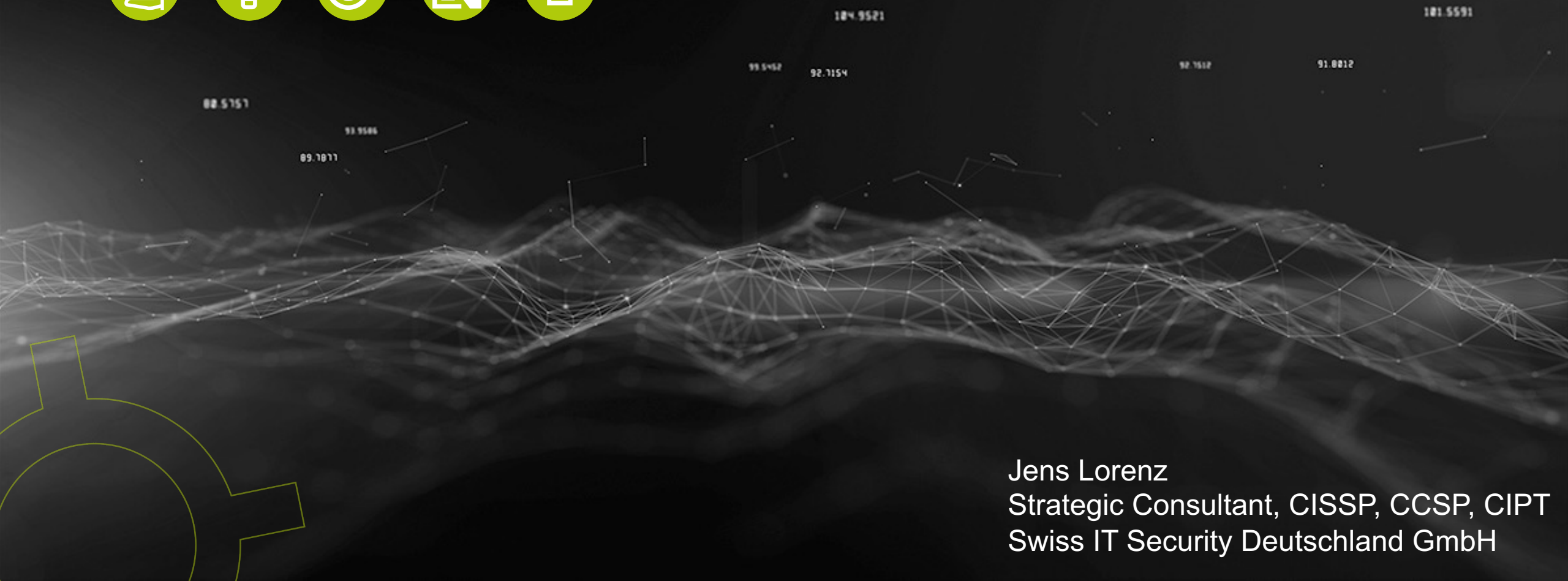
Compliance mit IT





Jens Lorenz
Strategic Consultant, CISSP, CCSP, CIPT
Swiss IT Security Deutschland GmbH

