itSMF Bulgaria
The IT Service Management Forum

ITIL (Version 5) AI Governance

Use AI without losing control





Roman Zhuravlev

29 April 2026

ITIL®

Agenda

01 Introduction

02 The ITIL AI Governance assessment and implementation approach

03 Practical recommendations

04 Key takeaways

05 ITIL (Version 5) is here!

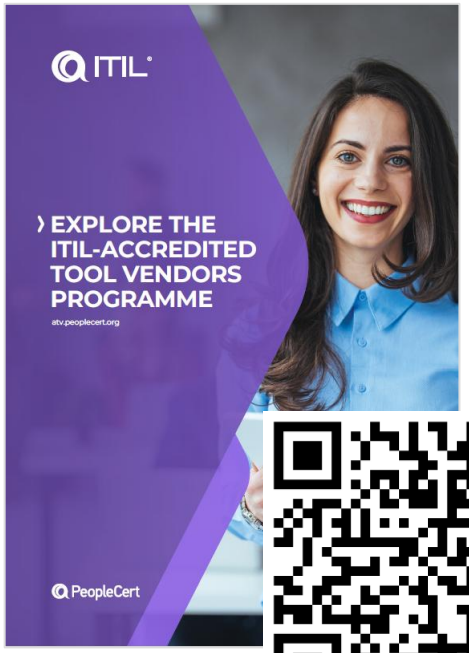
itSMF Bulgaria
The IT Service Management Forum

Introduction



ITIL®
by PeopleCert

ITIL and AI in 2025



The only official ITIL accreditation for tool vendors incorporating AI-based criteria



The AI in ITSM tools research conducted with Stephen Mann and 11 ATVs



The practical guide on effective AI governance for enterprises

And also webinars, thought-leadership content, and other materials available for PC+ members

The authoring team



James Finister



Dmitry Isaychenko



Kaimar Karu



Stephen Mann

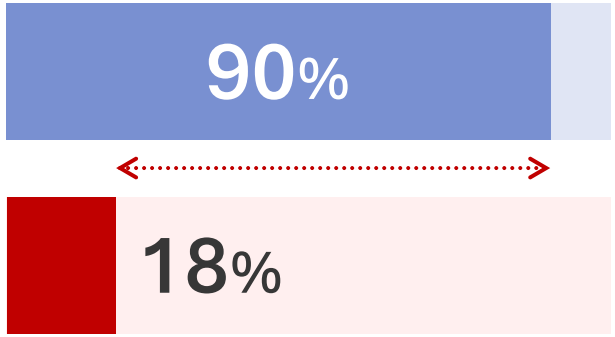


Simone Jo Moore



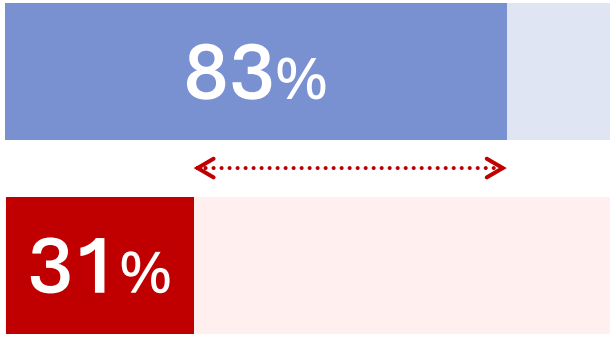
Roman Zhuravlev

AI governance is key



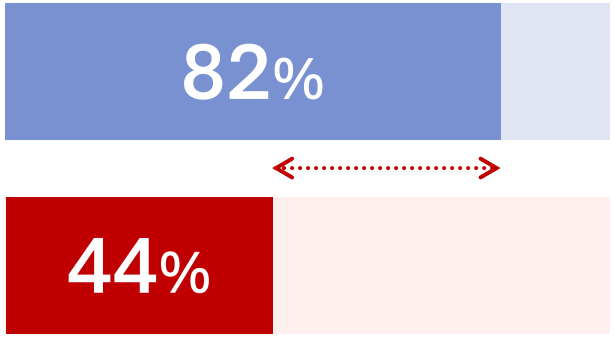
90% of organizations utilise AI in daily operations, only 18% have a fully implemented AI governance framework.

Legalfly: ‘The AI Governance Gap: 5 key findings’



83% of European businesses say staff are using AI, but only 31% have a comprehensive AI policy in place.

ISACA, 2025 “AI Use is outpacing policy and governance”



82% of organizations already use AI agents, but only 44% have policies in place to secure them.

SailPoint: ‘AI agents: The new attack surface…’

We adopt AI way faster than we learn how to effectively control it.

AI-specific challenges

AI governance perspective	AI-specific risks
Decision Authority & Risk Management	▪ Autonomy in decision-making ▪ Transparency and explainability
Ethical Principles & Responsible AI	▪ Bias and fairness risks ▪ Hallucination and mistakes in generated outputs
Data Governance & Performance Management	▪ Access control misalignment between source data and AI outputs ▪ Data availability and quality for AI training
Regulatory compliance & Operational standards	▪ Legal, regulatory, and compliance risks ▪ Extended supply chain and third-party AI governance risks ▪ Organizational readiness and skills ▪ Operational and lifecycle risks

Don’t assume your IT governance is AI-ready unless you test and prove it.

Before we jump to details…

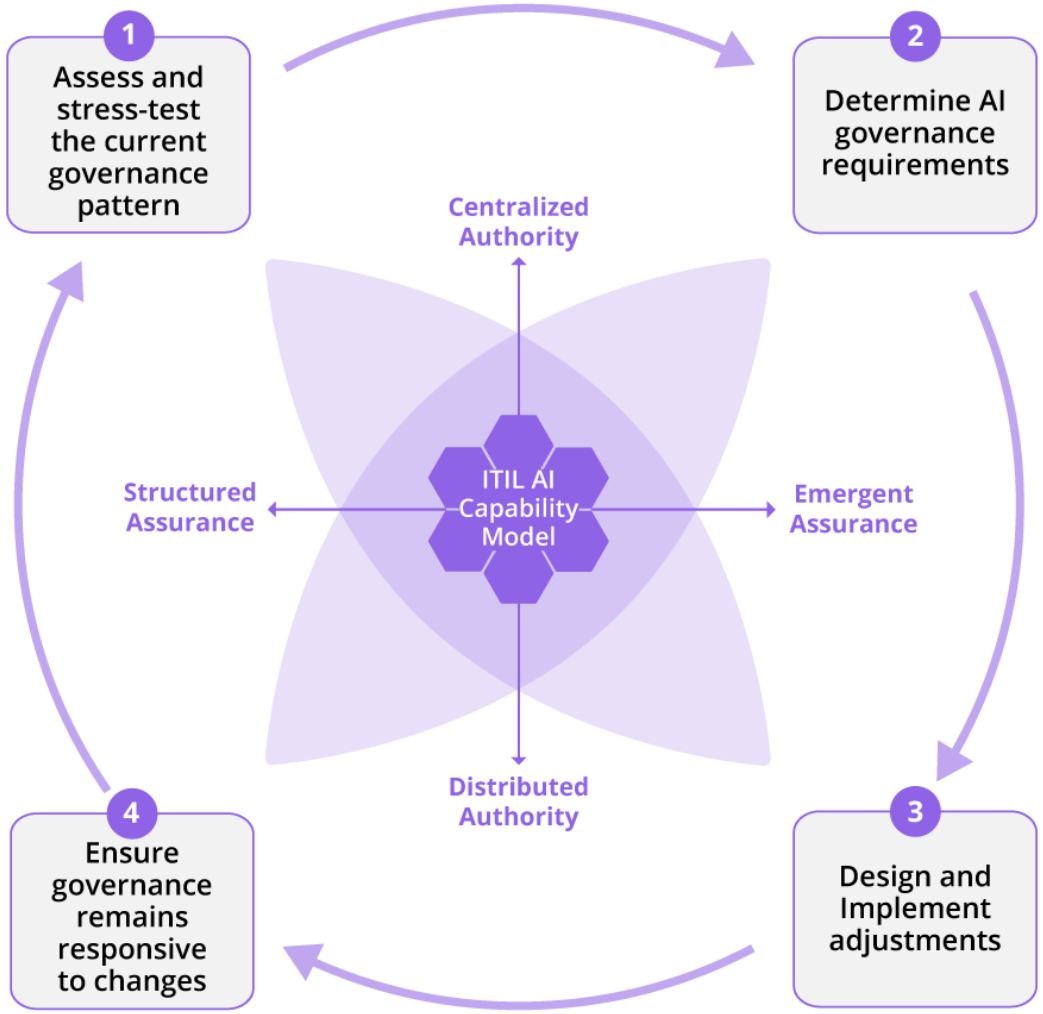
- Let's assume we have some IT governance system in place and need to adapt it to the challenges posed by AI
- If we were about to build the IT governance system from scratch, we could use:
  - ITIL Transformation (Version 5)
  - ISO/IEC 38500: Information technology – Governance of IT for the organization
  - ISO/IEC TS 38501: Information technology – Governance of IT for the organization – Implementation guide

