digiDations

ATLAS Security Validation for MAS TRM

Mapping the ATLAS Security Validation Platform™ to the MAS Technology

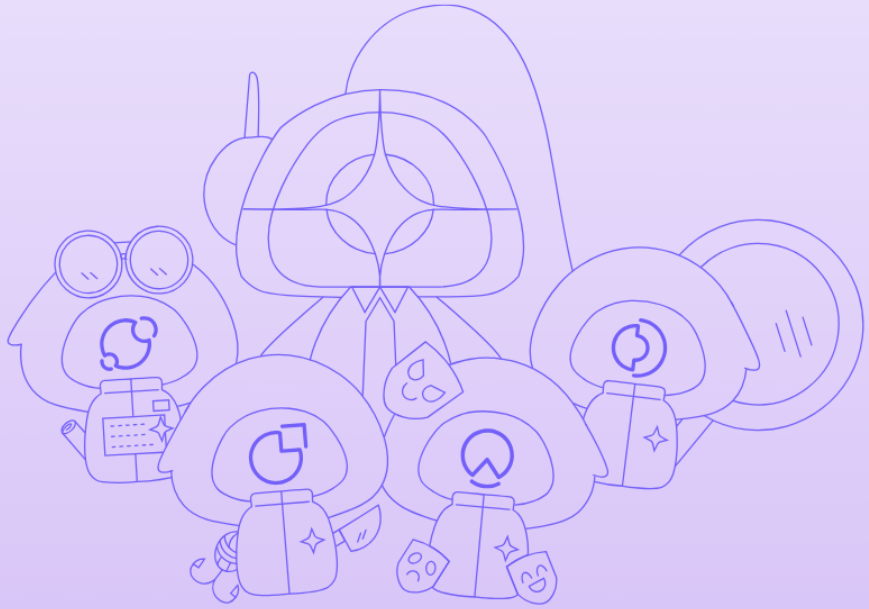

Table of Contents

Executive Summary

Financial institutions operate in an increasingly complex threat landscape where cyber threats continue to evolve in scale and sophistication. To address these risks, the Monetary Authority of Singapore (MAS) established the **Technology Risk Management (TRM) Guidelines**, which provide a comprehensive framework for managing technology risks, protecting critical financial infrastructure, and strengthening cyber resilience within the financial sector.

While the TRM Guidelines outline best practices and expectations for technology risk governance, security operations, and cyber resilience, financial institutions must also demonstrate that their security controls operate effectively against real-world adversary tactics, techniques, and procedures (TTPs). Traditional security assessments such as periodic penetration testing or vulnerability scans often provide only point-in-time insights and may not fully validate whether deployed security controls can detect, prevent, and respond to modern cyber threats.

This white paper explains how the **ATLAS Security Validation Platform** from digiDations helps financial institutions comply with the requirements of the MAS TRM Guidelines by continuously validating the effectiveness of their cybersecurity defenses. ATLAS uses adversarial simulation techniques to emulate real-world threat scenarios and evaluate the performance of security controls, detection rules, and incident response processes across the organization's environment.

The platform supports multiple areas highlighted in the MAS TRM Guidelines, including the **Technology Risk Management Framework**, **Data and Infrastructure Security**, **Cyber Security Operations**, and **Cyber Security Assessment**. Through continuous security validation, organizations can verify whether their defenses operate as intended, identify control gaps, and improve their ability to detect and respond to emerging threats.

By aligning continuous security validation with regulatory expectations, ATLAS enables financial institutions to move beyond theoretical compliance and gain measurable assurance of their cybersecurity posture. This approach strengthens operational resilience and helps organizations better defend against evolving threat actors targeting the financial sector.

MAS TRM Guidelines Compliance Mapping Table

The following tables provide a mapping between selected clauses from the **Monetary Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines** and capabilities of the **ATLAS Security Validation Platform**.

The mapping illustrates how ATLAS can support organizations in **validating the effectiveness of cybersecurity controls, monitoring mechanisms, and incident response processes** referenced in the MAS TRM Guidelines. By simulating realistic adversary techniques and evaluating how security controls perform during these simulations, organizations can gain measurable insight into the operational effectiveness of their defenses.