Die Situation der IT heute

(EU) 2016/943
GeschGehG

EU-DSGVO
BDSG-neu

ISO 31000
ISO/IEC 27005

CIS

FSIA sec. 701

ITAR

CLOUD-Act

Grundschutzkatalog
C5

§203 StGB

TISAX

PCI-DSS

Directive (EU) 2015/2366
PSD2

FDA

HIPAA

(EU) 2017/1148
KRITIS-V

COBIT

CSA

China

GoBD

APAC

ISO /IEC 27017

KWG
BAIT
MaRisk

VAG
VAIT
MaGo

KAGG
KAIT
KaMaRisk

ISO/IEC 27001
ISO/IEC 27701

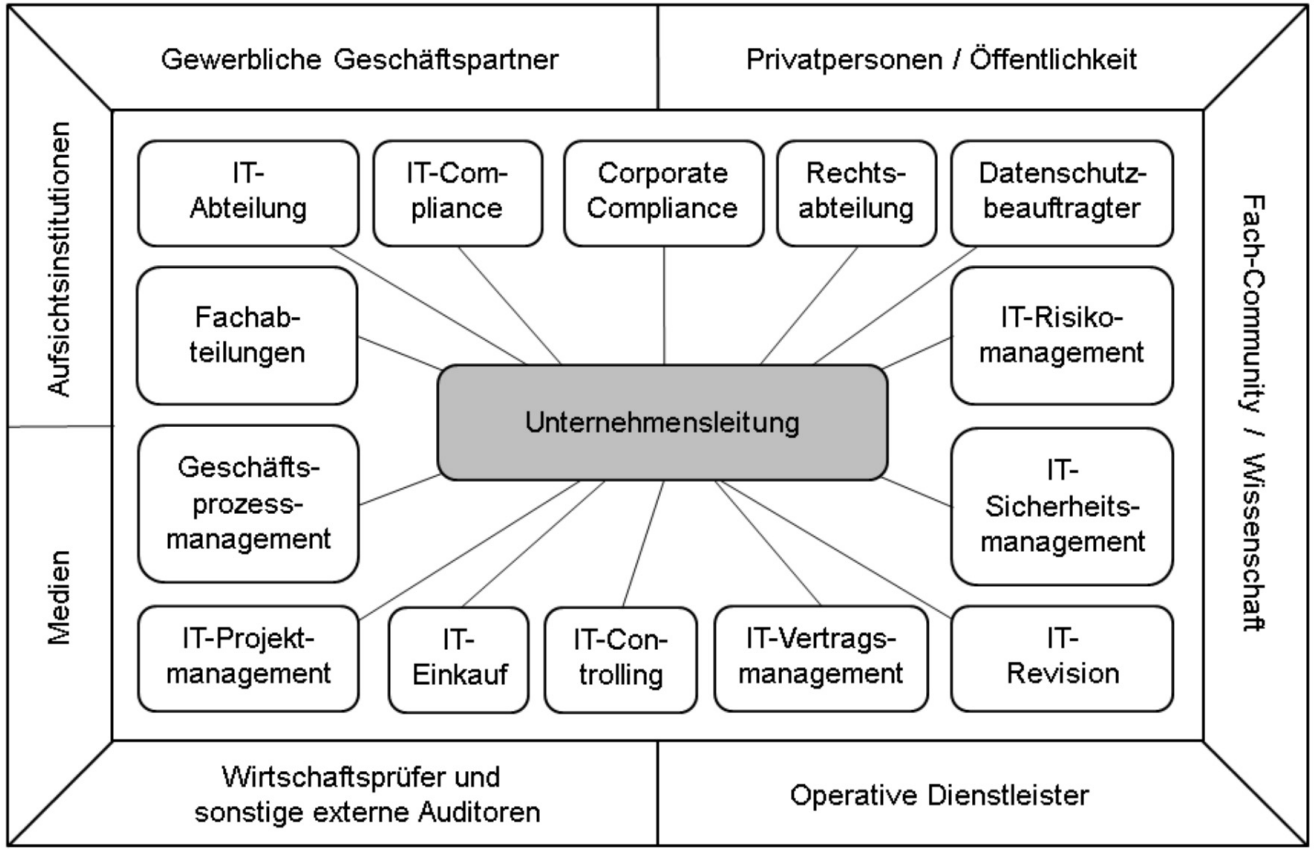
ISO 22301

Russland

ISO 29134

Die Rolle der IT im Unternehmen

IT-Ziele leiten sich aus Unternehmenszielen ab, interne und externe Interessensvertreter (Stakeholder) beeinflussen IT-Compliance.



Quelle: ISACA (Leitfaden IT-Compliance)

Das Spannungsfeld



Risiko als gemeinsame Sprache

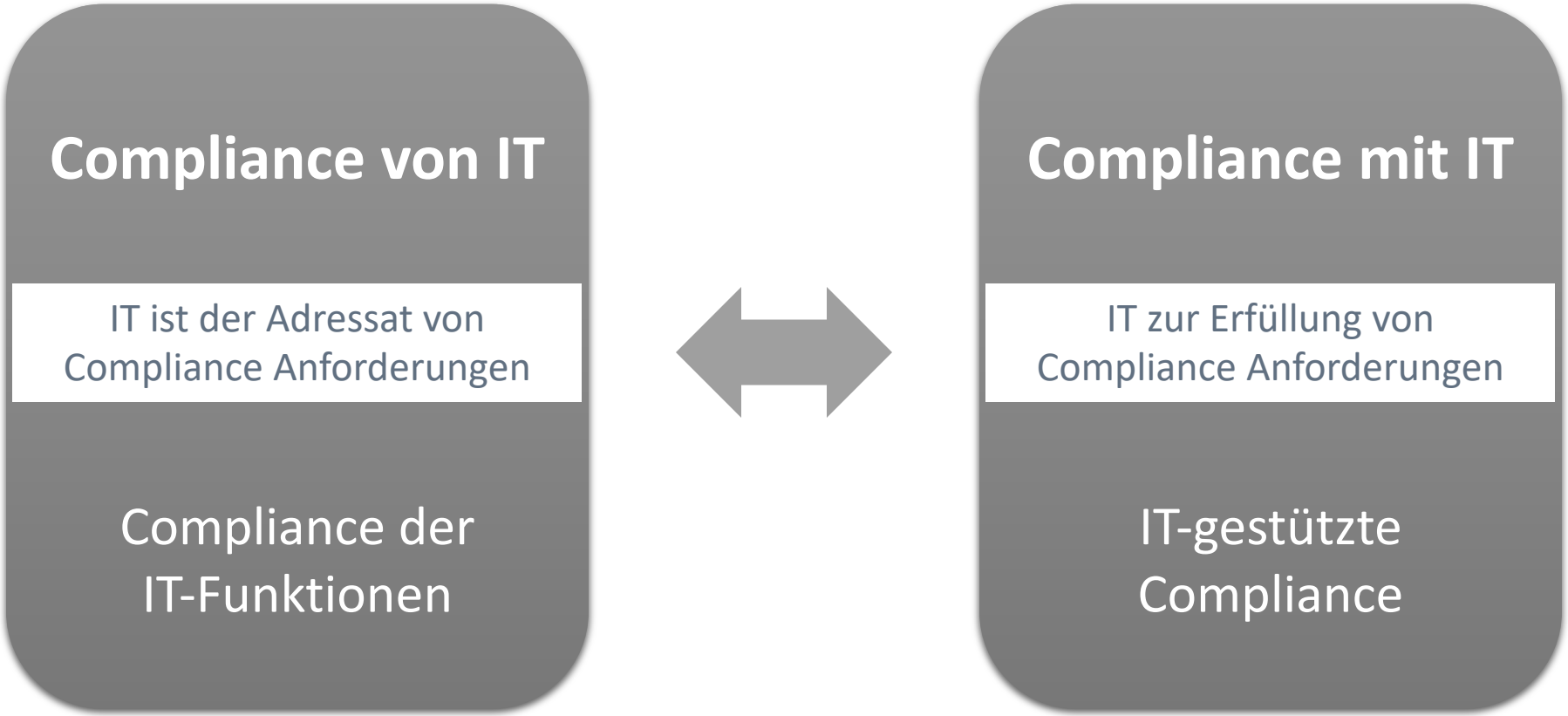
“Effekt von Ungewissheit auf Ziele”

ISO 31000:2018 - Terms and definitions 3.1: **risk**
“effect of uncertainty on objectives”

VUCA-World

Volatile	**V**ision
Uncertain	**U**nderstanding
Complex	**C**larity
Ambiguous	**A**gility

