Evaluating KIBO| A New Hybrid Software Development Method.

Your participation in this questionnaire **promotes scientific research** of the International Hellenic University, towards the evaluation of **a new hybrid software development method** with enhanced **IT/IS auditing**.

* Indicates required question

1. Email *

Informed Consent

*Participation in this study is voluntary. If you agree to participate in this study, you would be interviewed in the context of theoretical evaluation of **a new hybrid software system development method**. The interview includes questions about **the value arising from adapting the proposed method.***

*The information you will share with us will be kept **completely confidential** to the full extent of the law. **No one will be able to see your survey or even know whether you participated in this study**. Study findings will be presented only in summary form and your **name or email would not be used in any report**.*

If you have any questions about this study, please contact Mr. Ioannis Kirpitsas (ikirpit@cs.ihu.gr). If you have questions about your rights as a research participant, please contact Dr. Theodore Pachides, Associate Professor, International Hellenic University (pated@cs.ihu.gr).

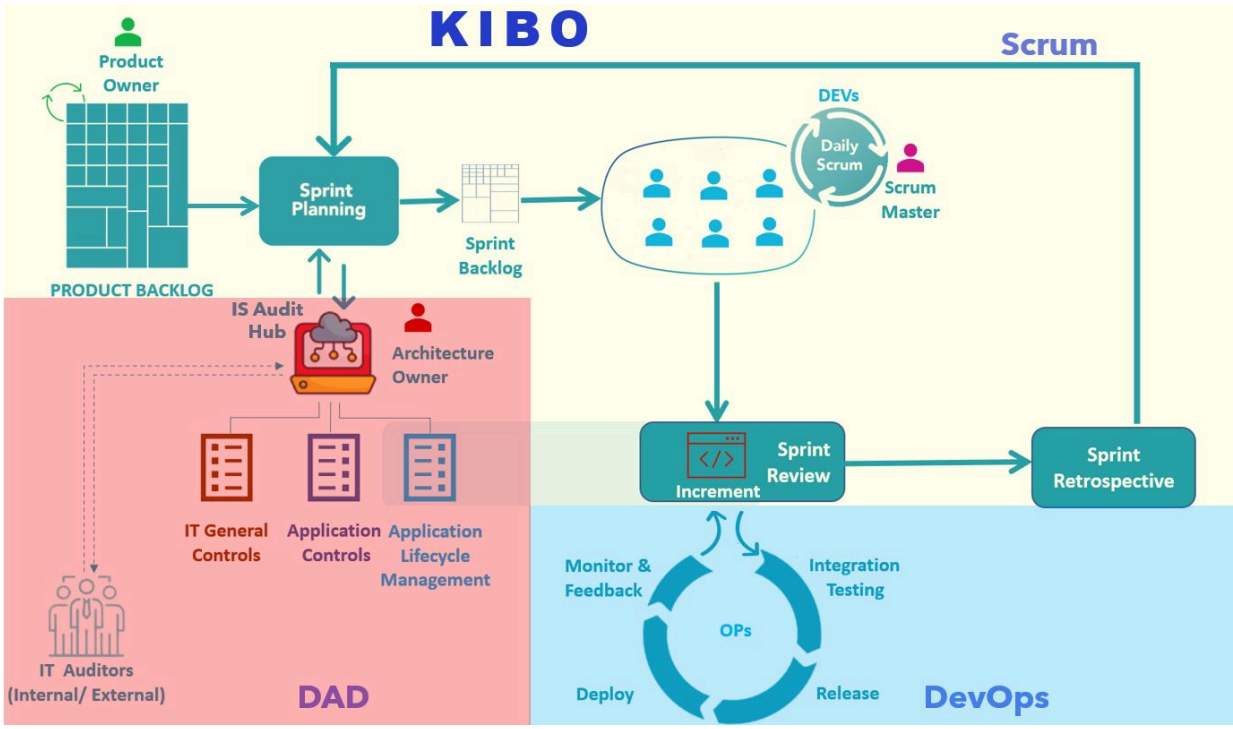
By completing this survey, you are consenting to participate in this study.

Summary

Software development nowadays combines elements from **traditional** and **lightweight** *(agile)* approaches, forming **hybrid methodologies**.
Current research identifies a significant **gap** between **software development** and assurance of **business value** as an SDLC outcome.

We highlight the benefits arise by combining agile methods towards an **IT/IS audit-ready** hybrid SDLC, to eliminate this gap. The proposed method ("***KIBO"***) combines elements from the following methods:

- **SCRUM**, as the basis for teamwork and solution delivery approach, adapting guidelines, events and artifacts.
- **DevOps** as the collaboration basis of the development and operation teams.
- **Disciplined Agile Delivery** (***DAD***), adapting the **Architecture Owner** role as the connection point of **IT/IS Audit function** with the development and operations teams.



Evaluating KIBO Using COBIT 2019 IT Governance Framework

KIBO is assessed using **COBIT® 2019** IT governance framework, that aims to align **IT goals** and **values** with **business objectives,** grouped under the following domains**:**

- Evaluate, Direct and Monitor (***EDM***)
- Align, Plan and Organize (***APO***)
- Build, Acquire and Implement (***BAI***)
- Deliver, Service and Support (***DSS***)
- Monitor, Evaluate and Assess (***MEA***)

