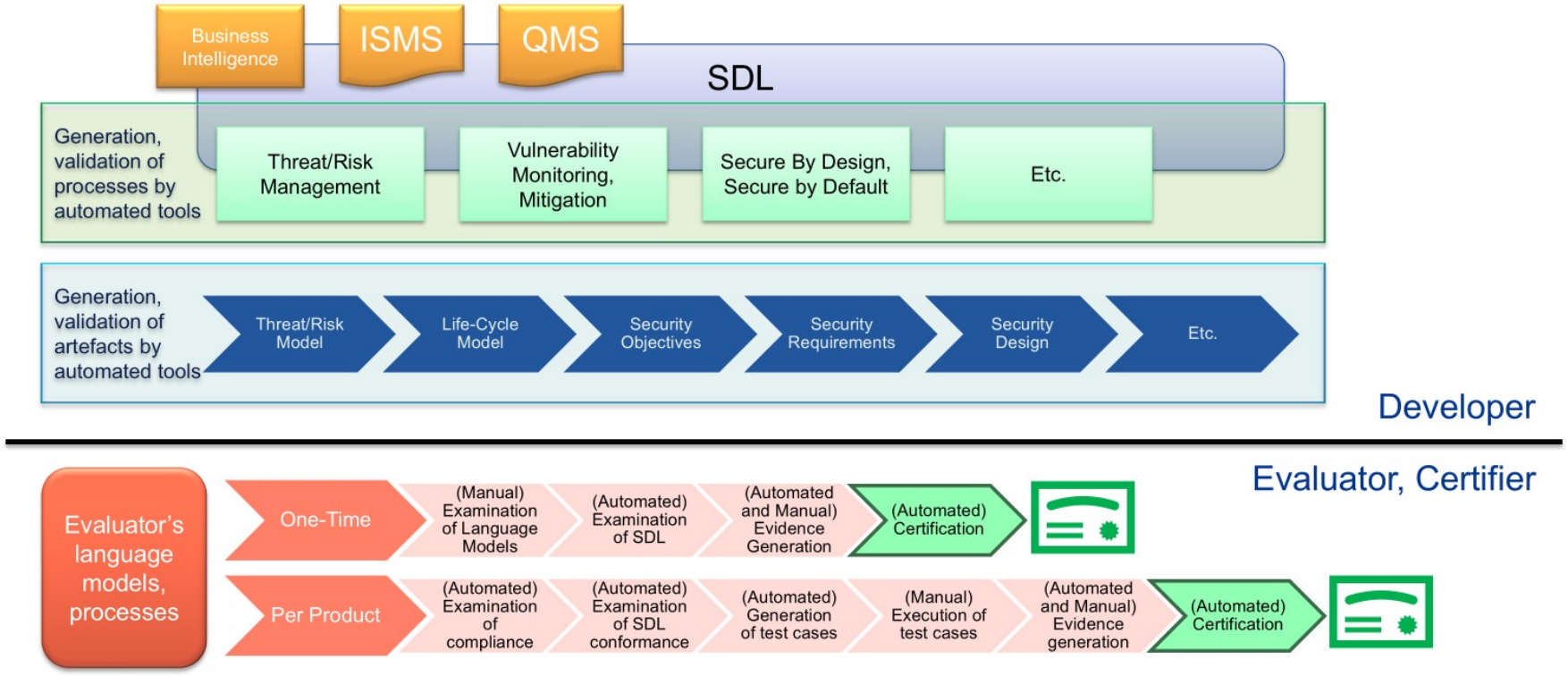
Early Validation of Compliance – High Level