The ATLAS Security Validation Platform **does not itself establish regulatory compliance**. Compliance with the MAS TRM Guidelines requires financial institutions to implement appropriate governance, risk management processes, and security controls in accordance with MAS supervisory expectations. ATLAS supports these efforts by providing continuous validation capabilities that help organizations assess whether their implemented controls and security operations function effectively against realistic threat scenarios.

The mapping focuses on specific clauses with TRM Guidelines most closely related to cybersecurity control validation, including **Section 4 (Technology Risk Management Framework), Section 11 (Data and Infrastructure Security), Section 12 (Cyber Security Operations), and Section 13 (Cyber Security Assessment).**

Table 1: Technology Risk Management Framework (Section 4)

MAS TRM Clause	MAS TRM Guidelines Requirement	ATLAS Validation Capability	Validation Evidence
TRM 4.1.5	**As business and IT environments, as well as the cyber threat landscape, evolve over time, the FI should review the adequacy and effectiveness of its risk management framework regularly.**	ATLAS continuously validates the effectiveness of security controls, monitoring logic, and response processes through adversarial simulations across the attack lifecycle.	Continuous simulation results and detection metrics demonstrate whether security controls remain effective against evolving adversary techniques.
TRM 4.2.1	**The financial institution should identify the threats and vulnerabilities applicable to its IT environment, including information assets maintained or supported by third-party service providers. Examples of threats include internal sabotage, malware, and data theft.**	ATLAS simulates realistic adversary campaigns and attack techniques based on threat group behavior and emerging threat intelligence. Simulations can replicate malware delivery, execution techniques, and data exfiltration scenarios to evaluate the effectiveness of existing security controls and detection rules.	Simulation findings highlight gaps in detection coverage and control effectiveness, enabling organizations to identify previously unrecognized attack paths or monitoring weaknesses.
TRM 4.3.2	**To facilitate the prioritisation of technology risks, financial institutions should establish criteria to measure and determine**	ATLAS executes adversary techniques aligned with recognized attack frameworks such as MITRE ATT&CK, allowing organizations to	Simulation outcomes reveal which attack techniques are most likely to succeed and which systems or applications are most exposed,

	the likelihood and impact of risk scenarios.	evaluate risk scenarios across multiple stages of the attack lifecycle.	helping organizations prioritize mitigation actions.
TRM 4.4.1	**IT control and risk mitigation approaches should be regularly reviewed and updated, taking into account changes in the threat landscape and the institution's risk profile.**	ATLAS provides sector-relevant adversary scenarios based on threat group targeting patterns and active attack campaigns. Simulation results help security teams refine detection rules, improve correlation logic, and strengthen defensive controls.	Detection improvement metrics and updated monitoring rules demonstrate how defensive controls evolve in response to gaps identified during validation exercises.
TRM 4.5.1	**The financial institution should institute processes to assess and monitor the design and operating effectiveness of IT controls against identified risks.**	ATLAS continuously verifies whether deployed security technologies and controls operate as expected when exposed to simulated adversary behavior. Controlled simulations test the effectiveness of monitoring tools and security controls across the environment.	Continuous validation reports and control performance metrics provide evidence that security controls are functioning as intended and effectively addressing identified technology risks.

Table 2: Data and Infrastructure Security (Section 11)

MAS TRM Clause	MAS TRM Guidelines Requirement	ATLAS Validation Capability	Validation Evidence
TRM 11.1.1	**The FI should develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorized access, modification, copying, or transmission of its confidential data, taking into consideration the following:** - **Data in motion** - **Data at rest**	ATLAS simulate various data exfiltration techniques to effectively validate the current security measures that are in place to protect data in motion ATLAS simulate realistic adversary attack techniques known to access, copy and modification of data at rest.	Detection alerts, simulation logs, and validation reports demonstrate whether defensive controls successfully identify simulated attack activity.
TRM 11.2.2	**To minimise the risk of cyber threats, such as lateral movement and insider threat, the FI should deploy effective security mechanisms to protect information assets. Information assets could be grouped into network segments based on the criticality of systems, the system's functional role (e.g. database and**	ATLAS simulates realistic lateral movement techniques used by threat actors based on threat group behavior and emerging threat intelligence. The result allows security team to have a quick overview of the effectiveness of the security mechanisms in place.	Simulation outcomes identify whether exploitation attempts trigger alerts or defensive responses, highlighting configuration gaps or monitoring weaknesses.