How to embed AI oversight into existing IT governance



ITIL® by PeopleCert

How do we get there?



Step 1. Assessing and stress-testing

- Assess and stress-test the current governance system
- Determine AI governance requirements
- Design and implement governance adjustments
- Ensure governance remains responsive to changes

Objectives

- Understand the current governance pattern of your organization
- Evaluate how current governance frameworks hold up under AI-related stress and identify governance “breaking points”

Key Activities

- Assess current governance pattern to better understand and visualize your organization’s baseline
- Conduct stress-testing for the current governance against AI scenarios

Key Results

- A documented governance baseline
- Clear documentation of where and why current governance breaks

Step 1. Assessing and stress-testing

- Assess and stress-test the current governance system
- Determine AI governance requirements
- Design and implement governance adjustments
- Ensure governance remains responsive to changes

Objectives

- Understand the current governance pattern of your organization
- Evaluate how current governance frameworks hold up under AI-related stress and identify governance “breaking points”

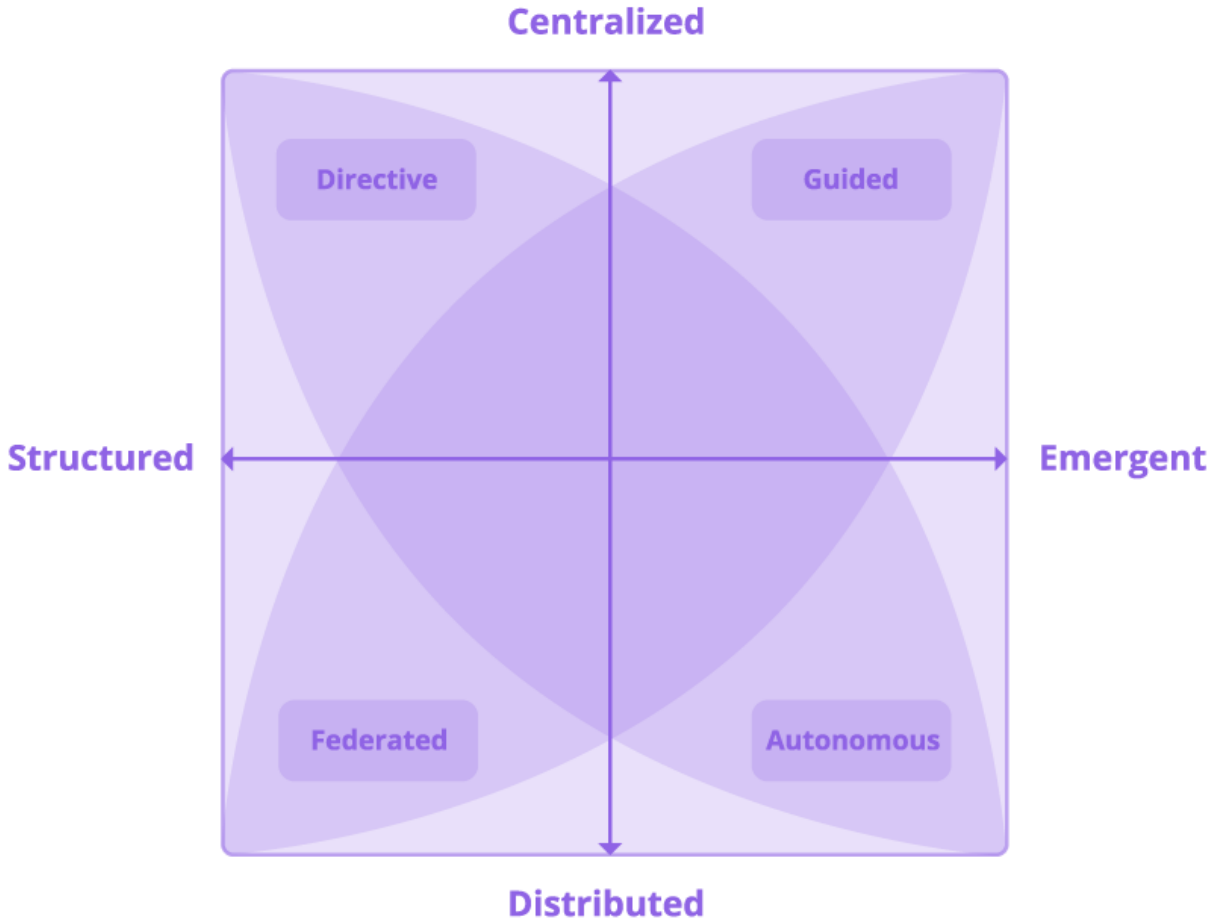
Key Activities

- **Assess current governance pattern to better understand and visualize your organization’s baseline**
- Conduct stress-testing for the current governance against AI scenarios

Key Results

- A documented governance baseline
- Clear documentation of where and why current governance breaks