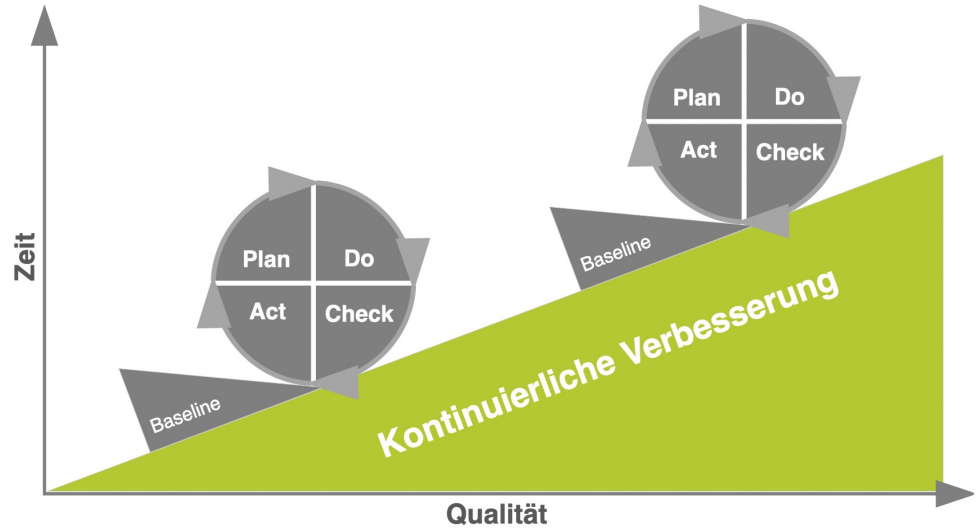
IT und IT-Compliance



Posture Management

Das Prinzip der kontinuierlichen Verbesserung

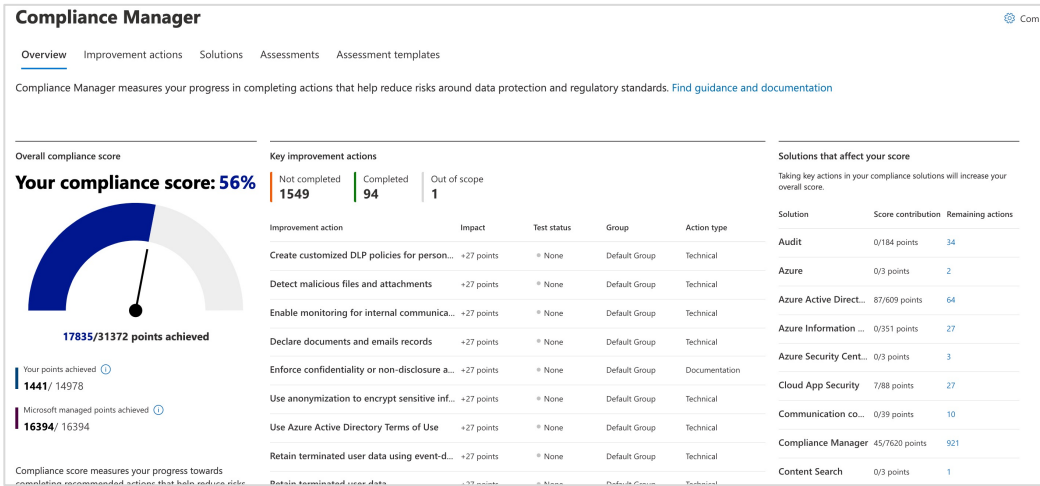
- Kontinuierliche Änderungen erfordern kontinuierliche Anpassungen
  - Durchschnittlich mehr als 200 Änderungen in internationalen Regulierungen täglich!
- Kontinuierliche Verbesserung als Prozess im Unternehmen
  - Kontinuierlicher Dialog aller Interessenvertreter erforderlich



Compliance Posture Management

Microsoft Compliance Manager

- „Universeller Übersetzer“ zwischen Compliance und IT
  - Ständig aktualisierte Informationen und Empfehlungen zu technischen- und organisatorischen Maßnahmen für Compliance mit Microsoft 365
  - Universelle Vorlagen für Drittanbieter und interne Systeme
  - Aktuell Unterstützung von 24 Sprachen
- Kontinuierliche Bewertung mit dem Compliance Score
  - Microsoft 365 Data Protection Baseline als initialer Basis-Score

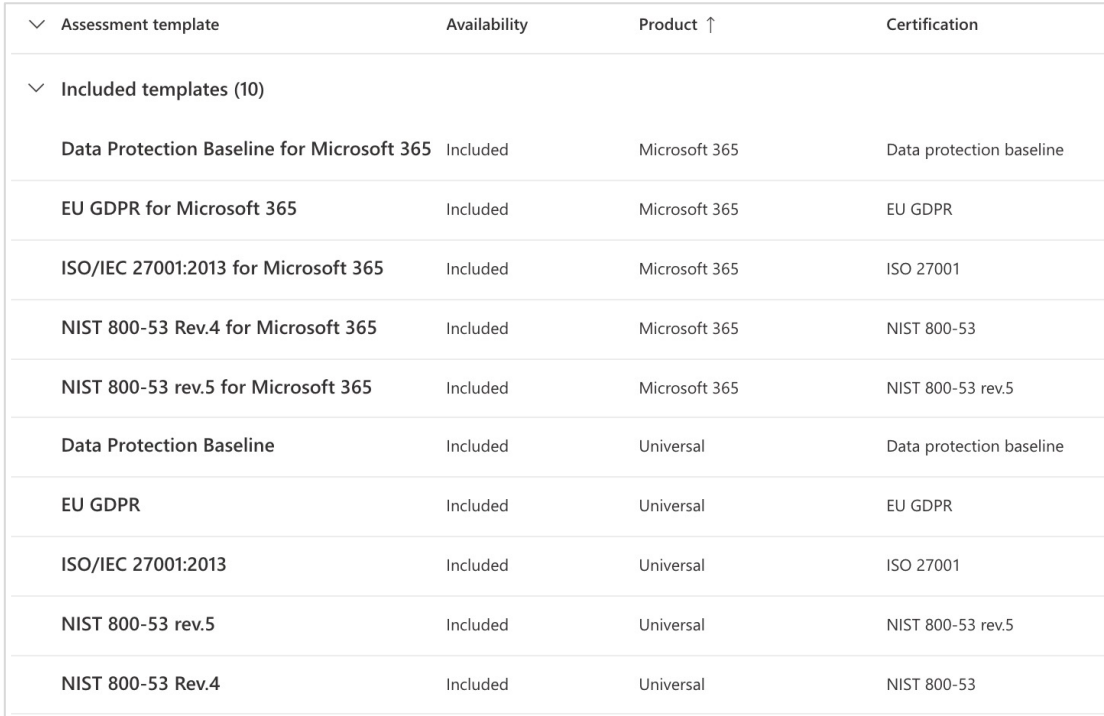


https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager

Microsoft Compliance Manager

Vorlagen für verschiedene Compliance Standards

- Office 365 E1/E3 und Microsoft 365 E3: Microsoft Data Protection Baseline
- Office 365 E5 und Microsoft 365 E5: EU GDPR, ISO/IEC 27001, NIST 800-53 und die Data Protection Baseline
- Jeweils als Microsoft 365 Assessment und als Universal Template