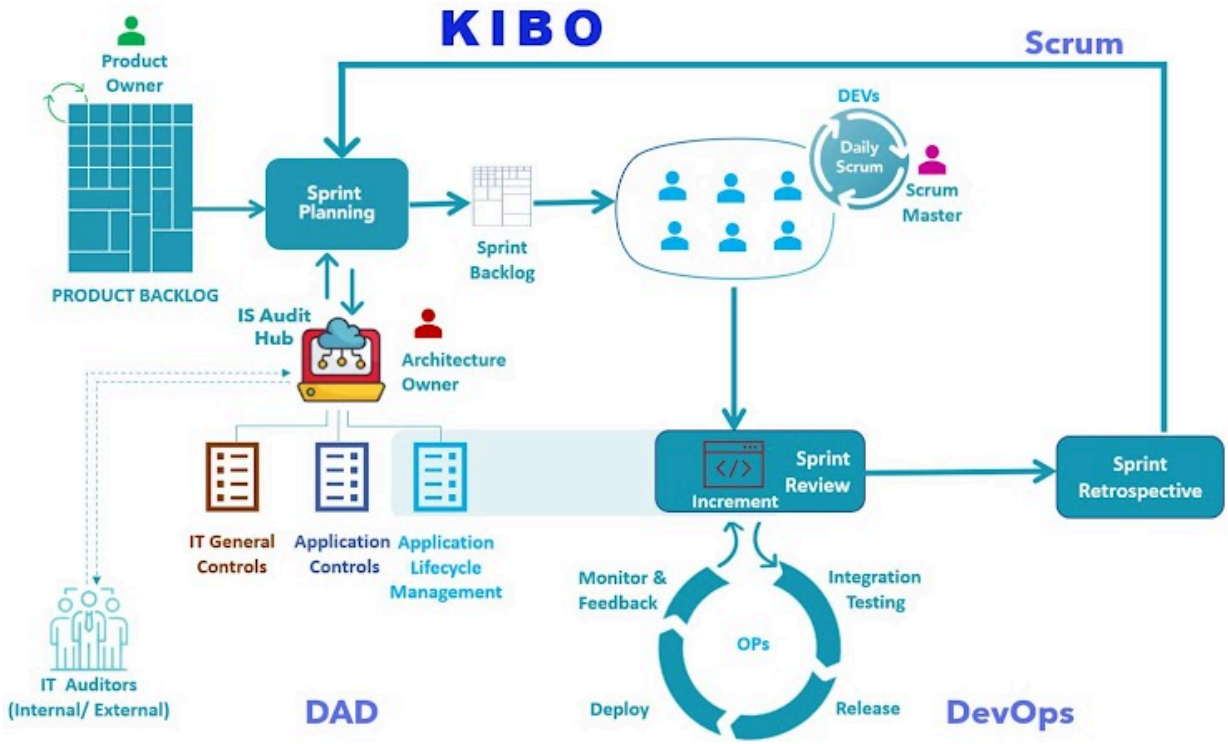
1. Evaluate Direct and Monitor (EDM)

This domain is responsible for **governing** and **managing IT-enabled business investments** through their complete life cycle. verifying that **standards are followed**.

2. **1.1. Ensured Benefits Delivery (*EDM02*)** *

In principle, SDLC activities must **secure optimal value** and **cost-efficient delivery** of a new software system.

KIBO practitioners expect an improvement in agile value driven development, by reducing the occurrence of cost implications due to setup and review of General IT and Application Controls at each sprint, by the Architecture Owner.



Mark only one oval.

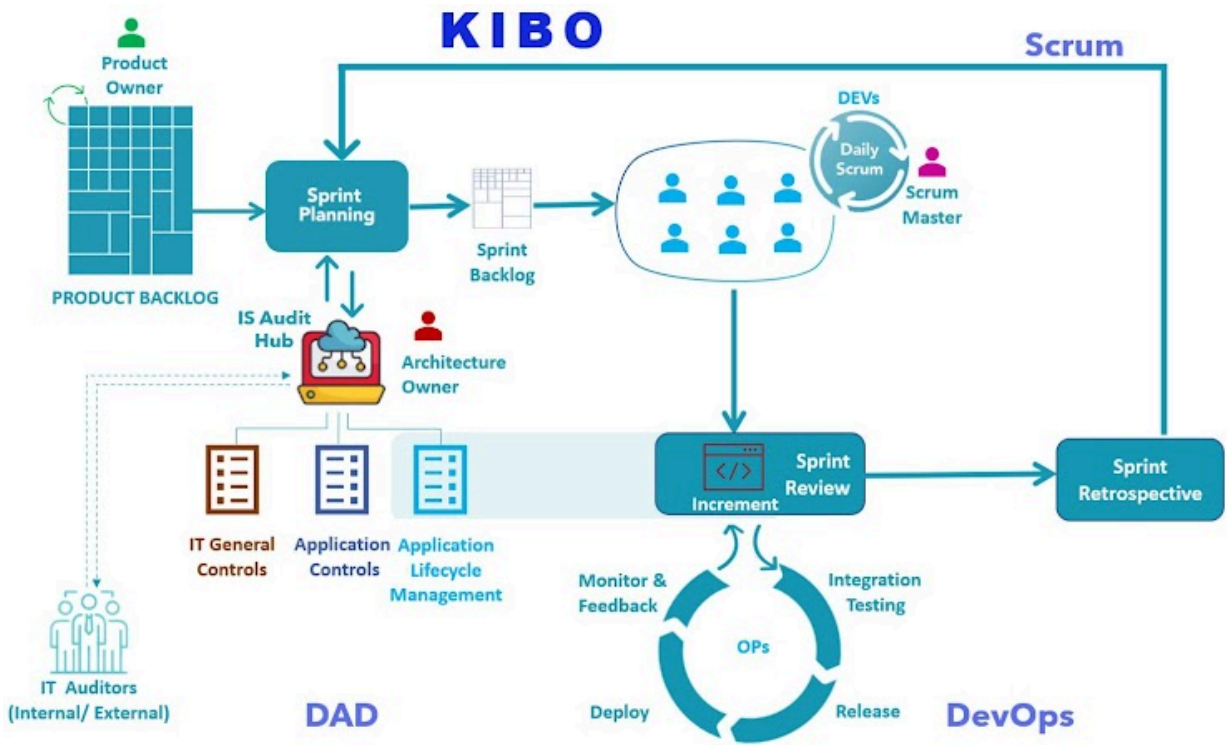
- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

1. Evaluate Direct and Monitor (EDM)

3. **1.2. Ensured Risk Optimization (*EDM03*)** *

Effective IT Governance requires the impact of **IT risk to business value** to be **identified** and **managed**, as well as **compliance failures** to be minimized.