Common governance patterns



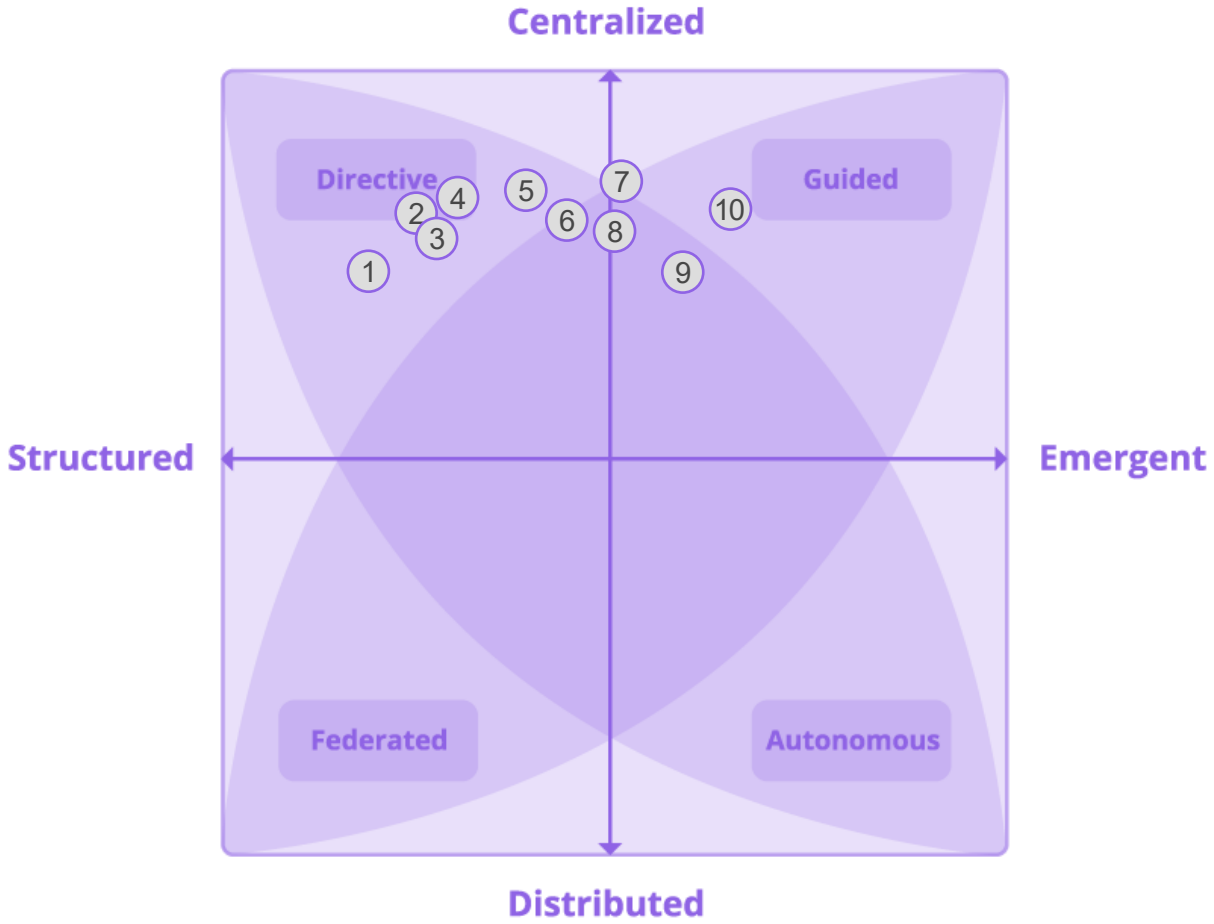
Directive: top-down control through formal hierarchies, strict procedures, and standardized processes

Guided: central vision and strategic direction with local freedom in execution and implementation

Federated: multiple distributed units with delegated authority coordinated through formal structures

Autonomous: self-organizing teams making decisions through peer collaboration and influence

Assessing governance patterns



1. Approach to change
2. Success metrics
3. Integration requirements
4. Risk tolerance
5. Environmental stability
6. Decision velocity
7. Compliance requirements
8. Stakeholder diversity
9. Governance scope
10. Governance capabilities

Step 1. Assessing and stress-testing

- Assess and stress-test the current governance system
- Determine AI governance requirements
- Design and implement governance adjustments
- Ensure governance remains responsive to changes

Objectives

- Understand the current governance pattern of your organization
- Evaluate how current governance frameworks hold up under AI-related stress and identify governance “breaking points”

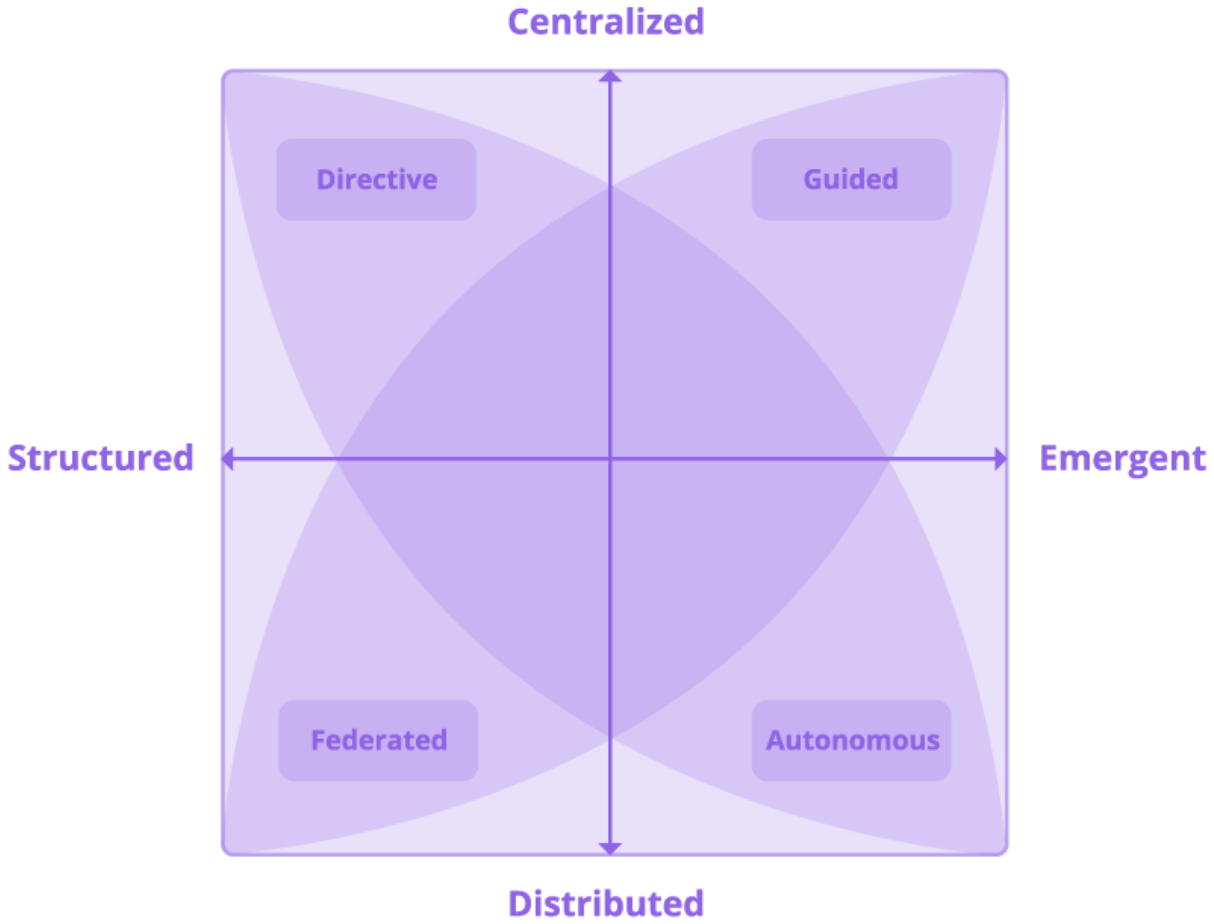
Key Activities

- Assess current governance pattern to better understand and visualize your organization’s baseline ☑
- **Conduct stress-testing for the current governance against AI scenarios**

Key Results

- A documented governance baseline
- Clear documentation of where and why current governance breaks

Common breaking points



Decision velocity becomes a breaking point when approval cycles built for humans can't match AI's machine-speed decision-making

Compliance requirements strain under AI's cross-border data flows and algorithmic opacity, making traditional audit and assurance processes ineffective

Governance capabilities prove insufficient when boards and IT leaders lack AI literacy

...

