IS Assurance – the capital C in PDCA

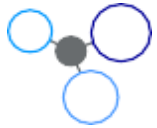
Frank Ackermann
Information Security Framework & Governance,
Deutsche Börse AG

19 November 2021

DEUTSCHE BÖRSE GROUP

“We at Deutsche Börse create trust in the markets of today and tomorrow.

Deutsche Börse Group: we cover the entire value chain



Information technology

Internal IT services, software development, connectivity services

Pre-trading

- Index and analytics products
- Investment management solutions (market-leading portfolio & risk analytics software solutions)
- Corporate governance and sustainable investment solutions
- Provision of ESG data

Trading & clearing

Cash market

- Connectivity to international trading participants
- Open electronic order books
- Trading in shares, ETFs, ETPs, warrants, funds, bonds
- Market data

Derivatives market

- Connectivity to international trading participants
- Open electronic order books
- Trading in derivatives (equity, equity-index and interest-rate derivatives)
- Verification of trade-related information
- Central counter-party for on- and off-exchange transactions (cash and derivatives markets)
- Risk management
- Market data

- Verification of trade-related information
- Central counter-party for on- and off-exchange transactions (cash and derivatives markets)
- Risk management
- Market data

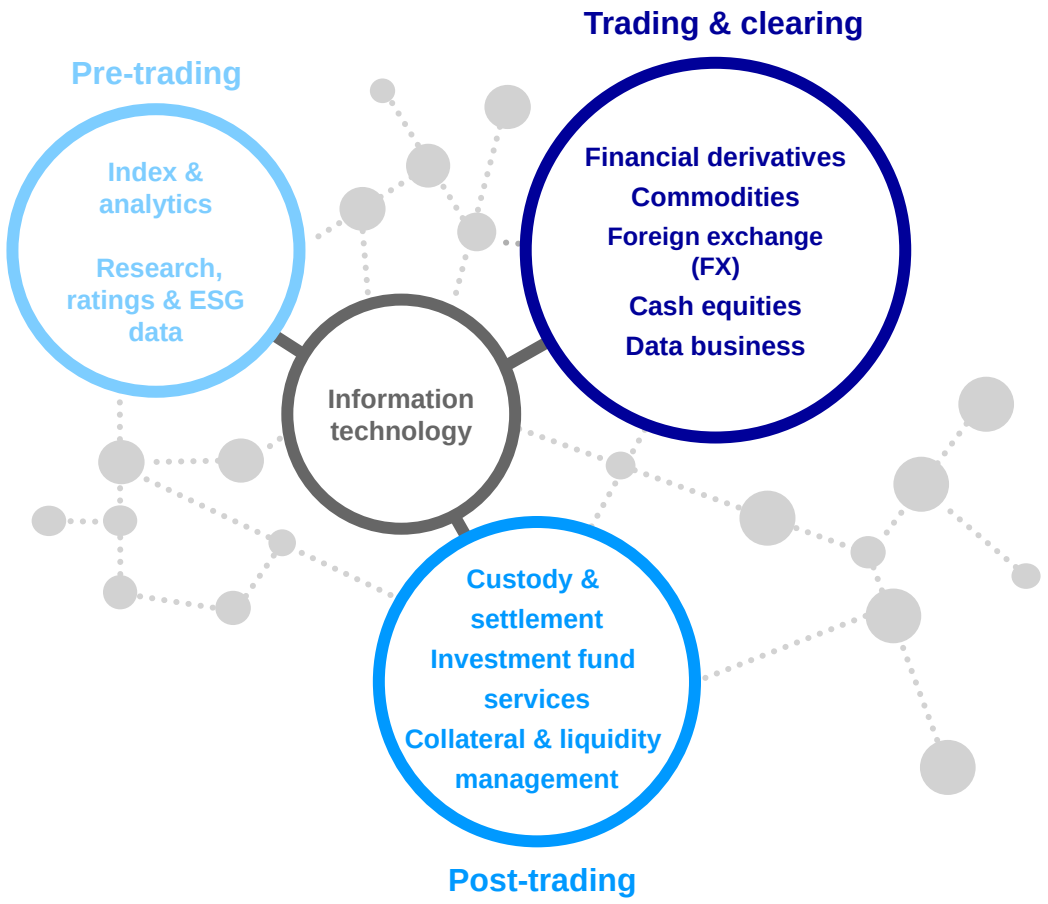
Post-trading

- Settlement and custody of securities
- Services for the issuance of new securities
- Collateral and liquidity management
- Corporate actions
- Tax services
- Trade repository services