KIBO practitioners foresee significant support to the Product Owner, providing risk assessment and monitoring capability during each sprint. Ensuring compliance is vital for achieving value maximization



Mark only one oval.

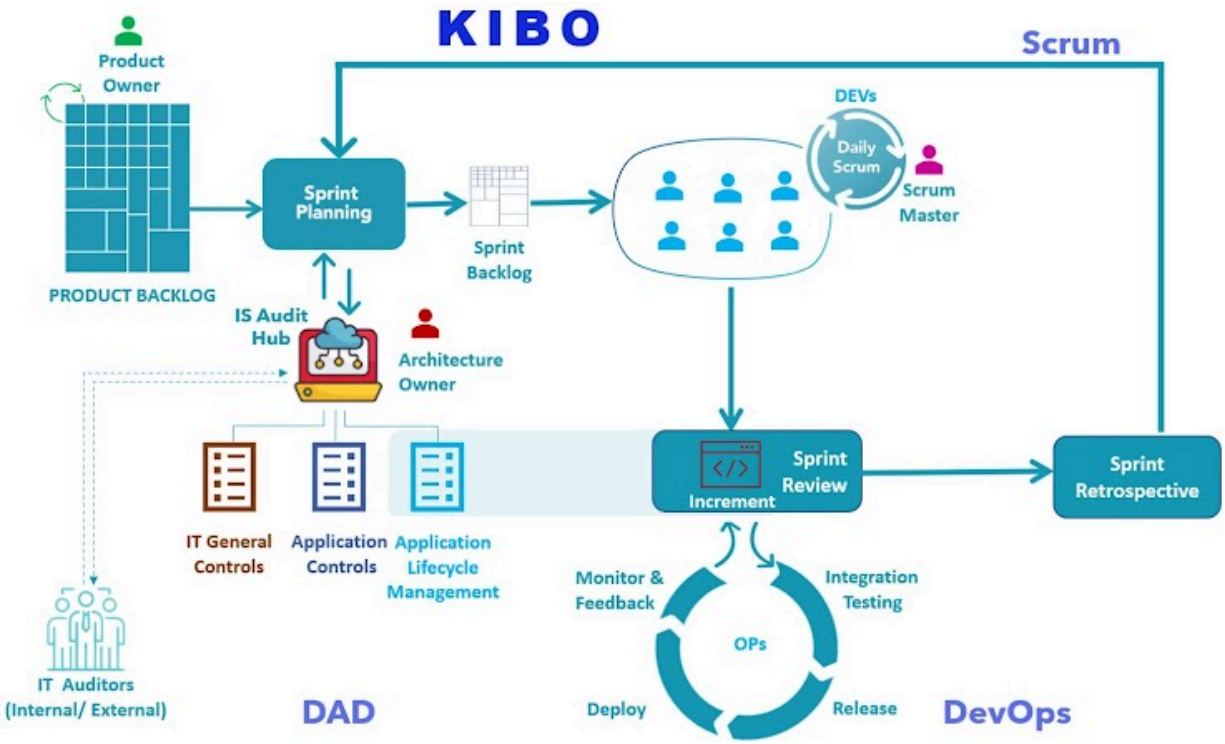
- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

1. Evaluate Direct and Monitor (EDM)

4. **1.3. Ensure Stakeholder Engagement (EDM05)** *

IT Governance requires **effective** and **timely communication** with **stakeholders**, establishing the foundation for reporting to **enhance overall performanc.**

KIBO practitioners expect that Scrum and DevOps metrics, which are visible to management, will be verifiably connected and continuously monitored with the Application and General IT controls.