Step 1. Assessing and stress-testing

- Assess and stress-test the current governance system
- Determine AI governance requirements
- Design and implement governance adjustments
- Ensure governance remains responsive to changes

Objectives

- Understand the current governance pattern of your organization
- Evaluate how current governance frameworks hold up under AI-related stress and identify governance “breaking points”

Key Activities

- Assess current governance pattern to better understand and visualize your organization’s baseline ☑
- Conduct stress-testing for the current governance against AI scenarios ☑

Key Results

- A documented governance baseline
- Documentation of where and why current governance breaks

Step 2. Determining requirements

Assess and stress-test the current governance system

Determine AI governance requirements

Design and implement governance adjustments

Ensure governance remains responsive to changes

Objectives

- Define what governance must achieve to ensure responsible, ethical, and effective AI use
- Translate insights from Step 1 into actionable, high-level governance needs

Key Activities

- Define governance requirements using the four AI impact perspectives
  - Decision Authority & Risk Management
  - Ethical Principles & Responsible AI
  - Data Governance & Performance Management
  - Regulatory compliance & Operational standards
- Analyze, document, and prioritize the requirements

Key Results

- A structured set of governance requirements
- A prioritized list of capability gaps and required enablers for effective AI governance

ITIL and AI in 2025

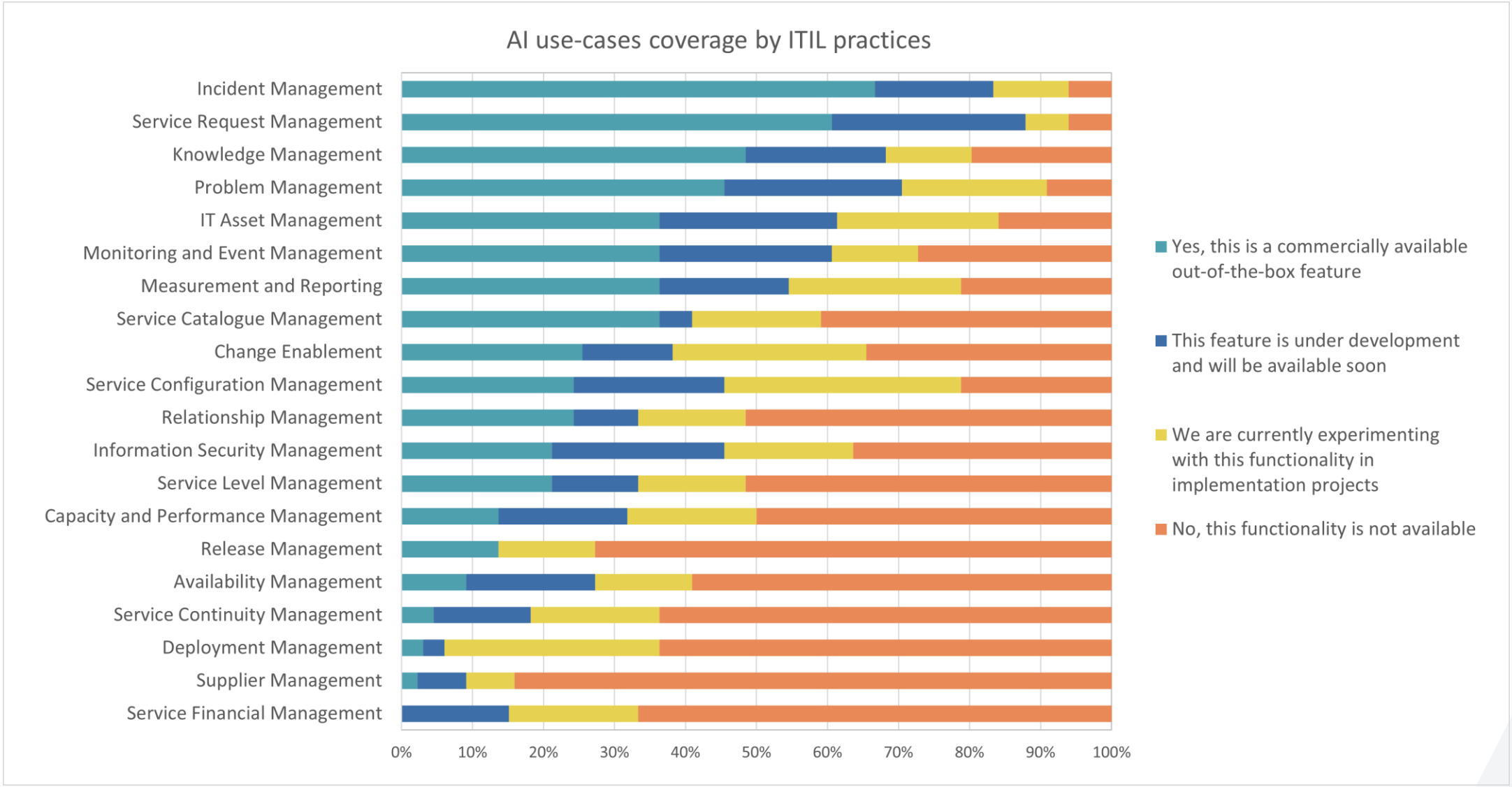


The AI in ITSM tools research conducted with Stephen Mann and 11 ATVs

- 11 ITIL Accredited Tool Vendors (ATVs)
- Self-assessment against 66 functional criteria across 20 ITIL practices
- Interviews with the ATVs to gather additional information and ‘soundbites’

ATLASSIAN · DCON · freshworks · invgate · ITOMIG · ManageEngine ServiceDesk Plus · MATRIX42 · OMNINET SOFTWARE SOLUTIONS · opentext™ · proactivanet · SysAid®

Common AI use cases in ITSM tools



Examples of AI use-cases

CRITERIUM	AVAILABLE	R&D	N/A
Incident Management			
13. AI capabilities to automatically categorise and assign incident tickets	82%	18%	0%
14. AI capabilities to automatically suggest the optimal resolution for incidents	82%	18%	0%
15. AI chatbots helping users to get technical support	73%	27%	0%
16. AI-enabled automatic escalation of high-impact incidents based on real-time analysis	36%	36%	27%
17. AI-enabled personalised major incident communication with end users	45%	45%	9%
18. AI-enabled summarisation of complex incident tickets for management reporting	82%	18%	0%
Knowledge Management			
26. AI capabilities to search for knowledge base (KB) articles	73%	18%	9%
27. AI-assisted knowledge gap analysis to highlight incidents, service requests, or events that could have been processed more efficiently if relevant KB articles were available and up to date	18%	64%	18%
28. AI-enabled automatic detection of obsolete KB articles	36%	36%	27%
29. Automatic drafting of KB articles based on existing incident or problem records	73%	27%	0%
30. Automatic rephrasing of KB articles for better clarity	73%	18%	9%
31. Automatic validation of KB articles by checking alignment with approved corporate policies and rules	18%	27%	55%
…			