	application) or the sensitivity of the data.		
TRM 11.2.3	**Network intrusion prevention systems should be deployed in the FI's network to detect and block malicious network traffic.**	ATLAS simulates various malicious network traffic such as, but not limited to: - Malware Transfer - Vulnerability Exploitation - Lateral Movement, - Command and Control (C2) - Covert Tunnel This allows security team to continuously validate the effectiveness of the network intrusion prevention system.	Simulation results reveal whether monitoring tools detect abnormal access patterns or data exfiltration behaviors associated with simulated adversary activity.
TRM 11.3.3	**Endpoint protection, which includes but is not limited to behavioural-based and signature-based solutions, should be implemented to protect the FI from malware infection and address common delivery channels of malware, such as malicious links, websites, email**	ATLAS simulates tactics, techniques, procedures (TTPs) that are known to deliver or execution of malware. This includes, but not limited to, the following: - Phishing Email containing malicious links or attachment - Operating System (Host) actions that perform malicious activities	Simulation results reveal whether endpoint protection can block TTPs relevant to the delivery or execution of malware.

	attachments or infected removable storage media.	such as downloading of malware, execution of malware, maintaining persistency - Dropping of malware to Operating System to test signature-based capabilities of endpoint protections. This allows security team to understand the effectiveness of the endpoint protection and include additional mitigation or protection when required.	
TRM 11.3.5	**To facilitate early detection and prompt remediation of suspicious or malicious systems activities, the FI should implement detection and response mechanisms to perform scanning of indicators of compromise (IOCs) in a timely manner, and proactively monitor systems', including endpoint systems', processes for anomalies and suspicious activities.**	ATLAS can launch simulation as and when needed. In addition, ATLAS, is constantly updated with the latest threat group TTPs based on emerging threat intelligence, this allows security team to continuously test their detection and response mechanism to identify potential gaps and areas of improvement within such workflow.	Simulation results contain detailed timestamp for every simulation ran; This includes execution start time, execution end time, detection time.

Table 3: Cyber Security Operations (Section 12)

MAS TRM Clause	MAS TRM Guidelines Requirements	ATLAS Validation Capability	Validation Evidence
TRM 12.2.5	**Correlation of multiple events registered on system logs should be performed to identify suspicious or anomalous system activity pattern.**	The log gateway components of ATLAS allow ingression of different security product logs related to the simulation. This allow security team to have a quick overview of what security product logs were generated, thus allowing them to validate if correlation is possible to identify suspicious activity.	Simulation result display the relevant security product logs that is related to the simulation ran.
TRM 12.3.2	**As part of the plan, the FI should establish a process to investigate and identify the security or control deficiencies that resulted in the security breach. The investigation should also evaluate the full extent of the impact to the FI.**	ATLAS can launch simulation as and when needed. This allows security team to continuously test their detection and response mechanism to identify potential gaps and areas of improvement within such workflow.	Simulation results contain detailed timestamp for every simulation ran; This includes execution start time, execution end time, detection time. Allowing accurate Mean-Time-To-Response (MTTR) calculation

TRM 12.3.3	**Information from cyber intelligence and lessons learnt from cyber incidents should be used to enhance the existing controls or improve the cyber incident management plan.**	ATLAS display the detailed payload of each the attacks. In addition, TARA AI that is inbuilt into ATLAS, allows generation of detection rule for each TTPs and provided in detail explanation and breakdown of the payload. Security team may use this information to deliver lesson learnt, enhancing existing controls and improving cyber incident management plan.	ATLAS display the list of payloads that an attack is going to be executed. TARA AI is available to assist with in-depth explanation of payload as well as provide recommendation such as mitigation control and detection rules.