Mark only one oval.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

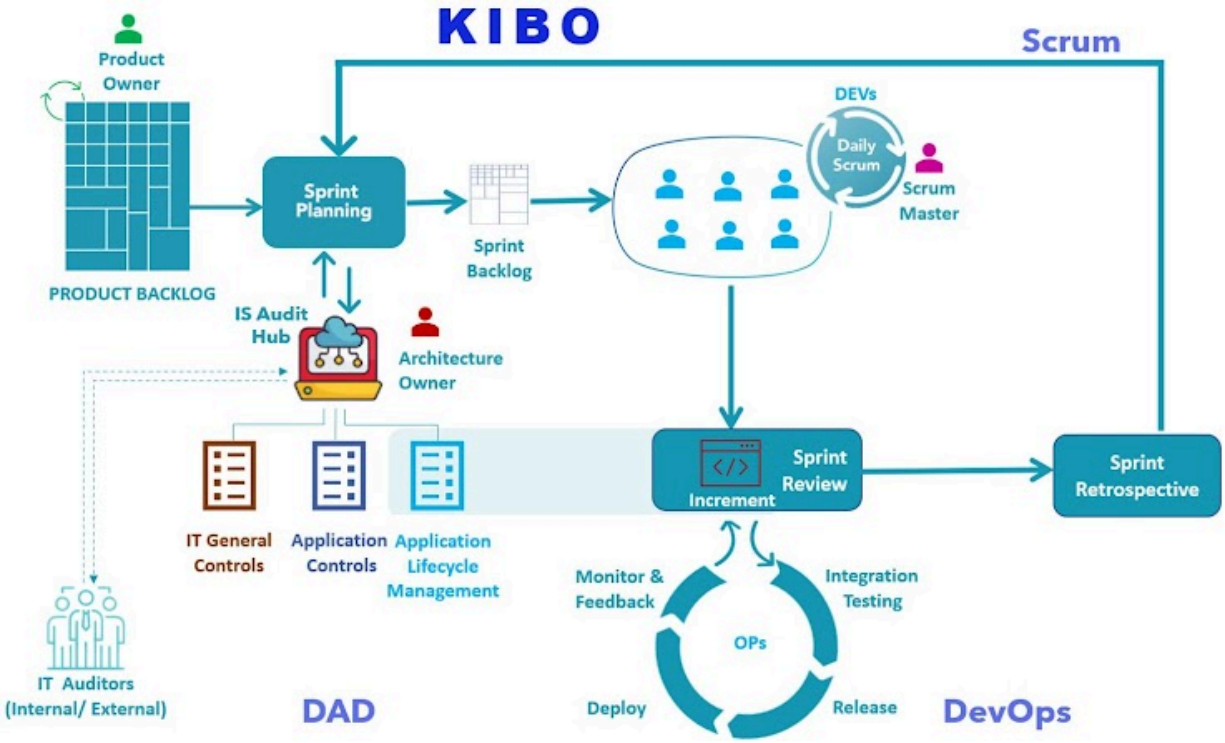
2. Align, Plan and Organize

This domain addresses the overall organization, strategy and supporting activities for information and technology (I&T)

5. **2.1. APO03: Managed Enterprise Architecture *(APO03)*** *

IT Governance highlights the need for a **common architecture** consisting of the necessary layers, including **business process, data, information application** and **technology architecture**.

KIBO practitioners foresee the existence of Application Lifecycle Management, overviewed by the Architecture Owner, enables integration and monitoring of people, data, tools and processes, which is are key elements of architecture governance.



Mark only one oval.

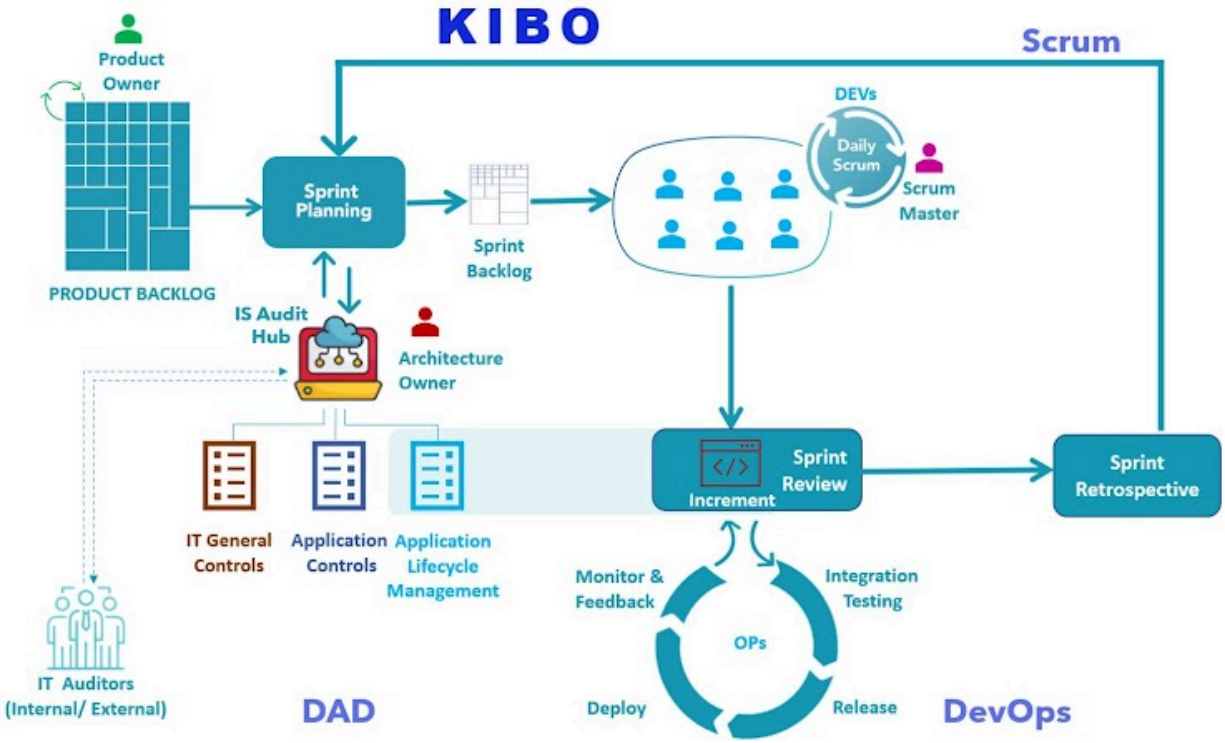
- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

2. Align, Plan and Organize

6. **2.2. Managed Quality *(APO11)*** *

An effectively governed organization ensures **consistent delivery** of software system solutions to meet the **quality requirements** of the enterprise and satisfy stakeholder needs.

KIBO practitioners state that the combination of Application Controls verification, in addition to incremental review and approval, serves to improve the quality of the outcome of each sprint.



Mark only one oval.