Investment fund services (IFS)

- Fund processing for all fund types, e.g. order routing, cash management and position reporting
- Fund distribution support services for fund distributors and asset managers

Deutsche Börse Group: an overview



- As an international exchange organisation and innovative market infrastructure provider, Deutsche Börse Group offers its customers a wide range of products, services and technologies covering the entire value chain of financial markets.
- Its business areas include the provision of index and ESG data, analytics and research solutions, trading and clearing services for investment instruments, securities settlement and custody, collateral and liquidity management, and investment fund services. In addition, the Group develops state-of-the-art IT solutions and offers IT systems all over the world.


Continuous Improvement!
IS Assurance?

Set-up of Information Security Framework & Governance

Information Security Framework & Governance

2nd Line of Defense Deutsche Börse AG

Information Security Risk

Threat landscape, information security risk management, etc.

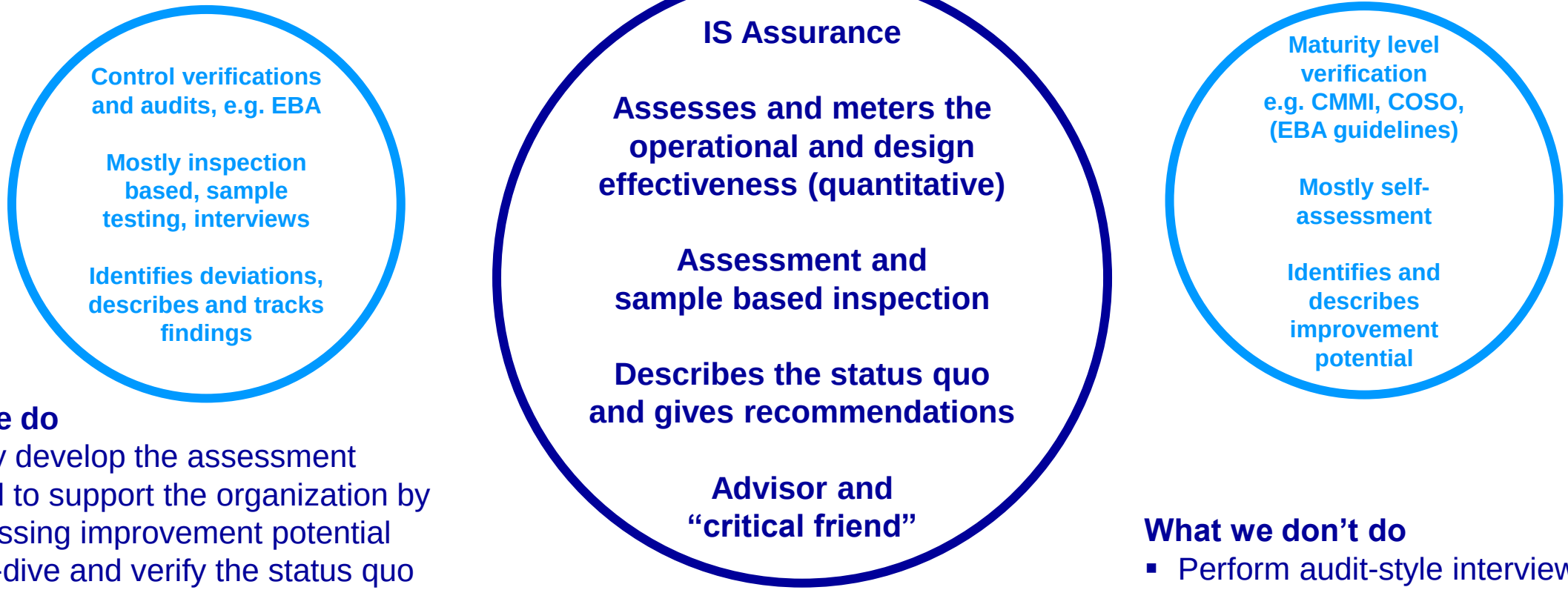
Information Security Governance

Management and development of the information security framework, staff awareness, etc.