Table 4: Cyber Security Assessment (Section 13)

MAS TRM Clause	MAS TRM Guidelines Requirements	ATLAS Validation Capability	Validation Evidence
TRM 13.4.1	**The FI should perform an adversarial attack simulation exercise to test and validate the effectiveness of its cyber defence and response plan against prevalent cyber threats.**	ATLAS allows simulation of realistic threat groups scenario to safely evaluate the effectiveness of the entire cyber defense stack including the detection and response capabilities. ATLAS is constantly updated with the latest TTPs and threat group behaviors based on emerging threat intelligence.	ATLAS contains: - 20000+ TTPs - 5000+ Detection Rules - 2000+ Scenarios - 400+ APT Groups Tracking - 160+ Ransomware Gangs Tracking
TRM 13.4.2	**The objectives, scope and rules of engagement should be defined before the commencement of the exercise, and the exercise should be conducted in a controlled manner under close supervision to ensure the activities carried out by the red team do not disrupt the FI's production systems.**	ATLAS contains various components that ensure simulation is perform under controller manner and do not disrupt production system.	The ATLAS components require for a simulation are as follows: Validators – It is a software application that are installed on the golden image of an organization, that are deployed across various security zones. It will execute a
TRM 13.5.1	**To simulate realistic adversarial attacks during any cyber security assessment, the threat scenario should be designed and based on**	The scenarios on ATLAS are build based on latest threat intelligence available. This allow security team to quickly identify threat group that are	ATLAS Scenario Explorer consist of different threat scenario related to various APT and ransomware group.

	challenging but plausible cyber threats.	of interest, understanding their behaviors and proceed with execution if required.	It also provides detail list of TTPs that are utilized within each scenario.
TRM 13.5.2	**The FI could also design the exercise scenario by using threat intelligence that is relevant to their IT environment to identify threat actors who are most likely to pose a threat to the FI; and identify the tactics, techniques and procedures most likely to be used in such attacks.**	The scenarios on ATLAS are build based on latest threat intelligence available. This allow security team to quickly identify threat group that are of interest, understanding their behaviors and proceed with execution if required.	ATLAS Scenario Explorer consist of different threat scenario related to various APT and ransomware group. It also provides detail list of TTPs that are utilized within each scenario.
TRM 13.6.1	**A comprehensive remediation process should be established to track and resolve issues identified from the cyber security assessments or exercises. The process should minimally include the following:** **(a) severity assessment and classification of an issue;** **(b) timeframe to remediate issues of different severity; and**	ATLAS can complement the remediation process as it provides comprehensive result of a simulation such as: - Blocked or Not Blocked - Detected or Not Detected - Execution Start and End Time - Attack Logged Time In addition, it is possible to do a re-simulation after the remediation	Simulation result contains detailed information of a simulation, providing necessary details required for the security team in remediating any gaps identified.

	(c) risk assessment and mitigation strategies to manage deviations from the framework.	process has been completed to re-verify if the remediation works in preventing TTPs that are not blocked or not detected.	

MAS Technology Risk Management Guidelines

The **Monetary Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines**, revised in **January 2021**, provide a comprehensive framework for financial institutions to manage technology risks and strengthen cyber resilience across their digital infrastructure. The guidelines outline supervisory expectations covering governance, technology risk management practices, security controls, cyber operations, and cybersecurity assessments to ensure that financial institutions can effectively safeguard their systems, data, and services against evolving cyber threats.

As financial institutions continue to expand digital services and interconnected technology environments, the complexity of technology risks and cyber threats has increased significantly. The MAS TRM Guidelines emphasize the need for organizations to adopt a structured approach to identifying, assessing, and managing technology risks while ensuring that cybersecurity controls remain effective in protecting critical financial services and sensitive information assets.

Overview of MAS TRM Guidelines

The MAS TRM Guidelines establish a comprehensive set of principles and best practices to help financial institutions manage technology-related risks in a rapidly evolving digital landscape. The guidelines address a wide range of areas, including technology governance, system security, data protection, cyber security operations, and security assessments.

Rather than prescribing specific technologies or solutions, the guidelines define supervisory expectations for how financial institutions should design and implement technology risk management practices. Institutions are expected to adopt appropriate controls that are commensurate with the complexity of their systems, the sensitivity of the data they manage, and the level of risk associated with their operations.

By establishing these expectations, MAS aims to ensure that financial institutions maintain secure and resilient technology environments capable of supporting critical financial services while mitigating risks arising from cyber threats, operational failures, and system vulnerabilities.

Key Cybersecurity Expectations for Financial Institutions

The MAS TRM Guidelines outline several cybersecurity expectations that financial institutions should implement to safeguard their technology infrastructure and information assets. These expectations focus on ensuring that institutions maintain strong preventive, detective, and responsive security capabilities.