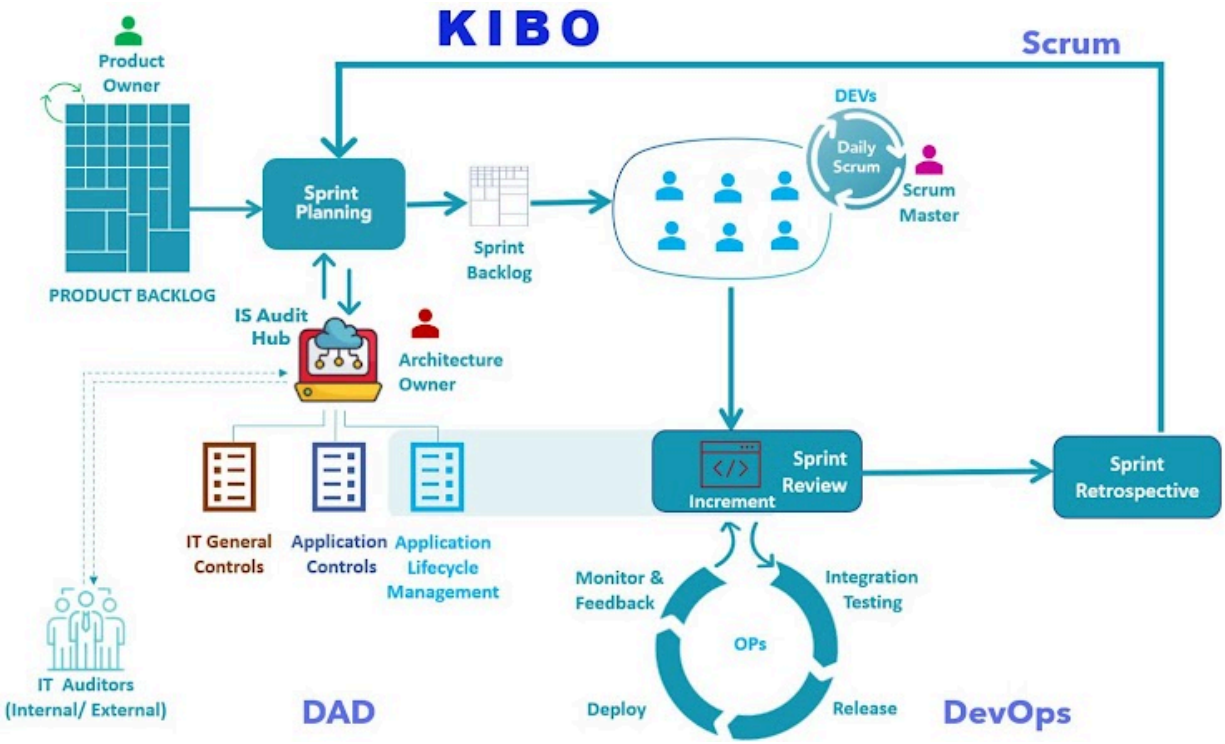
- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

2. Align, Plan and Organize

7. **2.3. Managed Risk *(APO12)*** *

COBIT suggests to continuously **identify**, **assess** and **reduce IT-related risk** within levels of tolerance set by the organization.

KIBO practitioners expect that *"development and release related risks can be precisely monitored, controlled and assessed by internal/external auditors at any point during the product lifecycle, through General IT and Application Controls management."*



Mark only one oval.

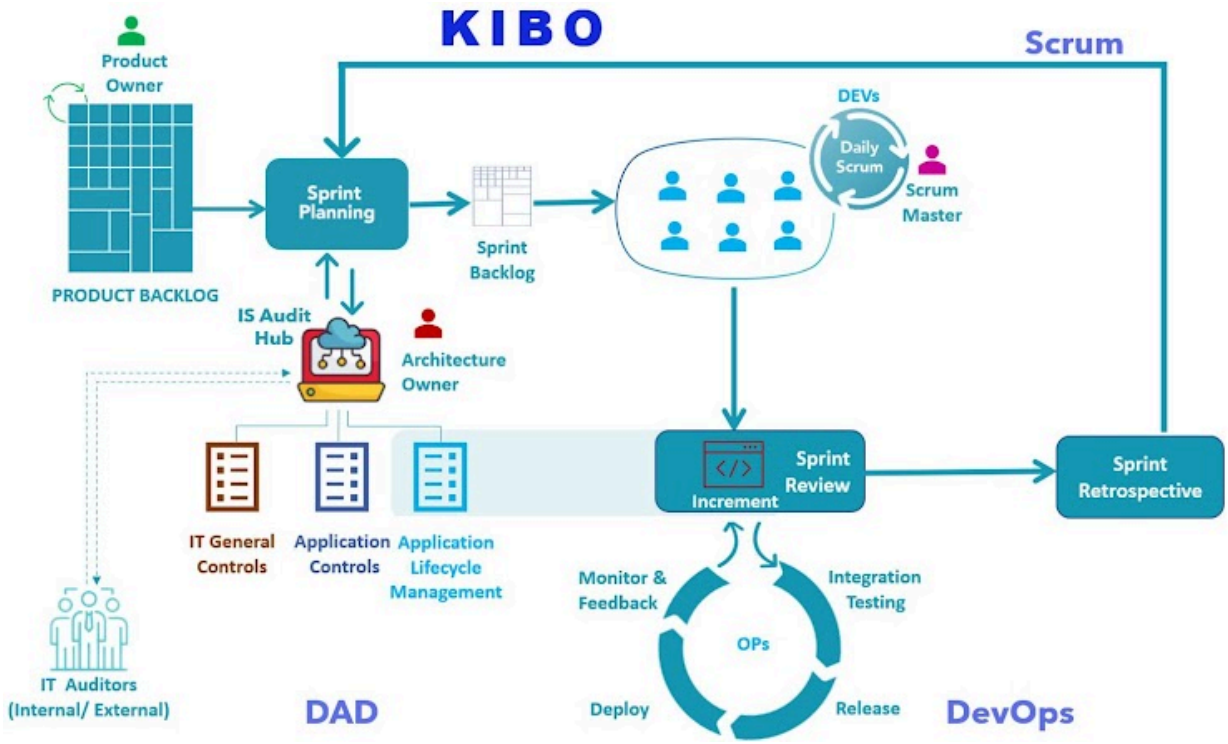
- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

2. Align, Plan and Organize

8. **2.4. Managed Security (APO13)** *

Among the main purposes of IT Governance is to keep the **impacts** and **occurrences** of **security breaches** within the enterprise's risk appetite levels

KIBO practitioners expect that developing software in a controlled environment, which includes vulnerability management as part of the Application Controls managed by the Architecture Owner, improves the effectiveness of enterprise security.