Step 3. Design and implementation

- Assess and stress-test the current governance system
- Determine AI governance requirements
- **Design and implement governance adjustments**
- Ensure governance remains responsive to changes

Objectives

- Adjust your governance system to the requirements from Step 2
- Bridge the gaps between current capabilities and the desired state

Key Activities

- Adapt within the organization's existing governance pattern
- Build permanent governance capabilities
- Apply AI governance tools and models to design practical controls

Key Results

- A detailed governance design integrating AI-specific oversight mechanisms
- A capability-development and implementation roadmap

Step 3. Design and implementation

- Assess and stress-test the current governance system
- Determine AI governance requirements
- **Design and implement governance adjustments**
- Ensure governance remains responsive to changes

Objectives

- Adjust your governance system to the requirements from Step 2
- Bridge the gaps between current capabilities and the desired state

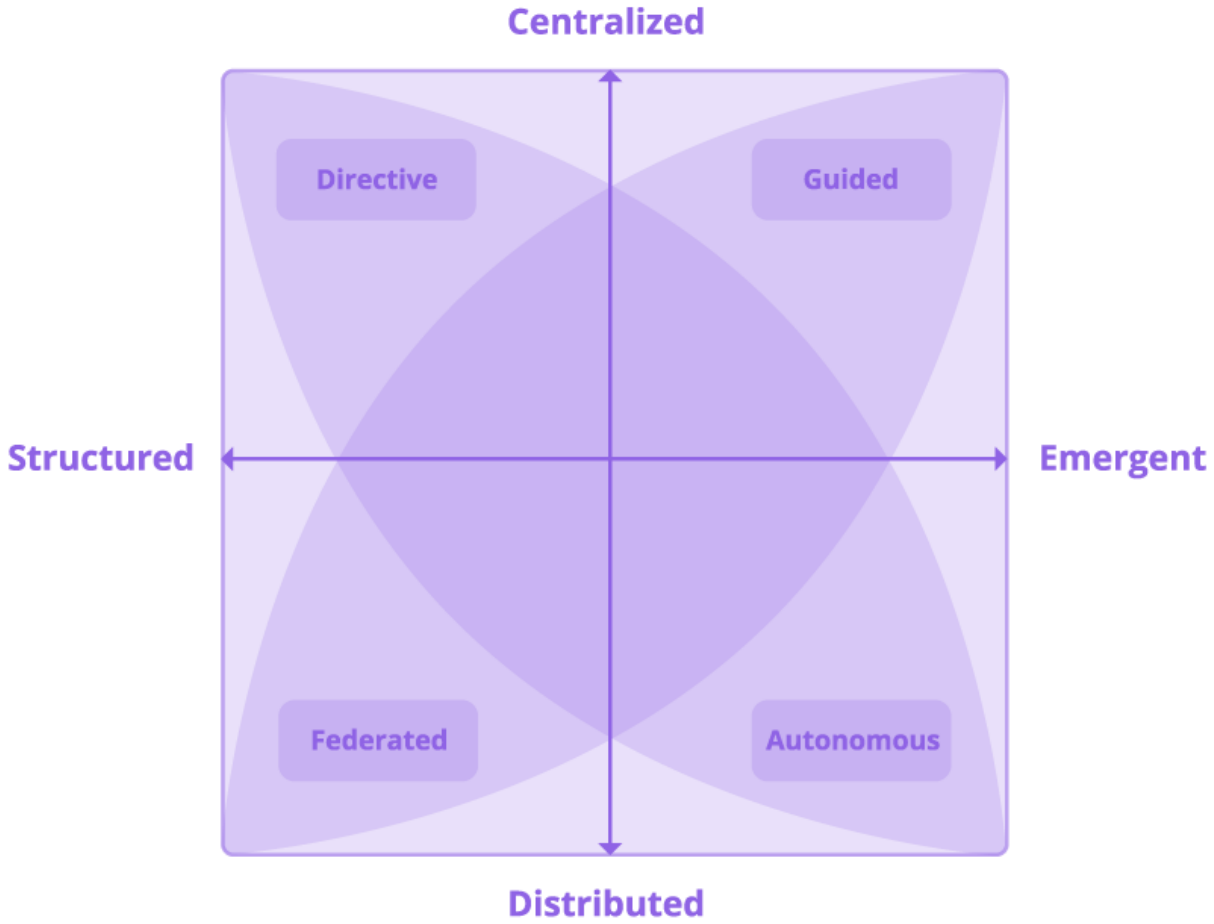
Key Activities

- **Adapt within the organization's existing governance pattern**
- Build permanent governance capabilities
- Apply AI governance tools and models to design practical controls

Key Results

- A detailed governance design integrating AI-specific oversight mechanisms
- A capability-development and implementation roadmap

Adapting existing governance patterns



Directive: introduce pre-approved AI decision parameters and clear escalation triggers

Guided: define high-level AI principles that allow flexible implementation

Federated: establish cross-unit AI councils and shared governance mechanisms

Autonomous: create peer-review and transparency frameworks for self-governing

Step 3. Design and implementation

- Assess and stress-test the current governance system
- Determine AI governance requirements
- **Design and implement governance adjustments**
- Ensure governance remains responsive to changes

Objectives

- Adjust your governance system to the requirements from Step 2
- Bridge the gaps between current capabilities and the desired state

Key Activities

- Adapt within the organization's existing governance pattern ☑
- Build permanent governance capabilities
- **Apply AI governance tools and models to design practical controls**

Key Results

- A detailed governance design integrating AI-specific oversight mechanisms
- A capability-development and implementation roadmap

AI risk management approach

Below is a **structured approach to creating AI risk profiles** by layering a functional AI model with typical AI risks and contextual risk factors. This will help enterprises identify, prioritise, and mitigate risks tailored to specific AI functionality, especially beyond its intended use.



Mark which AI functions the application performs (create a functional profile)