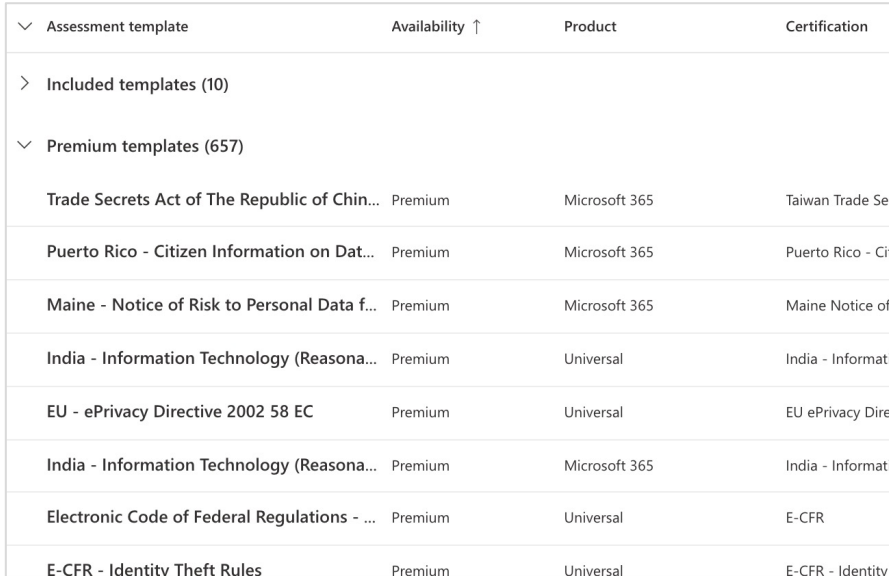
Assessment template	Availability	Product ↑	Certification
Included templates (10)			
Data Protection Baseline for Microsoft 365	Included	Microsoft 365	Data protection baseline
EU GDPR for Microsoft 365	Included	Microsoft 365	EU GDPR
ISO/IEC 27001:2013 for Microsoft 365	Included	Microsoft 365	ISO 27001
NIST 800-53 Rev.4 for Microsoft 365	Included	Microsoft 365	NIST 800-53
NIST 800-53 rev.5 for Microsoft 365	Included	Microsoft 365	NIST 800-53 rev.5
Data Protection Baseline	Included	Universal	Data protection baseline
EU GDPR	Included	Universal	EU GDPR
ISO/IEC 27001:2013	Included	Universal	ISO 27001
NIST 800-53 rev.5	Included	Universal	NIST 800-53 rev.5
NIST 800-53 Rev.4	Included	Universal	NIST 800-53

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-list

Microsoft Compliance Manager

Vorlagen für verschiedene Compliance Standards

- Premium Vorlagen mit jährlicher Laufzeit
  - Aktuell 335+ Vorlagen (Microsoft 365 plus Universal)
  - Vorlagen für Internationale Standards und Regularien, z.B.
    - Kriterienkatalog Cloud Computing C5
    - Bundesdatenschutzgesetz
    - COBIT 5
    - CIS Implementation Groups 1-3
    - CIS M365 Foundation Level 1 / Level 2
    - BAIT (Supervisory Requirements for IT in Financial Institutions)
    - MaRisk (Annotated text of the Minimum Requirements for Risk Management)
    - ISO/IEC 27701:2019 (PIMS)
    - ISO 27005:2018
    - ISO 31000:2018
    - ISO 22301:2019
    - PCI DSS v3.2.1
    - TISAX 5.0



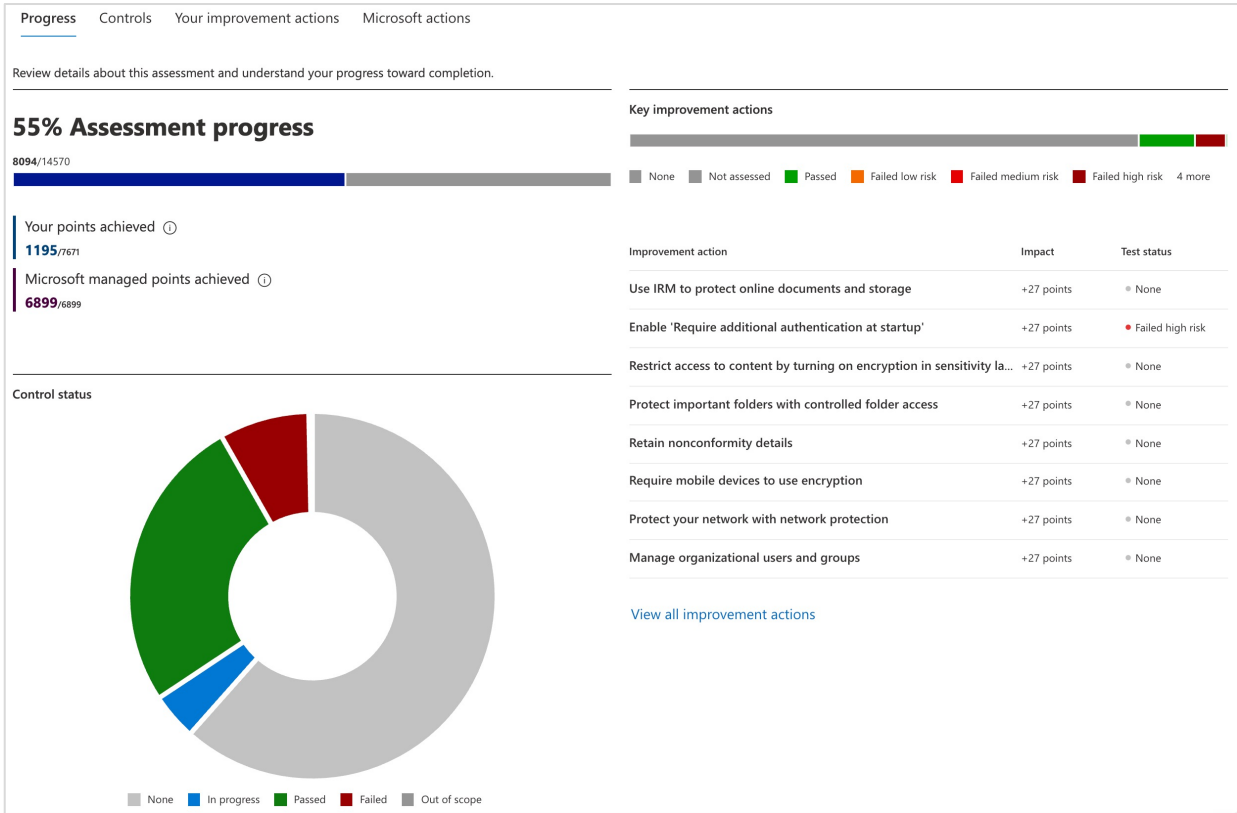
Assessment template	Availability	Product	Certification
Included templates (10)			
Premium templates (657)			
Trade Secrets Act of The Republic of Chin...	Premium	Microsoft 365	Taiwan Trade Se
Puerto Rico - Citizen Information on Dat...	Premium	Microsoft 365	Puerto Rico - Ci
Maine - Notice of Risk to Personal Data f...	Premium	Microsoft 365	Maine Notice of
India - Information Technology (Reasona...	Premium	Universal	India - Informat
EU - ePrivacy Directive 2002 58 EC	Premium	Universal	EU ePrivacy Dire
India - Information Technology (Reasona...	Premium	Microsoft 365	India - Informat
Electronic Code of Federal Regulations - ...	Premium	Universal	E-CFR
E-CFR - Identity Theft Rules	Premium	Universal	E-CFR - Identity