Information Security Assurance

Verifying the design and operational effectiveness and implemented controls

Joint worlds: control and maturity verification



What we do

- Jointly develop the assessment
- Intend to support the organization by addressing improvement potential
- Deep-dive and verify the status quo
- Grade the effectiveness and give outlook with respect to a maturity level
- Describe recommendations for improvement

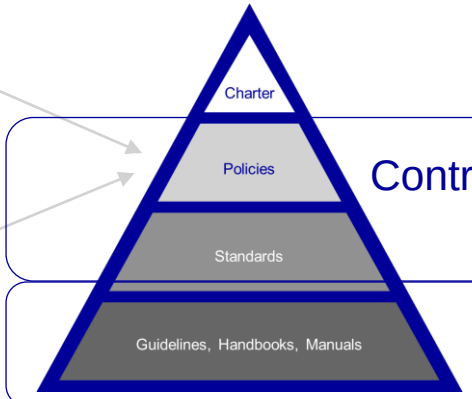
What we don't do

- Perform audit-style interviews
- Send out self-assessment questionaries
- Work in silos

Joint worlds: control and maturity verification

Information security objective(s) and requirements

Legal requirements e.g. BAIT, CSSF and standards e.g. ISO 2700x



Control objectives and requirements

Design and implementation

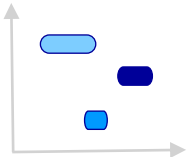
Security Process

IS Assurance
Verifying the adequacy and effectiveness of the related controls framework.

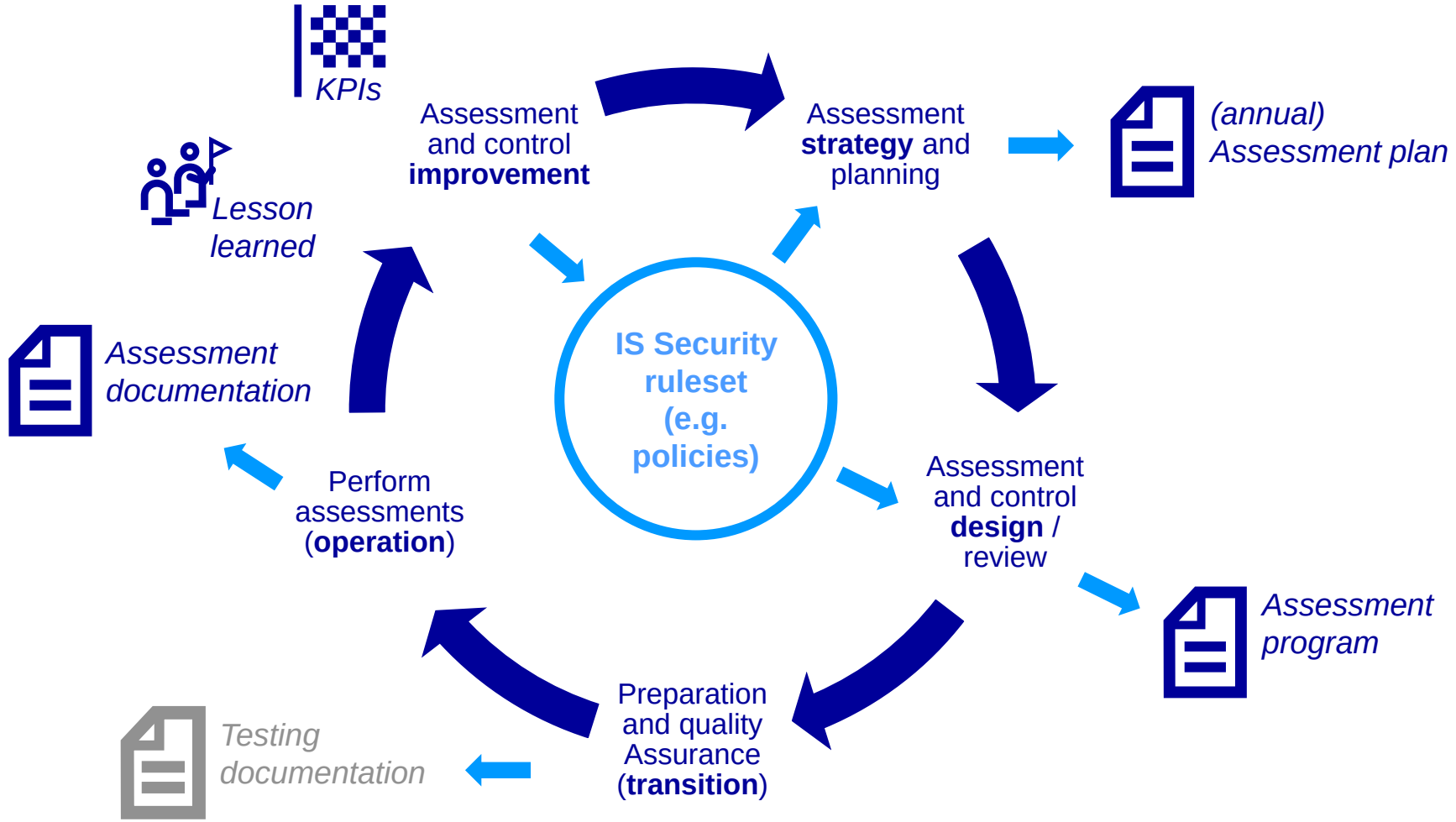
Verifying the maturity of the process (end to end).