6 DNV ©

DNV CYBER

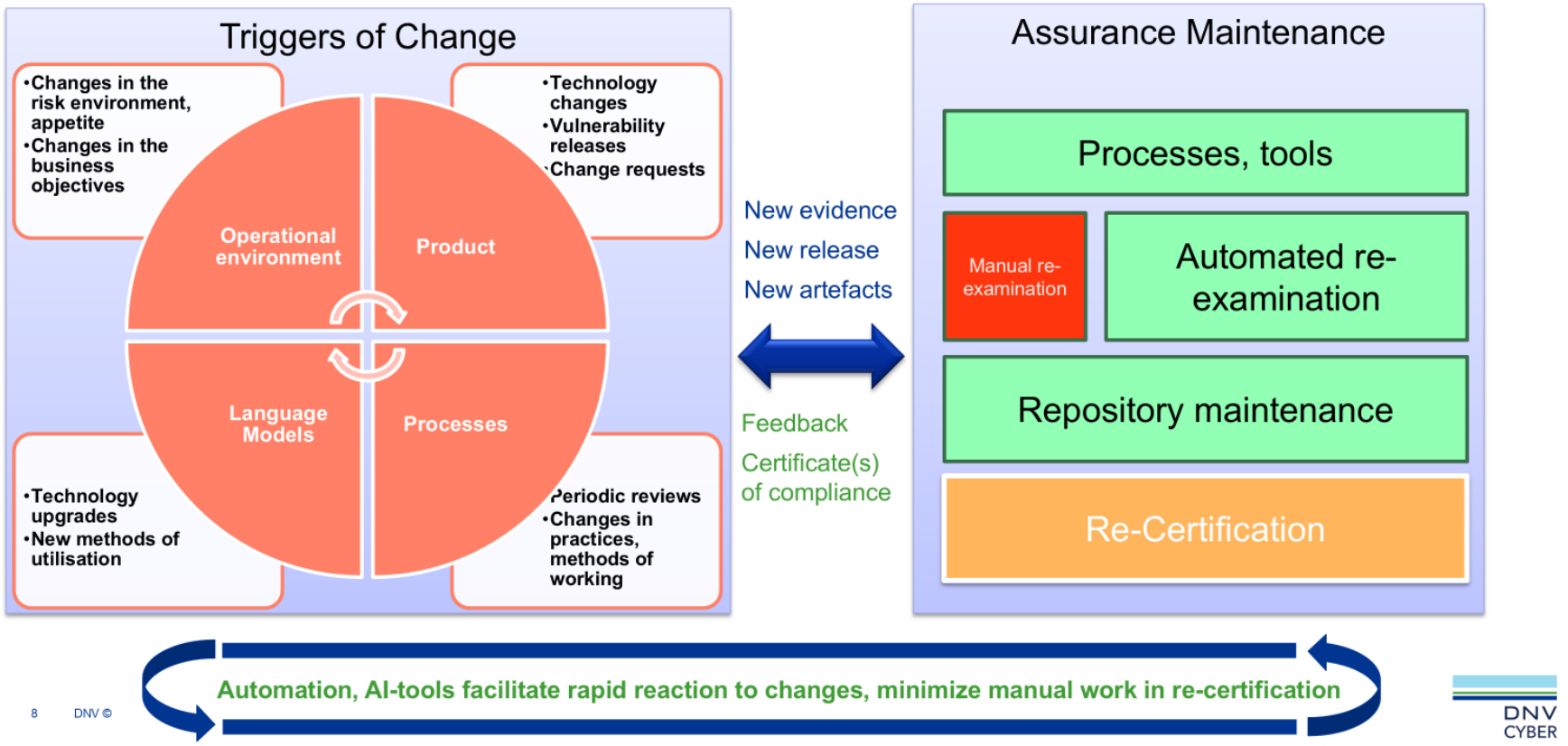
Early Validation of Compliance – A Few Details