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-list

Microsoft Compliance Manager

Bewertungen und Control-Implementierung

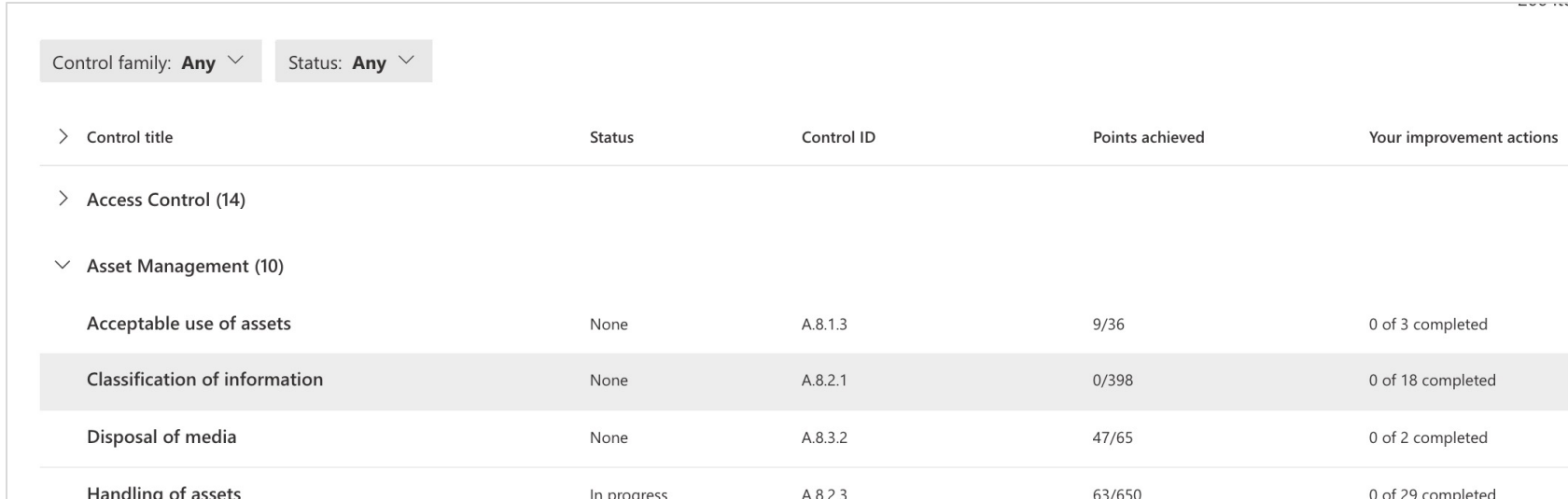
- Darstellung des Fortschritts in der Bewertung und Implementierung
- Empfehlungen zur Verbesserung (Improvement Actions)
- Informationen zur Implementierung



Microsoft Compliance Manager

Bewertungen und Control-Implementierung

- Beispiel: ISO/IEC 27001 – Annex-A Controls
  - Control Gruppen – Beispiel: Asset Management
    - Control – Beispiel: Classification of information (A.8.2.1)