Mark only one oval.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

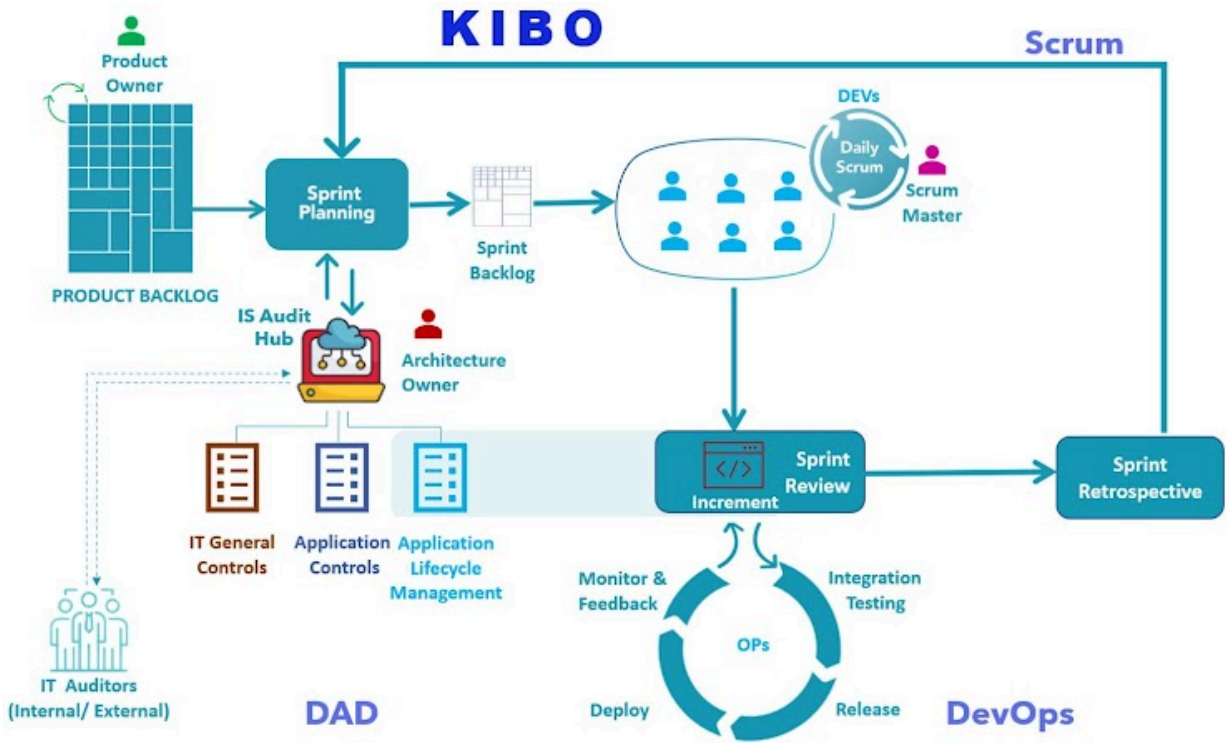
3. Build, Acquire and Implement (BAi)

This domain addresses the definition, acquisition and implementation of I&T solutions and their integration in business processes

9. **3.1. Managed Requirements Definition (BAI02)** *

COBIT recommends systematically coordinating the **consideration of feasible options** alongside affected stakeholders, including **cost/benefit** and **risk analysis**, as well as the **approval of requirements and proposed solutions**.

KIBO practitioners expect that, given the limited documentation and gatewayed approvals in agile development, the Architecture Owner bridges this gap by establishing the necessary controls to safeguard the Development and Operations teams.



Mark only one oval.

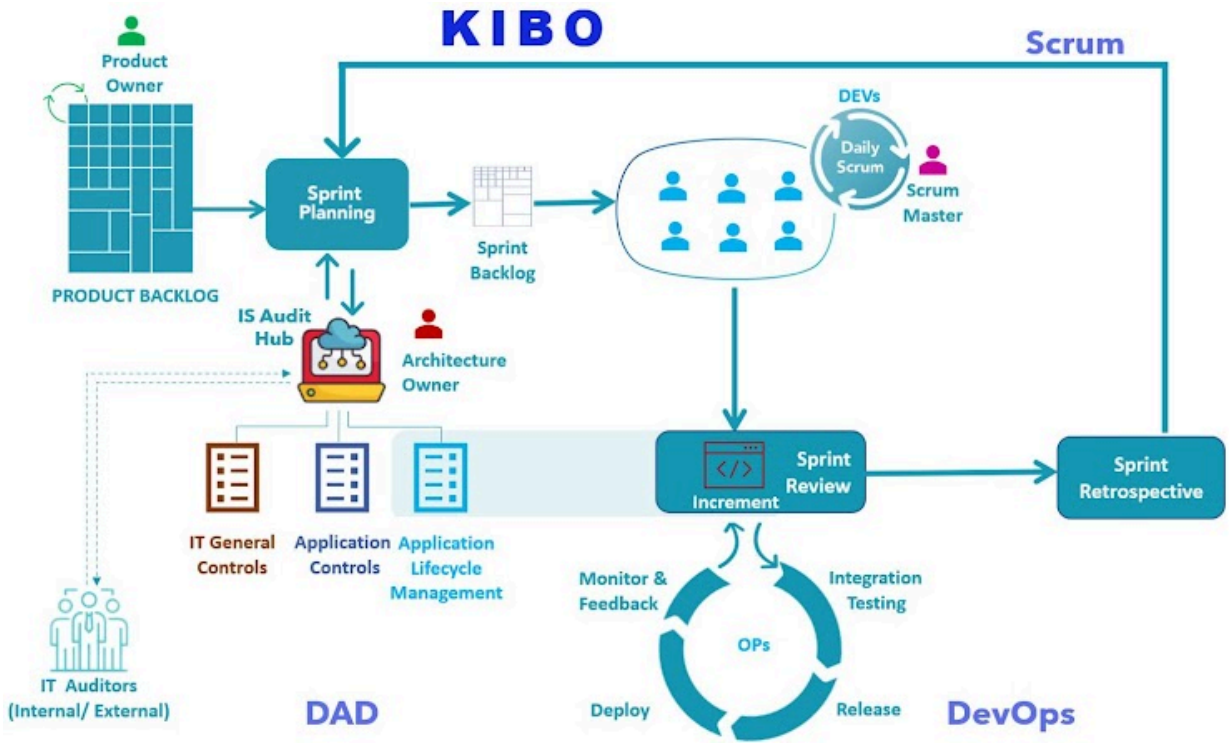
- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