Financial institutions are expected to implement security controls to protect sensitive data, maintain secure network and system configurations, and deploy monitoring mechanisms capable of detecting suspicious activities and potential cyber intrusions. Effective cyber security operations are also required to ensure that organizations can identify threats, respond to incidents, and mitigate potential impacts to financial services.

In addition, the guidelines emphasize the importance of continuous monitoring and regular evaluation of cybersecurity controls. Organizations should ensure that their defenses remain effective against emerging threats and that security capabilities evolve in response to changes in the threat landscape.

The Challenge of Demonstrating Security Control Effectiveness

While financial institutions deploy a wide range of security technologies and controls, demonstrating the **effectiveness of these controls** remains a key challenge. Traditional security assessments, such as vulnerability scans, penetration testing, and periodic audits, often provide only point-in-time insights into an organization's security posture.

At the same time, cyber threats continue to evolve as adversaries develop new tactics, techniques, and procedures designed to bypass existing security defenses. As a result, organizations must ensure that their cybersecurity controls are not only deployed correctly but are also capable of detecting and responding to realistic attack scenarios.

The MAS TRM Guidelines recognize the importance of validating cybersecurity defenses through regular security assessments and adversarial simulation exercises. These practices enable financial institutions to identify gaps in their defenses, improve detection and response capabilities, and strengthen overall cyber resilience.

ATLAS Security Validation Platform

Organizations today operate in increasingly complex technology environments where traditional security assessments alone may not provide sufficient visibility into the effectiveness of deployed security controls. As cyber threats evolve, organizations require continuous methods to validate whether defensive technologies, monitoring mechanisms, and response processes operate effectively against modern adversary techniques.

The **ATLAS Security Validation Platform** from digiDations enables organizations to continuously test and validate the effectiveness of their cybersecurity defenses. By simulating realistic adversary techniques in controlled scenarios, the platform provides measurable insight into how security controls detect, prevent, and respond to potential attacks across the organization's environment.

Through continuous validation, organizations can identify gaps in detection coverage, evaluate the effectiveness of monitoring and response processes, and strengthen their overall cybersecurity posture.

Overview of the ATLAS Security Validation Platform

The **ATLAS Security Validation Platform** is designed to evaluate the operational effectiveness of security controls through adversarial simulation. The platform replicates techniques used by real-world threat actors and executes them safely within controlled testing scenarios.

These simulations enable organizations to observe how deployed security technologies — including endpoint protection platforms, network security controls, and security monitoring systems — respond to adversary techniques across different stages of the attack lifecycle.

Unlike traditional security assessments that provide only periodic insight, ATLAS supports **continuous validation**, allowing organizations to regularly test defensive capabilities as infrastructure changes and new threats emerge.

ATLAS Security Validation Methodology

ATLAS follows a structured validation methodology that helps organizations continuously evaluate and improve their cybersecurity defenses.

This validation process can be viewed as four stages:

Verify – Operational Design

Validate baseline configurations and confirm that foundational security controls are functioning correctly.

Evaluate – Security Effectiveness

Simulate realistic adversary techniques to determine whether deployed security technologies detect or prevent malicious activity.

Analyze – Threat Correlation and Security Operations Efficiency

Assess how effectively monitoring systems and analytics platforms correlate alerts and identify potential attack activity across the environment.

Optimize – Incident Response Readiness

Evaluate incident response processes and identify opportunities to improve detection accuracy and response speed.

Through this continuous validation cycle, organizations can measure the effectiveness of their security defenses and strengthen operational readiness.

Capabilities Supporting Security Control Validation

The ATLAS Security Validation Platform provides several capabilities that help organizations validate the effectiveness of their cybersecurity defenses.

First, the platform enables **realistic adversary simulation**, replicating techniques aligned with established attack frameworks such as MITRE ATT&CK. These simulations allow organizations to evaluate how security technologies detect and respond to specific adversary behaviors.

Second, ATLAS supports **continuous validation of security controls**, allowing organizations to regularly test detection mechanisms, monitoring systems, and defensive technologies against simulated attack scenarios.

Third, the platform provides **visibility into detection and response performance**, enabling security teams to identify gaps in monitoring coverage, detection logic, and incident response processes.

By providing continuous insight into how security controls operate under simulated attack conditions, ATLAS enables organizations to strengthen their defensive capabilities and maintain greater confidence in the effectiveness of their cybersecurity controls.