Microsoft Compliance Manager

Bewertungen und Control-Implementierung

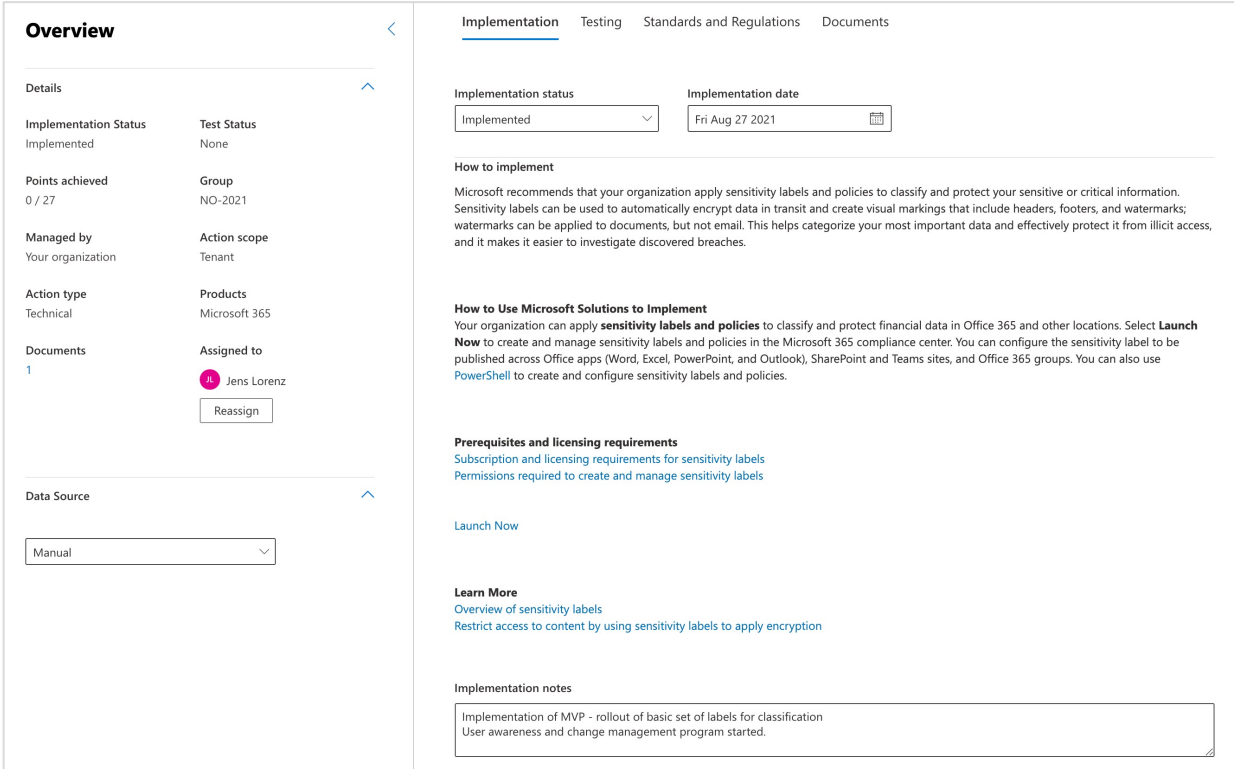
- Improvement Actions
  - Beispiel: Apply sensitivity labels to protect sensitive or critical data
  - Impact auf den Score (Points)
    - Bewertung (Risiko/Benefit)

Improvement action	Products	Test status	Impact	P
Categorize information	Microsoft 365	None	9	0
Review label activity and analytics	Microsoft 365	None	1	0
Classify assets into risk-based categories	Microsoft 365	None	1	0
Develop business classification schemes	Microsoft 365	None	9	0
Define a device value	Microsoft 365	None	27	0
Create service side labeling policies	Microsoft 365	None	27	0
Create customized or use built-in trainable classifiers	Microsoft 365	None	27	0
Apply sensitivity labels to protect ePHI	Microsoft 365	None	27	0
Apply sensitivity labels to protect financial data	Microsoft 365	None	27	0
Automatically apply Client Side Sensitivity Labels	Microsoft 365	None	27	0
Use sensitivity labels for container-level classification	Microsoft 365	None	27	0
Automatically apply record labels	Microsoft 365	None	27	0
Apply sensitivity labels to protect sensitive or critical data	Microsoft 365	None	27	0
Apply sensitivity labels to protect personal data	Microsoft 365	None	27	0
Automate protection of content in supported containers	Microsoft 365	None	27	0

Microsoft Compliance Manager

Bewertungen und Control-Implementierung

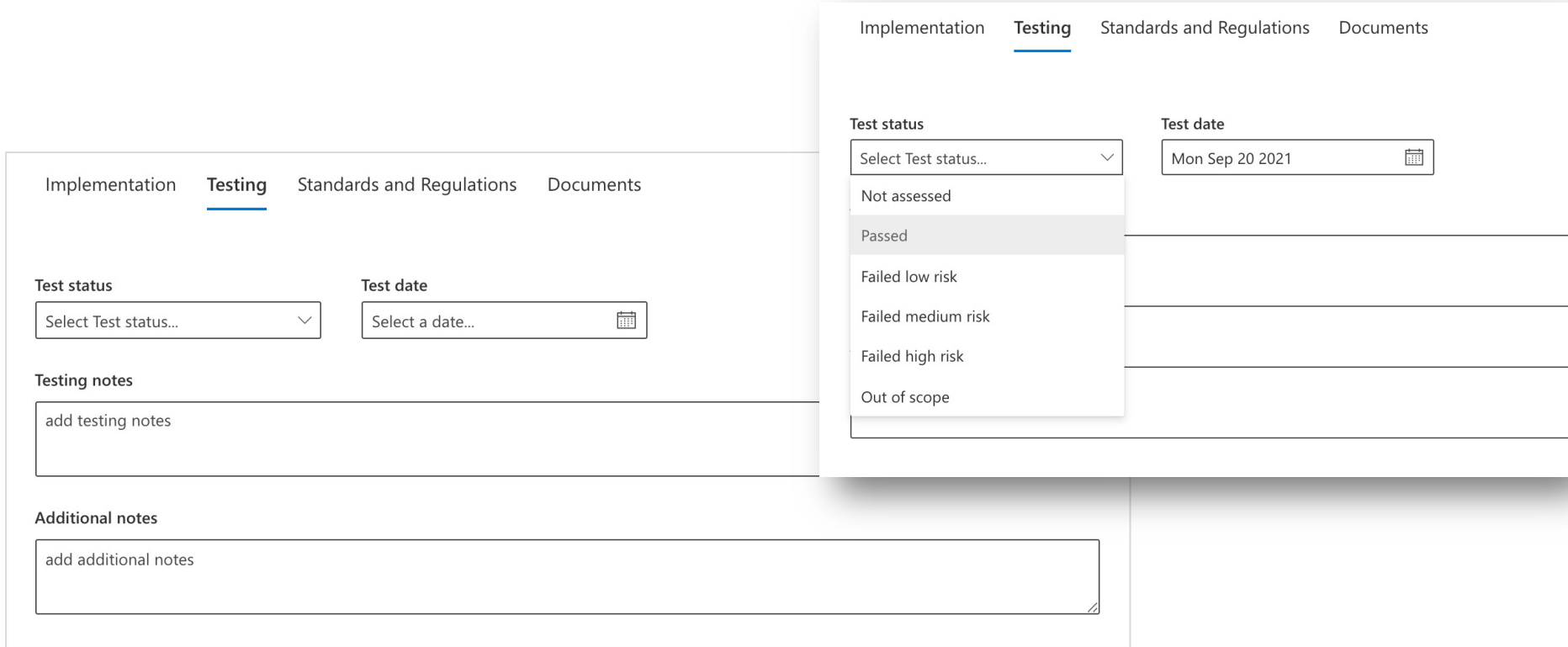
- Empfehlungen und Informationen zur Implementierung
- Workflows für Delegation und Nachverfolgung
  - Zuweisungen für Implementierung
  - Dokumentation
  - Status