3. Build, Acquire and Implement (BAi)

10. **3.2. Managed Solutions Identification and Build (BAI03)** *

IT Governance mandates the **establishment** and **maintenance** of identified **solutions that cover design, development, procurement/sourcing,** and **partnerships with vendors**, all in support of operational objectives.

KIBO practitioners foresee benefits in terms of the capability to develop and document high-level solution designs, supporting progressive elaboration and ensuring that all control requirements in the business processes, supporting technology, and infrastructure services are addressed and monitored by the Architecture Owner.



Mark only one oval.

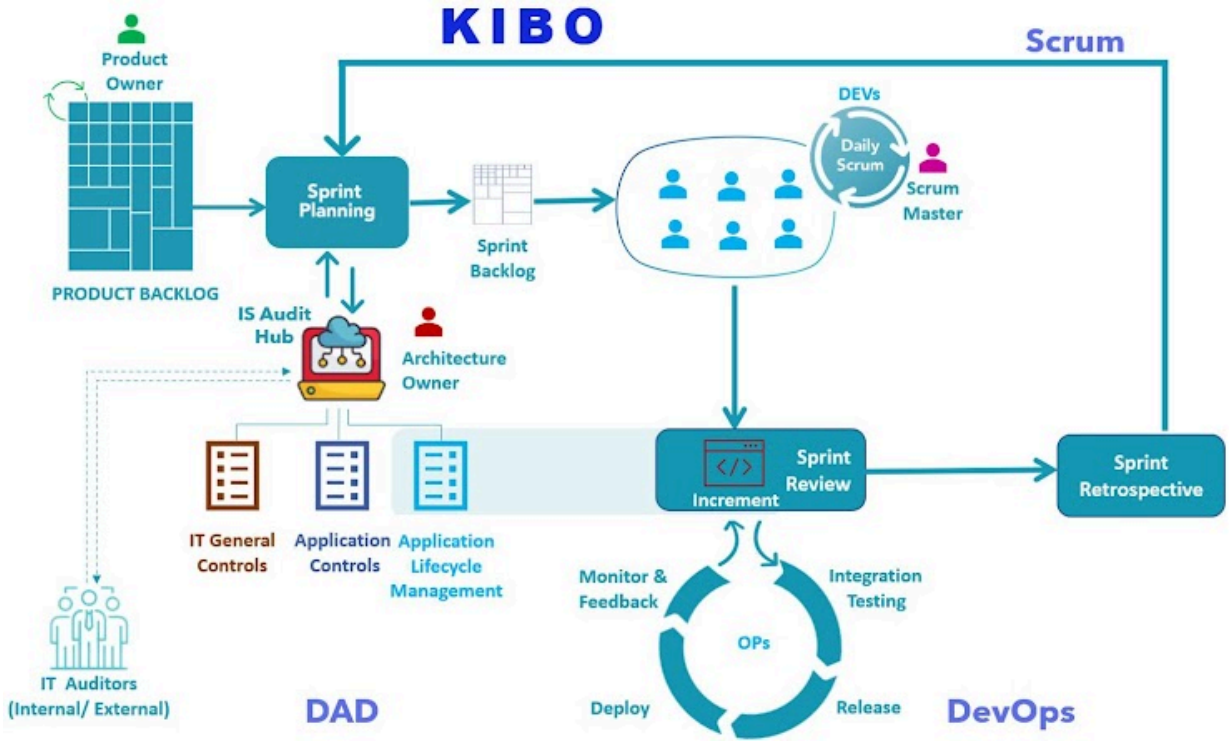
- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

3. Build, Acquire and Implement (BAi)

11. **3.3. Managed Availability and Capacity *(BAI04)*** *

COBIT highlights the importance of ensuring **service availability, efficiently managing resources**, and **optimizing system performance** by predicting **future performance** and **capacity requirements**.

KIBO practitioners expect improved design based on Confidentiality, Integrity, and Availability (CIA) viewpoints, systematically established and monitored by the Architecture Owner.



Mark only one oval.