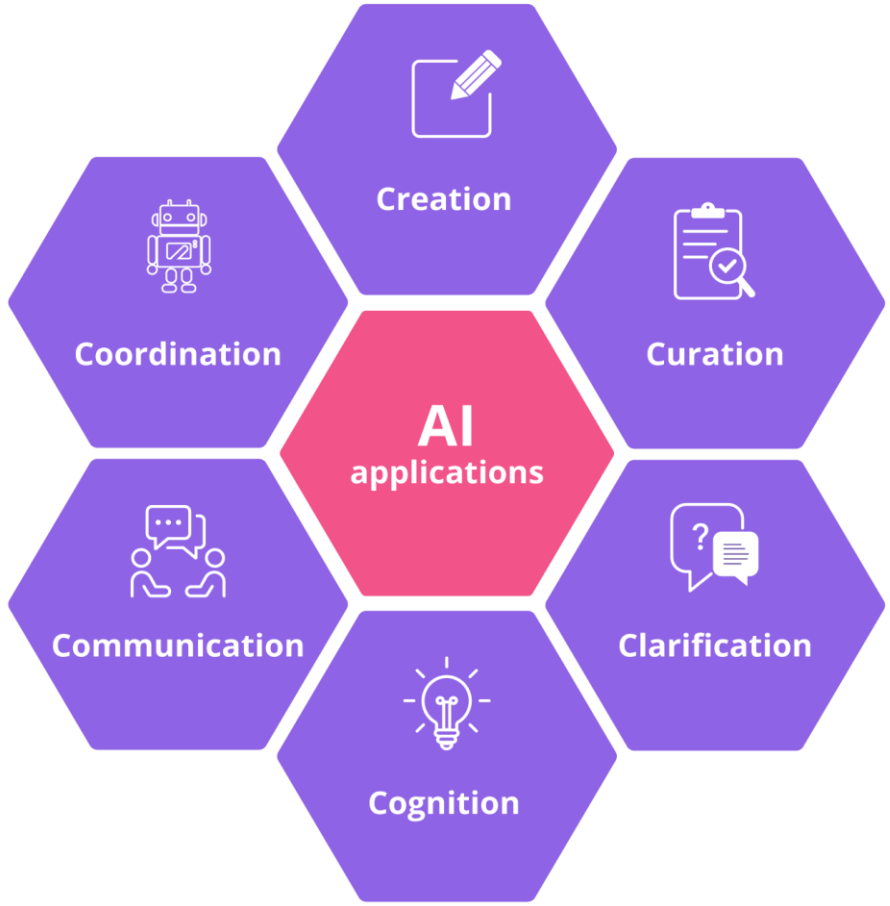
Use the identified AI functions to understand the risk profile*

Complete the risk profile by applying contextual risk factors that influence risk relevance and severity

Select and tailor risk mitigations based on the structured risk profile and common risk controls

(*) Non-AI-specific risks should also be identified and added to the risk profile at this stage.

1. 6C Model for AI



The model provides a **functional classification** of AI solutions.

It **helps understand and communicate** the range of possible applications of AI.

It can also **enhance AI governance** by helping organisations tailor risk profiles, controls, and countermeasures to the specific functions of AI solutions.

AI in IT management

Creation

AI generates net-new outputs in response to prompts or triggers. This includes producing code, documentation, or any other artefacts that didn't exist before.

- Generating answers to users questions
- Writing code to perform specific functions based on user input
- Generating a workflow based on defined conditions or business rules

Clarification

AI helps users navigate, understand, or improve existing content by summarising, rephrasing, restructuring, or translating it.

- Summarising a complex incident ticket for management reporting
- Rewriting a knowledge article for easier understanding
- Generating a context-specific summary report using a natural language prompt

Communication

AI acts as a communicative interface helping users interact with services and systems naturally.

- Chatbots helping users to get technical support
- Virtual agents assisting with service request submission
- Personalised major incident communication with end users

Curation

AI improves the quality, organisation, and relevance of existing data or knowledge by identifying redundancies, outdated information, or inconsistencies.

- Detecting and flagging obsolete knowledge base articles
- Cleaning up duplicated CI records in CMDB
- Validating documents by checking alignment with approved corporate policies and rules

Cognition

AI identifies patterns, anomalies, or hidden insights across data, enabling proactive detection, forecasting, and analysis.

- Detecting recurring incident trends indicating a deeper problem
- Identifying potential issues caused by changes in complex environments
- Predicting system workload based on historical usage data and seasonal trends

Coordination

AI autonomously executes, orchestrates, or triggers actions across systems – often in response to events, requests, or patterns.

- Triaging incoming user requests and assigning them to appropriate teams
- Automatically escalating high-impact incidents based on real-time analysis
- Triggering remediation workflows after detecting specific errors, events, or trends

2. AI risk heatmap

Risk category	Creation	Curation	Clarification	Cognition	Communication	Coordination
1. Autonomy in decision-making	Low	Low	Low	Medium	Medium	High
2. Transparency and explainability	Medium	Medium	Medium	High	Medium	High
3. Access control misalignment between source data and AI outputs	High	Medium	Medium	Medium	High	Low
4. Hallucination and mistakes in generated outputs	High	Low	Medium	Medium	High	Medium
5. Bias and fairness risks	High	Medium	High	High	High	Medium
6. Data availability and quality for AI training	High	High	Medium	High	Medium	High
7. Operational and lifecycle risks	Medium	Medium	Medium	High	Medium	High
8. Extended supply chain and third-party AI governance risks	Medium	Medium	Medium	Medium	Medium	Medium
9. Legal, regulatory, and compliance risks	High	Medium	Medium	High	High	High
10. Organizational readiness and skills	Medium	Low	Low	Medium	Medium	Medium

3. Contextual Risk Factors (CRF)

CRF	Key Questions / Considerations	Examples
Data Sensitivity	Does the AI handle personal, confidential, or regulated data?	HR records, financial info, patient data
User Impact	What is the scale and criticality of users affected?	Internal staff only vs. public customers
Automation Level	Is the AI fully autonomous, or does it require human oversight?	Autonomous remediation vs. advisory only
Regulatory Environment	Are there specific compliance requirements?	GDPR, HIPAA, industry standards
Operational Criticality	How critical is AI to business operations or safety?	Incident response system vs. long-term trend analysis
Stakeholder Diversity	Does it serve diverse groups (languages, cultures, roles)?	Multi-region, multilingual users

4. Common AI risk controls (1/2)

1. Autonomy in decision-making

- Define clear accountability and human oversight roles for AI decisions.
- Establish policies for human-in-the-loop or human-on-the-loop controls.
- Set predefined conditions or thresholds for when human intervention is mandatory (high level of risk, low confidence score, ethical or sensitive decisions, etc.).

2. Transparency and explainability

- Use inherently interpretable models when possible.
- Ensure that AI models are designed and implemented to support post-hoc explainability techniques when complex models are used.
- Define explainability expectations based on the system's risk profile and require model cards detailing purpose, limitations, and interpretability approach.

3. Access control misalignment between source data and AI outputs

- Consider using policy-aware or context-aware Retrieval-Augmented Generation (RAG) to constrain the information retrieved and used in AI-generated outputs based on user roles and rights.
- Use model segregation or data tagging to restrict output access.
- Audit AI outputs regularly for unauthorized data disclosures.
- Avoid applying AI models to highly sensitive data unless effective security enforcement mechanisms are in place.

4. Hallucination and mistakes in generated outputs

- Establish human review and validation processes for critical AI outputs.
- Continuously monitor AI outputs for errors and inconsistencies.
- Train staff and users to critically assess and verify AI-generated outputs before acting on them, especially in high-risk or decision-making contexts.
- Develop escalation protocols for detected mistakes.

5. Bias and fairness risks

- Use diverse and representative training datasets.
- Involve diverse stakeholders in model review.
- Perform bias audits on training data and AI models.
- Establish remediation plans for identified biases.

6. Data availability and quality for AI training

- Estimate data sufficiency and quality before model training when possible.
- Implement data cleansing and augmentation practices.
- Monitor model performance for signs of data-related issues.

4. Common AI risk controls (2/2)

7. Operational and lifecycle risks

- Implement continuous monitoring for model drift and performance degradation.
- Develop robust model update, retraining, and retirement procedures.
- Establish AI-specific incident response plans.
- Maintain version control and documentation for AI models.