Microsoft Compliance Manager

Bewertungen und Control-Implementierung

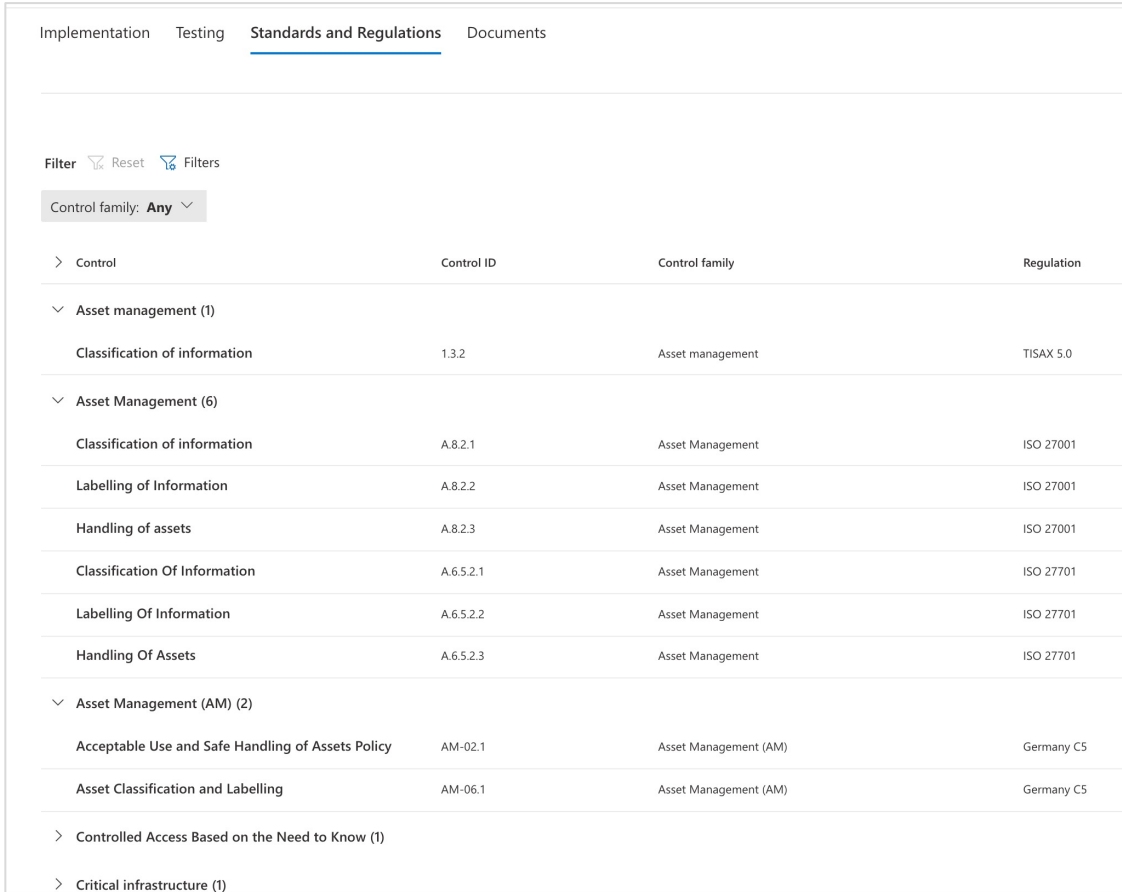
- Bewertung der Implementierung und interne Audits
  - Test-Status, Test-Datum, Anmerkungen und Notizen



Microsoft Compliance Manager

Bewertungen und Control-Implementierung

- Anwendbarkeit auf weitere Standards und Regularien
  - Informationen zu Anforderungen
  - Ergänzung des Umfangs der Implementierung



Microsoft Compliance Manager

Berechnung des Compliance Score

- Improvement Points basieren auf dem assoziierten Risiko

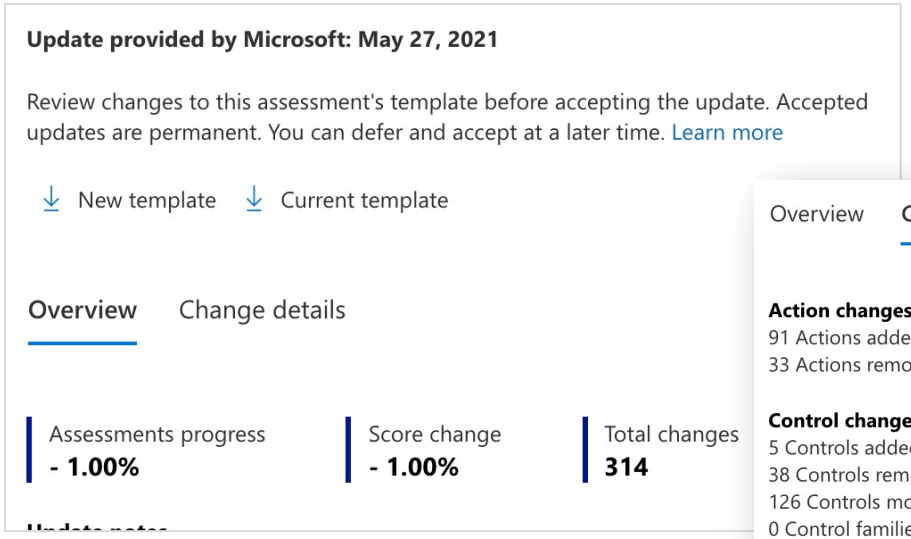


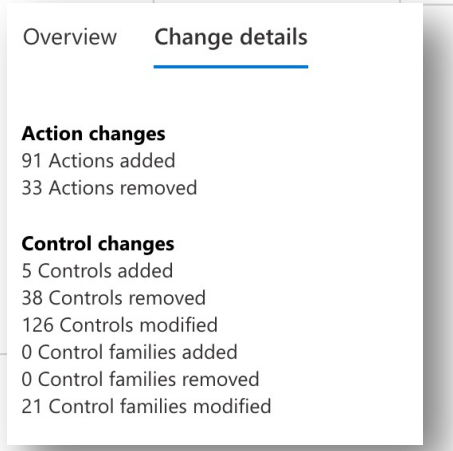
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-methodology