7 DNV ©

DNV CYBER

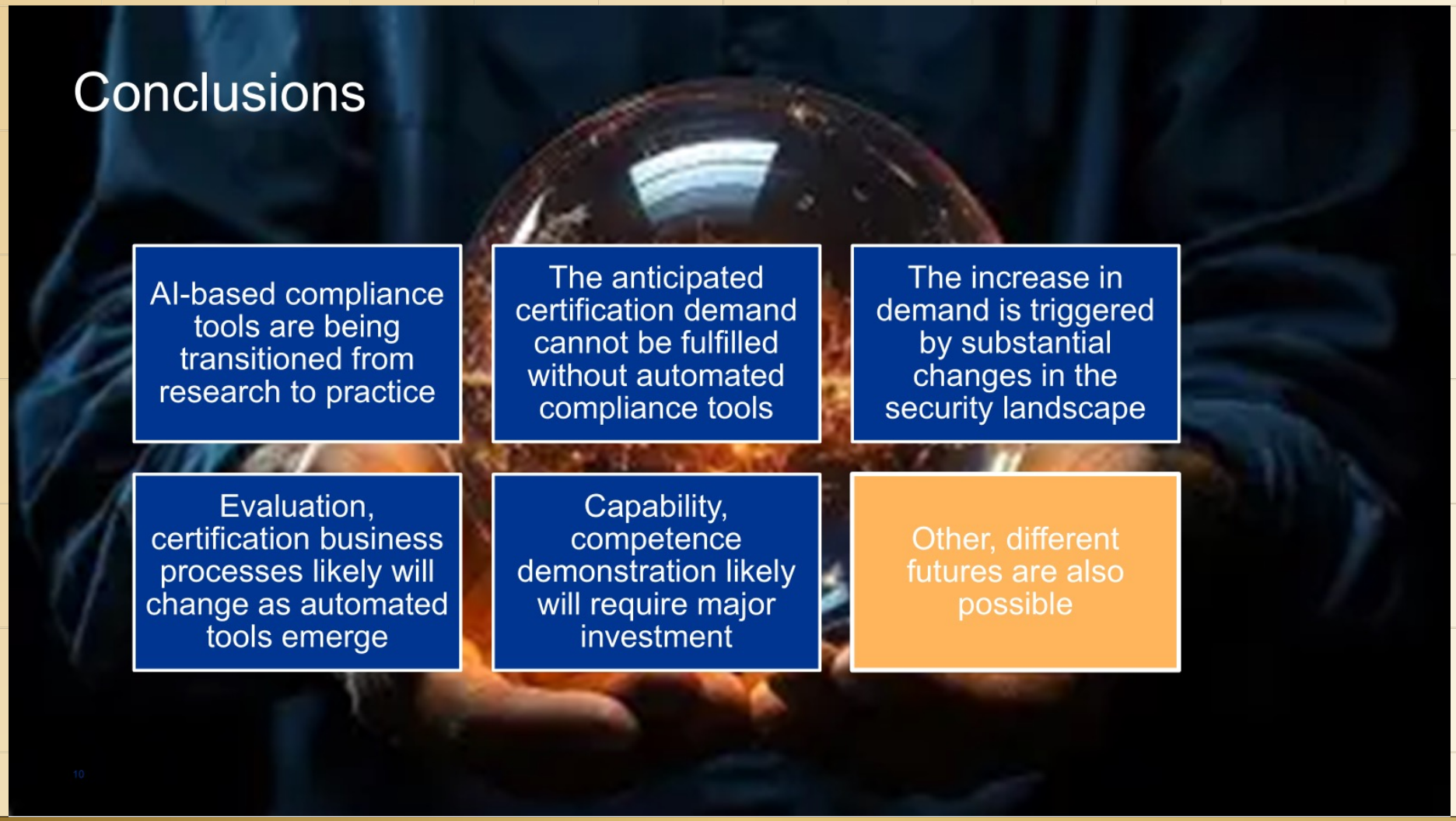
Agile, Continuous Evaluation and Certification



DNV CYBER

Can This All Be Trusted?

- Substantial effort required to validate the language models and their application
- Trustworthiness of the certificates depends on the validity, proper application of the language models
- Evaluators, certifiers must demonstrate their capabilities to the accreditation bodies
- Commonly accepted means, methods of validation of language models likely to be required
- Is language model validation an assessment method, evaluation of an artefact, or validation of a development tool?
- Likely the rigour of validation should depend on the sought assurance level
- Evaluators, certifiers must demonstrate integrity, authenticity of the language models, security of the cloud access models


Conclusions
AI-based compliance tools are being transitioned from research to practice
The anticipated certification demand cannot be fulfilled without automated compliance tools
The increase in demand is triggered by substantial changes in the security landscape
Evaluation, certification business processes likely will change as automated tools emerge
Capability, competence demonstration likely will require major investment
Other, different futures are also possible
10

Thank You

Jussi.Leiwo@dnv.com

No Large Language Models Were Harmed in the Making of This Presentation

www.dnv.com/cyber

DNV CYBER