8. Extended supply chain and third-party AI governance risks

- Conduct due diligence on AI governance practices of suppliers.
- Include AI governance requirements in contracts.
- Monitor and audit third-party AI usage regularly.
- Establish incident reporting agreements.
- Define and enforce policies specifying data types or sensitivity levels that are prohibited from being processed or stored in third-party or cloud environments.

9. Legal, regulatory, and compliance risks

- Maintain up-to-date knowledge of applicable AI and data regulations and standards.
- Integrate regulatory requirements into the design, procurement, and deployment of AI systems.
- Document compliance measures and maintain audit trails for AI system operations.
- Train staff regularly on relevant legal and ethical requirements.

10. Organizational readiness and skills

- Provide AI literacy and ethics training.
- Build organizational awareness, clear accountability, open communication, and leadership commitment to ensure responsible and ethical AI use.
- Align AI initiatives with business strategy.
- Establish clear communication channels for AI governance.

Step 3. Design and implementation

Assess and stress-test the current governance system

Determine AI governance requirements

Design and implement governance adjustments

Ensure governance remains responsive to changes

Objectives

- Adjust your governance system to the requirements from Step 2
- Bridge the gaps between current capabilities and the desired state

Key Activities

- Adapt within the organization's existing governance pattern ☑
- Build permanent governance capabilities
- Apply AI governance tools and models to design practical controls ☑

Key Results

- A detailed governance design integrating AI-specific oversight mechanisms
- A capability-development and implementation roadmap

Step 4. Operating and maintaining AI governance

- Assess and stress-test the current governance system
- Determine AI governance requirements
- Design and implement governance adjustments
- **Ensure governance remains responsive to changes**

Objectives

- Ensure governance remains adaptive and relevant as AI systems and regulations evolve

Key Activities

- Establish operational cycles
- Monitor effectiveness
- Adapt to AI evolution
- Manage stakeholder feedback

Key Results

- A feedback loop connecting AI performance, risks, and value
- A continuously improving AI governance system aligned with organizational targets and external factors

Key takeaways

01 We adopt AI way faster than we learn to effectively control it

02 AI poses specific challenges to existing IT governance systems

03 Don’t assume your IT governance is AI-ready unless you test and prove it

04 An effective AI governance system is more than just about control – It is about care. It is the scaffolding that holds up trust and ensures value

05 New ITIL publications provide practical guidance on how to assess and adjust the existing IT governance systems to ensure responsible AI

ITIL (Version 5) is here



ITIL®
by PeopleCert

ITIL and AI in 2026 and beyond



The practical guide on effective AI governance for enterprises

Why it matters

- Organizations adopt AI faster than learn learn to control it
- Existing technology governance is not enough

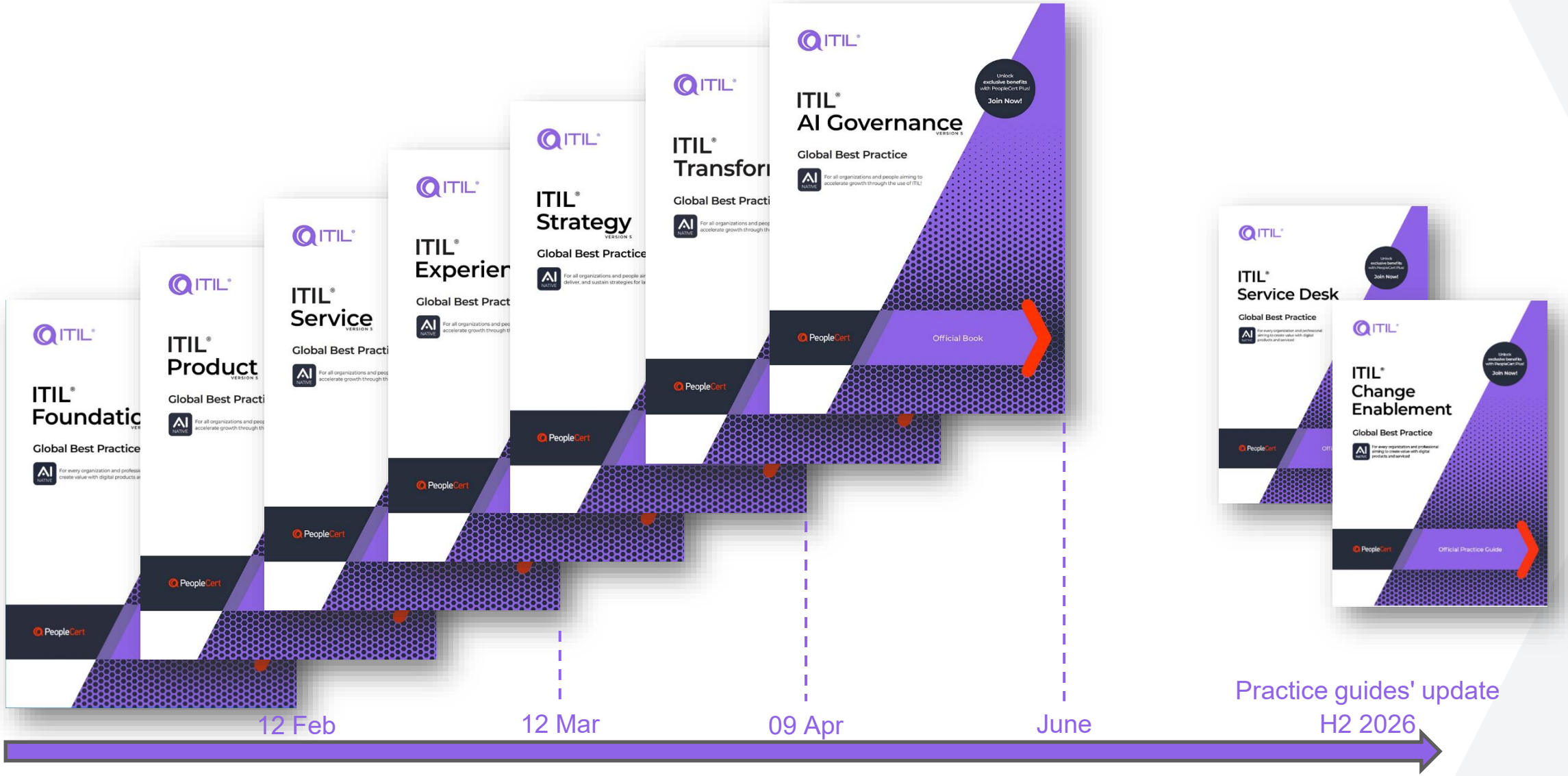
What's inside

- New governance assessment and development model
- New AI Capability model
- Risk assessment guide
- Actionable governance development guidance