Result of assessment

Document and grade on effectiveness (meeting the requirements) including grade the maturity (on business demand).



IS Assurance as a service (lifecycle)

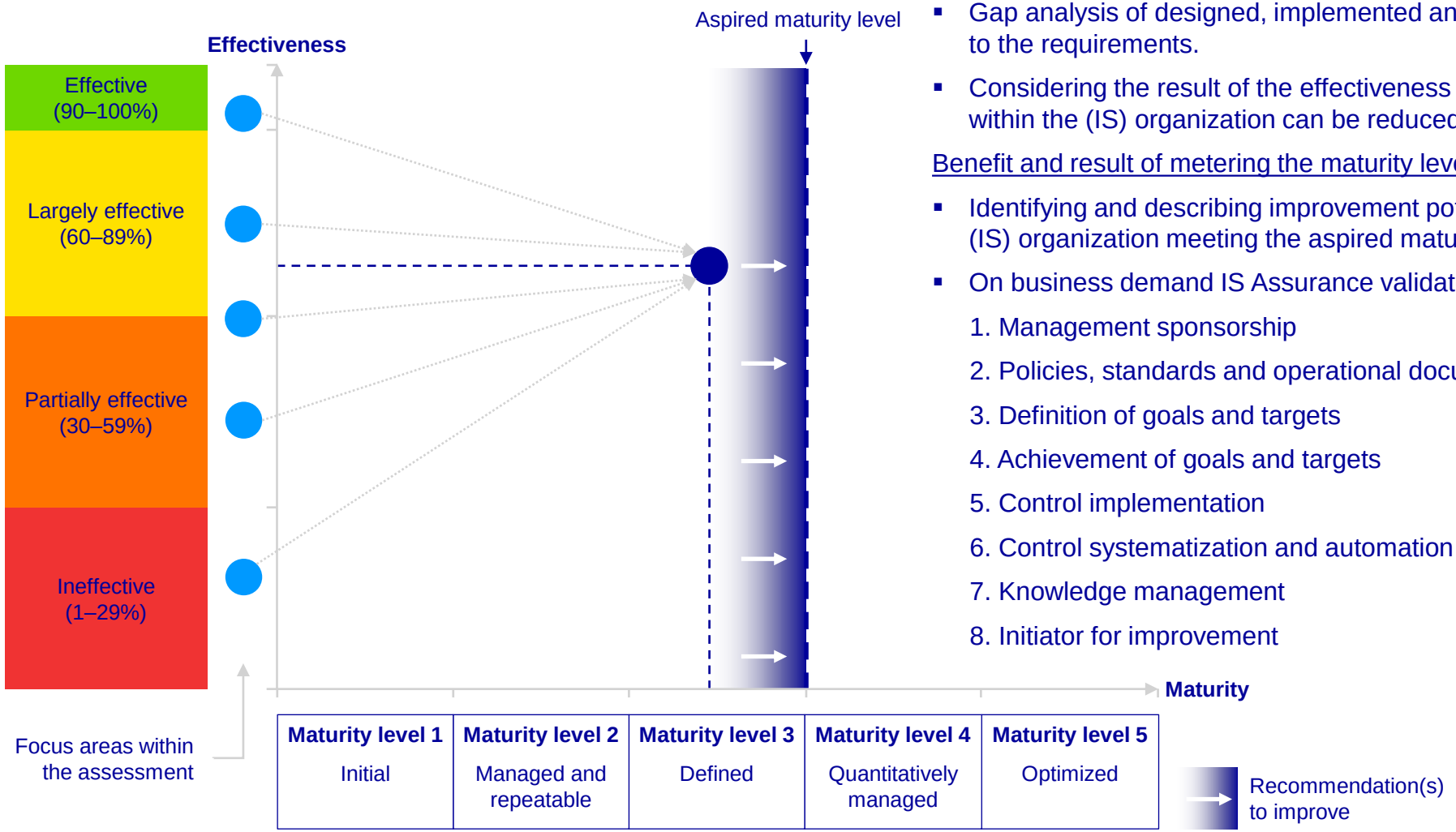


Grade the effectiveness

Metering the design and its implementation.