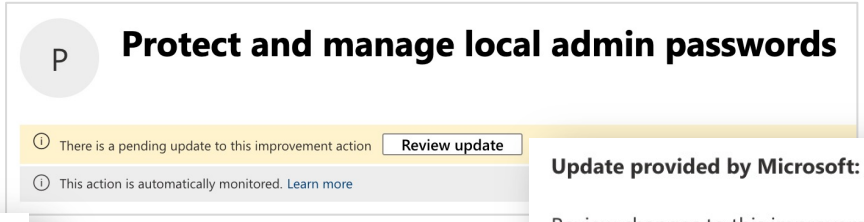
Microsoft Compliance Manager

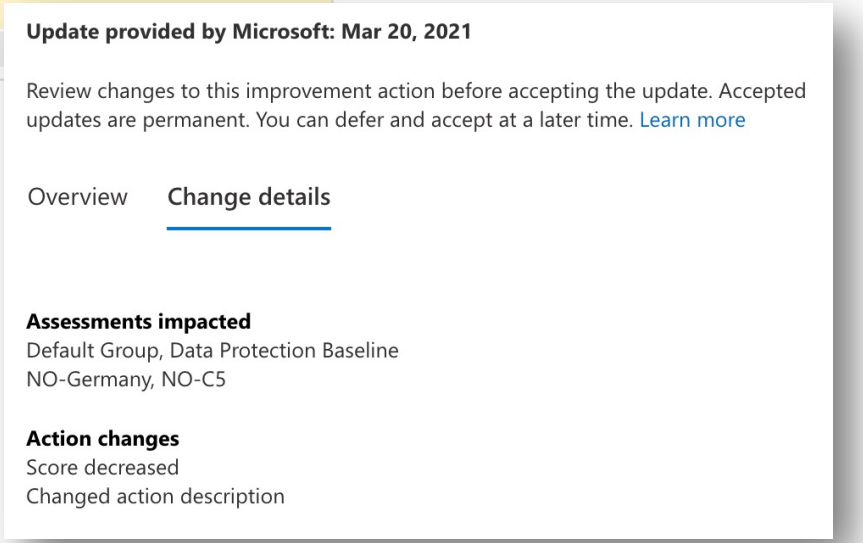
Kontinuierliche Verbesserung

- Kontinuierliche Aktualisierung der Vorlagen durch Microsoft
- Kontinuierliche Aktualisierung von Improvement Actions
  - Bewertungen und Implementierungs-Empfehlungen





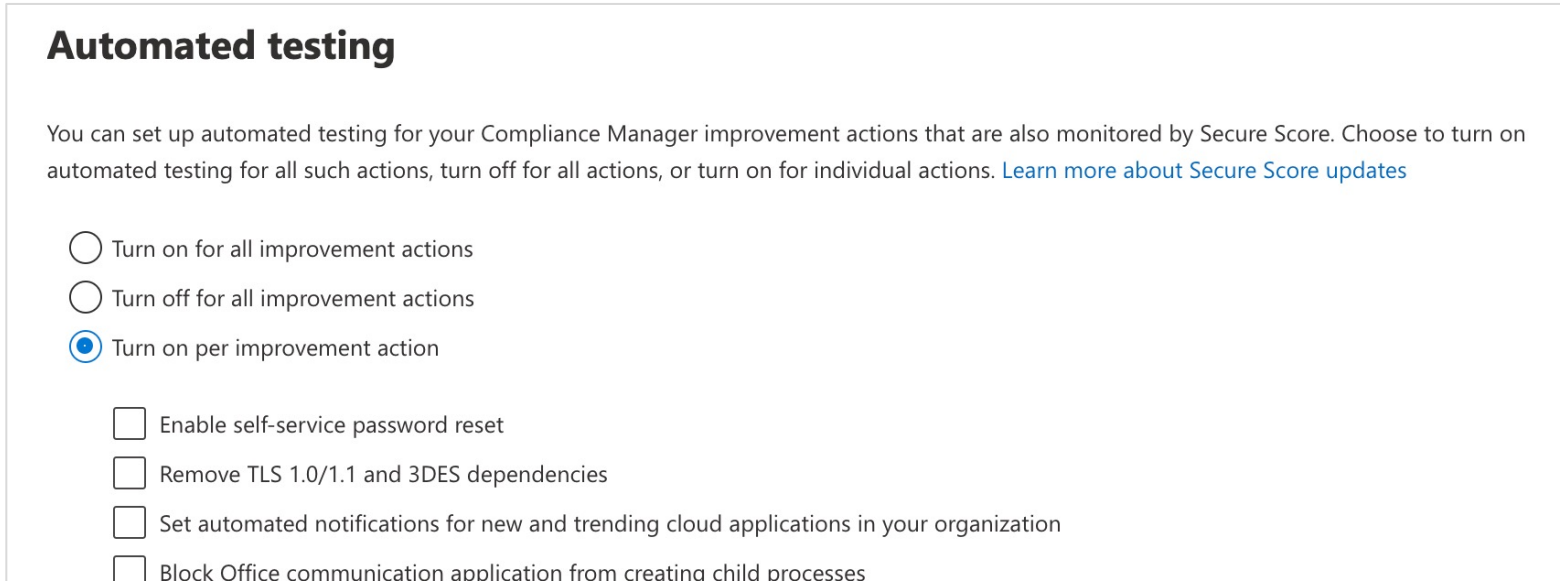




Microsoft Compliance Manager

Automatische Tests (Continuous Assessment)

- Technische Maßnahmen, die durch den Microsoft Secure Score überwacht werden, können automatisch getestet werden
  - Alle Improvement Actions oder spezifische Actions
  - Aktualisierung alle 24 Stunden



Webinar-Reihe „Compliance mit IT“

https://sits.group/sci

- Mittwoch, 24.9.2021: *Identity Governance & Administration (IGA) im Kontext Compliance* (Anmelden)
- Mittwoch, 27.10.2021: *Datenmanagement im Kontext Compliance* (Anmelden)
- Mittwoch, 24.11.2021: *Adressieren von Insider-Risiken* (Anmelden)

Jens Lorenz
Strategic Consultant, CISSP, CSSP, CIPT

mail: jens.lorenz@sits-d.de
fon: +49-170-4516565

LinkedIn: https://de.linkedin.com/in/jenslorenz