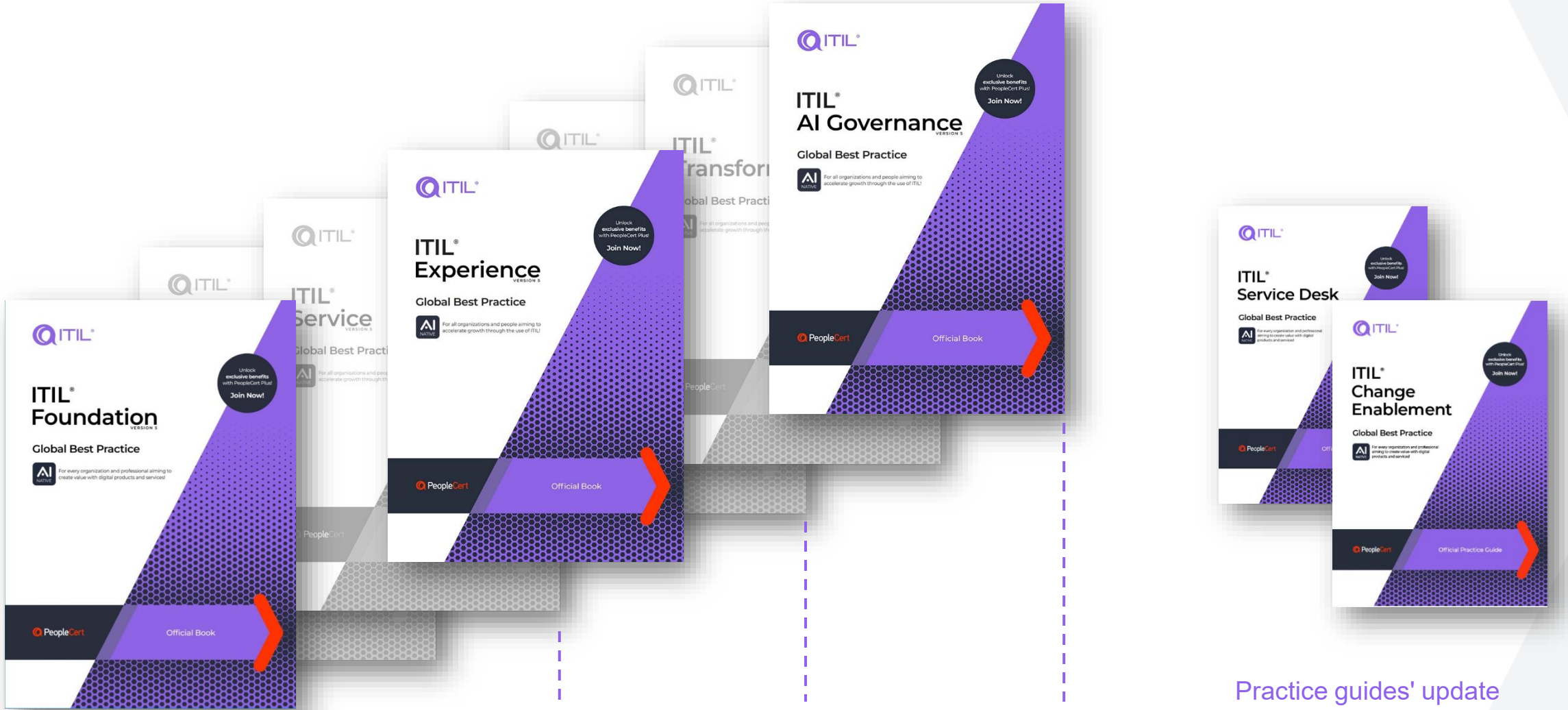
Availability

- June 2026

ITIL and AI in 2026 and beyond

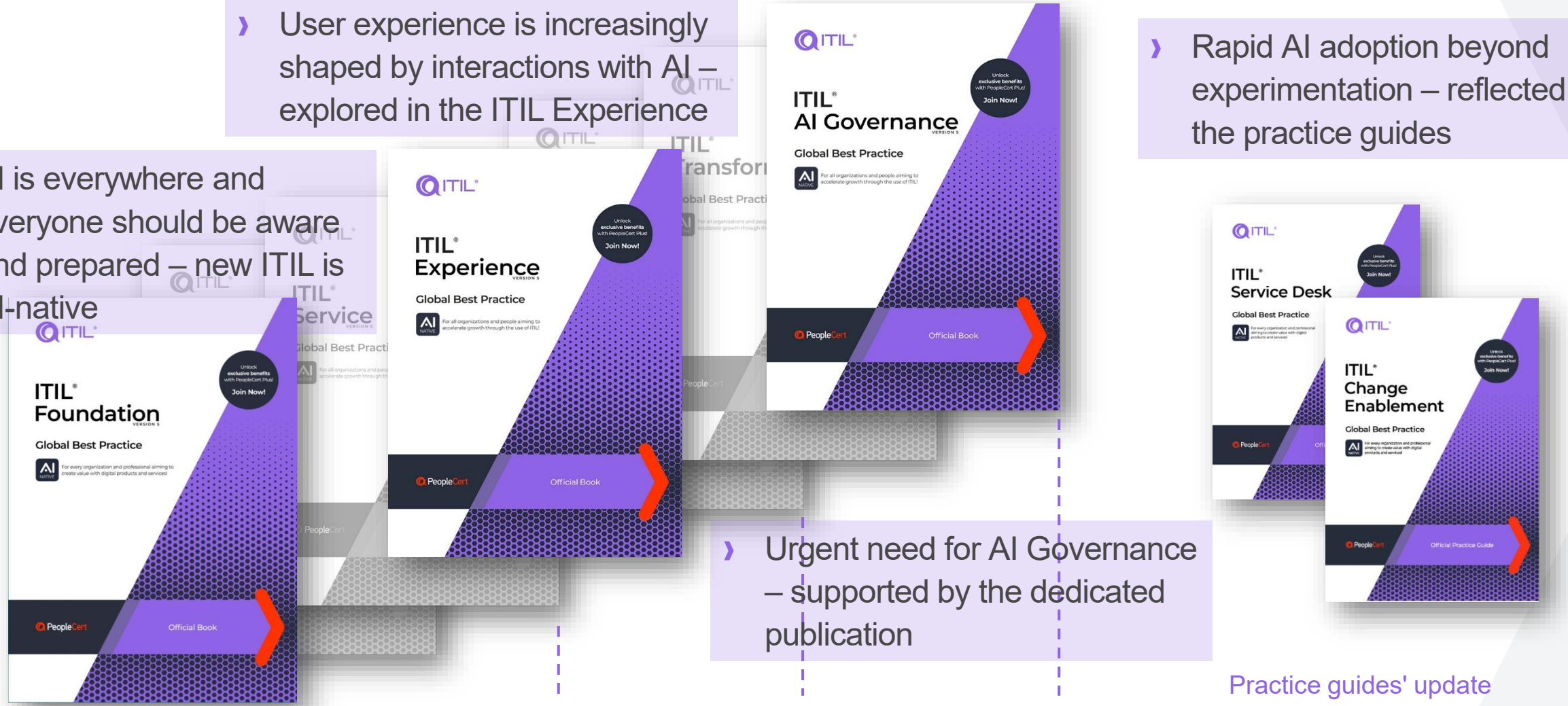


ITIL and AI in 2026 and beyond



ITIL and AI in 2026 and beyond

- User experience is increasingly shaped by interactions with AI – explored in the ITIL Experience
- AI is everywhere and everyone should be aware and prepared – new ITIL is AI-native
- Rapid AI adoption beyond experimentation – reflected in the practice guides
- Urgent need for AI Governance – supported by the dedicated publication



itSMF Bulgaria
The IT Service Management Forum

Thank you!
We might have time for questions



https://www.linkedin.com/in/jourro/
www.youtube.com/@Roman_ITSM



ITIL®

by PeopleCert