IS Assurance effectiveness grading	→ ref. “Cyber Resilience Oversight Expectations for Financial Market infrastructures” (European Central Bank) → ref. the expectation grading of Banque centrale du Luxembourg
Effective (90-100%)	The controls, processes or documentation respect and meet the expectation.
Largely effective (60-89%)	The controls, processes or documentation require minor improvement in some areas in order to fully respect and meet the expectation. Actions should be taken with a lower priority to fulfill expectations and to manage potential minor or moderate shortcomings.
Partially effective (30-59%)	The controls, processes or documentation are not fully in place nor consistent and require improvement. Actions should be taken with a medium priority to fulfill expectations and to manage potential minor, moderate or considerable shortcomings.
Ineffective (1-29%)	The controls, processes or documentation are not sufficient and require improvement. Actions should be take with a high priority to fulfill expectations and to manage potential minor, moderate, considerable and material shortcomings.

Effectiveness meets Maturity



Benefit of assessing the design and operational effectiveness:

- Gap analysis of designed, implemented and performed IS controls compared to the requirements.
- Considering the result of the effectiveness verification, the risk exposure within the (IS) organization can be reduced.

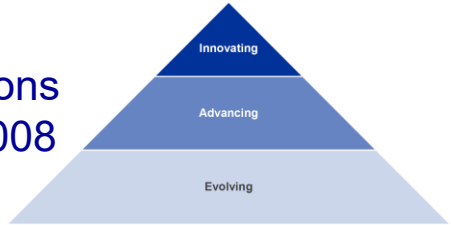
Benefit and result of metering the maturity level:

- Identifying and describing improvement potentials to support the (IS) organization meeting the aspired maturity level.
- On business demand IS Assurance validates the maturity of the focus areas:
  1. Management sponsorship
  2. Policies, standards and operational documents
  3. Definition of goals and targets
  4. Achievement of goals and targets
  5. Control implementation
  6. Control systematization and automation
  7. Knowledge management
  8. Initiator for improvement

Who meters maturity?

Is CMMI really an industry-proof method?

ECB, ”Cyber resilience oversight expectations for financial market infrastructures”, Dec 2008



How does the Digital Maturity Model enable digital transformation?

We understand that digital transformation is a journey involving a complex ecosystem of capabilities. The DMM can be used in each phase of transformation to help identify where there are gaps, establish key areas to focus on, and where to start.

It does not replace an overarching transformation framework, but is meant to serve as a guide and tool to be referred to throughout the process.

Which levels does the maturity model contain?

Maturity levels

The KPMG Blockchain Maturity model is based upon the Capability Maturity Model (CMMI) for IT maturity. CMMI is a model owned by ISACA, the international professional body for IT governance. The CMMI uses five maturity levels to measure maturity, ranging from 1 (processes unpredictable, poorly controlled; lowest level) to 5 (focus on process improvement; highest level). The scale is further explained in the figure on the right. Based on the CMMI scale you can easily define your ambition level for blockchain maturity.

Scoring

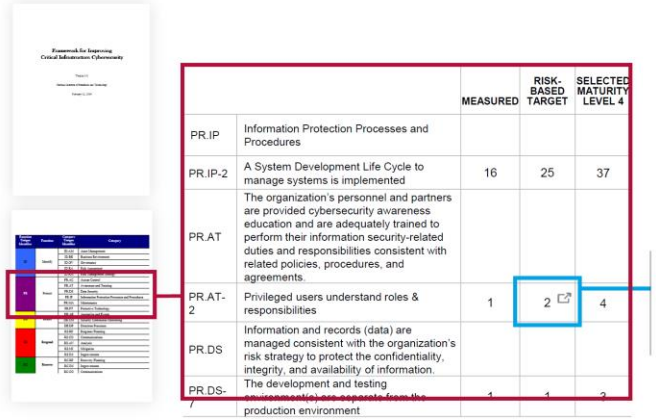
KPMG scores each blockchain risk area against the CMMI maturity model resulting in a maturity score per risk area. This helps you to identify which risk areas are below your desired maturity level. KPMG provides specific recommendations to improve the maturity level and help you get your blockchain Proof-of-Concept to production level from an IT governance perspective.