Going Beyond Compliance

Regulatory frameworks such as the **MAS Technology Risk Management (TRM) Guidelines** establish important expectations for managing technology risks and maintaining effective cybersecurity controls. However, compliance with regulatory requirements alone does not guarantee that an organization's defenses are capable of detecting or preventing modern cyber attacks.

As cyber threats evolve and adversaries develop increasingly sophisticated techniques, organizations must move beyond periodic assessments and compliance checks to ensure that their security controls, monitoring capabilities, and incident response processes remain effective.

Limitations of Traditional Security Assessments

Traditional security assessments such as penetration testing and red team exercises have long been used to evaluate an organization's cybersecurity posture. While these assessments can provide valuable insights into vulnerabilities and potential attack paths, they also have several inherent limitations.

Penetration testing engagements are typically conducted over limited timeframes and depend heavily on the expertise and experience of the testers involved. As a result, the range of techniques explored during an engagement may be constrained by time and available resources. In addition, testing activities conducted in production environments often require safeguards to prevent operational disruption, limiting the realism of the assessment.

Similarly, red team exercises simulate adversarial behavior to test detection and response capabilities, but these exercises are often performed infrequently—such as annually or quarterly. Because of their limited duration and scope, they may not provide continuous visibility into how defensive controls perform as systems evolve and new threats emerge.

As a result, these traditional approaches provide **point-in-time insights** rather than continuous assurance of security control effectiveness.

Continuous Security Validation

To address the limitations of traditional assessments, organizations are increasingly adopting **continuous security validation** practices. This approach involves regularly simulating adversary techniques to evaluate how security controls detect and respond to potential attacks across the organization's technology environment.

By replicating realistic attack techniques and observing how defensive technologies respond, security teams can identify gaps in detection coverage, validate the effectiveness of monitoring systems, and measure the readiness of incident response processes.

Continuous validation provides a more comprehensive understanding of an organization's security posture by testing defensive capabilities against a wide range of adversary techniques across multiple stages of the attack lifecycle.

Strengthening Cyber Resilience

Continuous security validation enables organizations to move beyond a purely compliance-driven approach to cybersecurity. Instead of focusing solely on meeting regulatory requirements, organizations can continuously measure and improve the effectiveness of their defensive capabilities.

The **ATLAS Security Validation Platform** supports this approach by enabling organizations to safely simulate real-world adversary techniques and evaluate how security controls perform during these simulations. By incorporating continuous validation into their cybersecurity programs, organizations can strengthen their ability to detect and respond to emerging threats while maintaining greater confidence in the effectiveness of their security defenses.

behavior across different stages of the attack lifecycle. These simulations enable security teams to observe how existing defensive tools and processes respond to real-world attack techniques.

Unlike traditional point-in-time assessments, ATLAS supports continuous validation of security controls across on-premises, cloud, and hybrid environments. The platform orchestrates controlled adversarial simulations and analyzes the resulting telemetry to determine whether security controls successfully detect, block, or respond to simulated attack activities.

The platform architecture includes multiple components that work together to execute simulations and collect validation results, including a centralized management console, simulation agents, telemetry collectors, and sandbox environments for executing high-risk attack behaviors safely. These components enable organizations to validate detection, response, and mitigation capabilities across their entire security architecture.

About digiDations

digiDations is an AI Native cybersecurity company helping organizations replace security assumptions with continuous, measurable validation. The question it answers is not whether an organization has vulnerabilities. It is whether their defenses can keep up with the threats targeting them right now.

Founded by cybersecurity veterans and AI researchers, digiDations built its product portfolio on Digital Mind, a proprietary AI foundation that continuously collects, correlates, and operationalizes real-world attack intelligence. The AI-Driven AEV portfolio includes ATLAS for Security Validation, APOLLO for Continuous Automated Red Teaming, and HELIOS for External Attack Surface Management. ORION for Threat Intelligence extends digiDations' CTEM coverage with adversary intelligence and visibility into emerging attack surfaces.

digiDations is building toward Autonomous Cyber Defense with TARA AI, the Autonomous CTEM Agent that self-directs across all four products: determining which scenarios to run, orchestrating execution, interpreting results, and generating reports, with teams approving decisions rather than defining the workflow.