KPMG

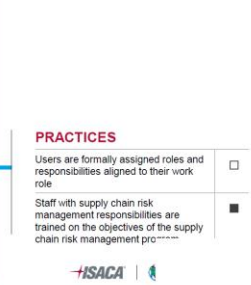
NIST CYBERSECURITY ALIGNMENT BY PRACTICE AREA

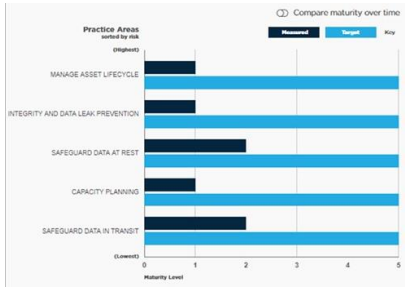
FILTERED RESULTS

NIST Cybersecurity Framework



		MEASURED	RISK-BASED TARGET	SELECTED MATURITY LEVEL 4
PR.IP	Information Protection Processes and Procedures			
PR.IP-2	A System Development Life Cycle to manage systems is implemented	16	25	37
PR.AT	The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.			
PR.AT-2	Privileged users understand roles & responsibilities	1	2	4
PR.DS	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.			
PR.DS-7	The development and testing environment(s) are separate from the production environment	1	1	2





Lessons learned

1	**First think – then act!**	Outline what is relevant to you and your company. How do you see yourself as an assurance function? Audit? Self assessment? Advisor?
2	**Describe your methodology**	Define and set your methodology, criteria and definitions. Clear. Understandable. As precise as possible.
3	**Get buy-in**	Collaborate with stakeholders and critical friends. Identify supporters to perform a showcase assessment.
4	**Communicate**	Demonstrate and present the value of your outcome. Communicate and explain what and how you perform assessments. Be transparent.
5	**Improve**	After implementing the methodology and performing some assessments: challenge your status quo and your deliverables. What worked? What went wrong? What should be improved? … and → go back to 1.


Highly rated:
True passion
for coding.
Share value
Thank you!
… and: apply now – positions are open!

Contact

Frank Ackermann
Lead Information Security (IS) Assurance

Deutsche Börse AG
Mergenthalerallee 61
65760 Eschborn

E-mail
Frank.Ackermann @ deutsche-boerse.com

- Longstanding experience in cyber security (in various DAX companies and industry sectors)
- Held diverse expert and lead functions in all three Lines of Defense
- Willingly challenged the status quo to improve the respective security organizations
- Credo: security is not my job – it is my passion.
- With Deutsche Börse Group since August 2020

DEUTSCHE BÖRSE
GROUP

Disclaimer

Deutsche Börse AG (DBAG), Clearstream Banking AG (Clearstream), Eurex Frankfurt AG, Eurex Clearing AG (Eurex Clearing) and Eurex Repo GmbH (Eurex Repo) are corporate entities and are registered under German law. Eurex Global Derivatives AG is a corporate entity and is registered under Swiss law. Clearstream Banking S.A. is a corporate entity and is registered under Luxembourg law. Deutsche Boerse Asia Holding Pte. Ltd., Eurex Clearing Asia Pte. Ltd. and Eurex Exchange Asia Pte. Ltd are corporate entities and are registered under Singapore law. Eurex Frankfurt AG (Eurex) is the administrating and operating institution of Eurex Deutschland. Eurex Deutschland is in the following referred to as the "Eurex Exchange".

All intellectual property, proprietary and other rights and interests in this publication and the subject matter hereof (other than certain trademarks and service marks listed below) are owned by DBAG and its affiliates and subsidiaries including, without limitation, all patent, registered design, copyright, trademark and service mark rights. While reasonable care has been taken in the preparation of this publication to provide details that are accurate and not misleading at the time of publication DBAG, Clearstream, Eurex, Eurex Clearing, Eurex Repo as well as the Eurex Exchange and their respective servants and agents (a) do not make any representations or warranties regarding the information contained herein, whether express or implied, including without limitation any implied warranty of merchantability or fitness for a particular purpose or any warranty with respect to the accuracy, correctness, quality, completeness or timeliness of such information, and (b) shall not be responsible or liable for any third party's use of any information contained herein under any circumstances, including, without limitation, in connection with actual trading or otherwise or for any errors or omissions contained in this publication.

This publication is published for information purposes only and shall not constitute investment advice respectively does not constitute an offer, solicitation or recommendation to acquire or dispose of any investment or to engage in any other transaction. This publication is not intended for solicitation purposes but only for use as general information.
All descriptions, examples and calculations contained in this publication are for illustrative purposes only.

Eurex and Eurex Clearing offer services directly to members of the Eurex Exchange respectively to clearing members of Eurex Clearing. Those who desire to trade any products available on the Eurex market or who desire to offer and sell any such products to others or who desire to possess a clearing license of Eurex Clearing in order to participate in the clearing process provided by Eurex Clearing, should consider legal and regulatory requirements of those jurisdictions relevant to them, as well as the risks associated with such products, before doing so.

Only Eurex derivatives that are CFTC-approved may be traded via direct access in the United States or by United States persons. A complete, up-to-date list of Eurex derivatives that are CFTC-approved is available at: http://www.eurexchange.com/exchange-en/products/eurex-derivatives-us. In addition, Eurex representatives and participants may familiarise U.S. Qualified Institutional Buyers (QIBs) and broker-dealers with certain eligible Eurex equity options and equity index options pursuant to the terms of the SEC's July 1, 2013 Class No-Action Relief.
A complete, up-to-date list of Eurex options that are eligible under the SEC Class No-Action Relief is available at: http://www.eurexchange.com/exchange-en/products/eurex-derivatives-us/eurex-options-in-the-us-for-eligible-customers... Lastly, U.S. QIBs and broker-dealers trading on behalf of QIBs may trade certain single-security futures and narrow-based security index futures subject to terms and conditions of the SEC's Exchange Act Release No. 60,194 (June 30, 2009), 74 Fed. Reg. 32,200 (July 7, 2009) and the CFTC's Division of Clearing and Intermediary Oversight Advisory Concerning the Offer and Sale of Foreign Security Futures Products to Customers Located in the United States
(June 8, 2010).

Trademarks and Service Marks

Buxl®, DAX®, DivDAX®, eb.rexx®, Eurex®, Eurex Repo®, Eurex Strategy WizardSM, Euro GC Pooling®, FDAX®, FWB®, GC Pooling®,,GCPI®, MDAX®, ODAX®, SDAX®, TecDAX®, USD GC Pooling®, VDAX®, VDAX-NEW® and Xetra® are registered trademarks of DBAG. All MSCI indexes are service marks and the exclusive property of MSCI Barra. ATX®, ATX® five, CECE® and RDX® are registered trademarks of Vienna Stock Exchange AG. IPD® UK Quarterly Indexes are registered trademarks of Investment Property Databank Ltd. IPD and have been licensed for the use by Eurex for derivatives. SLI®, SMI® and SMIM® are registered trademarks of SIX Swiss Exchange AG. The STOXX® indexes, the data included therein and the trademarks used in the index names are the intellectual property of STOXX Limited and/or its licensors Eurex derivatives based on the STOXX® indexes are in no way sponsored, endorsed, sold or promoted by STOXX and its licensors and neither STOXX nor its licensors shall have any liability with respect thereto. Bloomberg Commodity IndexSM and any related sub-indexes are service marks of Bloomberg L.P. PCS® and Property Claim Services® are registered trademarks of ISO Services, Inc. Korea Exchange, KRX, KOSPI
and KOSPI 200 are registered trademarks of Korea Exchange Inc. BSE and SENSEX are trademarks/service marks of Bombay Stock Exchange (BSE) and all rights accruing from the same, statutory or otherwise, wholly vest with BSE. Any violation of the above would constitute an offence under the laws of India and international treaties governing the same.
The names of other companies and third party products may be trademarks or service marks of their respective owners.

Eurex Deutschland qualifies as manufacturer of packaged retail and insurance-based investment products (PRIIPs) under Regulation (EU) No 1286/2014 on key information documents for packaged retail and insurance-based investment products (PRIIPs Regulation), and provides key information documents (KIDs) covering PRIIPs traded on Eurex Deutschland on its website under the following link: http://www.eurexchange.com/exchange-en/resources/regulations/eu-regulations/priips-kids.

In addition, according to Art. 14(1) PRIIPs Regulation the person advising on, or selling, a PRIIP shall provide the KID to retail investors free of charge.