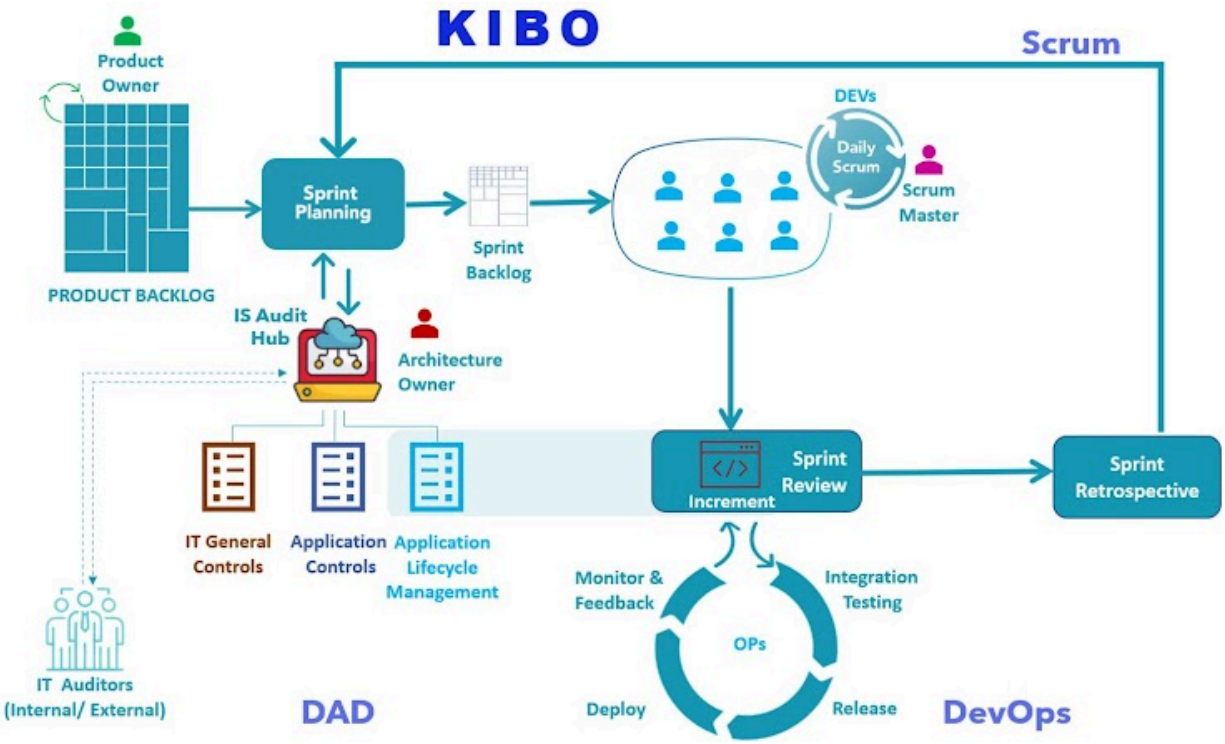
- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

3. Build, Acquire and Implement (BAi)

12. **3.4. Managed IT Changes (*BAI06)*** *

IT Governance acknowledges the need to **manage all changes** in a **controlled manner**, including standard changes and emergency maintenance.

KIBO practitioners expect higher visibility and traceability of changes, as monitored and controlled by the Application Lifecycle Management (ALM), owned by the Architecture Owner.



Mark only one oval.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

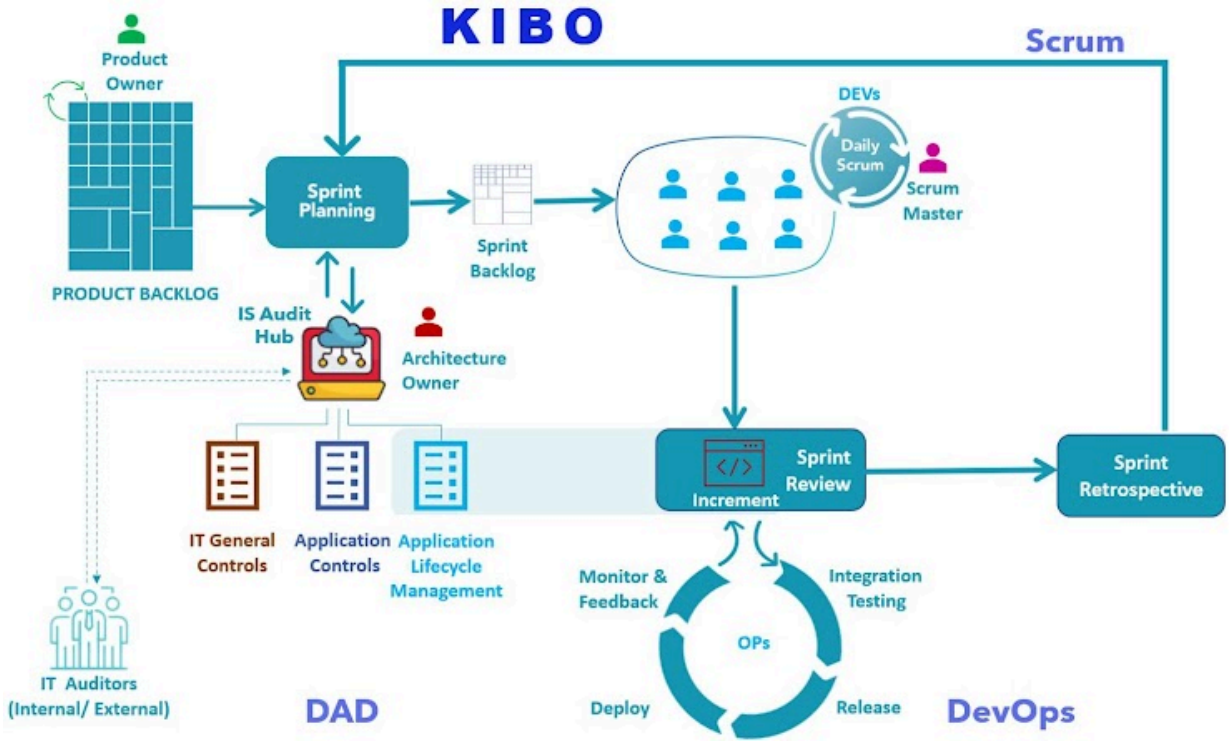
4. Delivery, Service and Support (DSS)

This domain addresses the operational delivery and support of I&T services, including security

13. **4.1. Managed Operations (DSS01)** *

IT Governance involves the execution of **predefined standard operating procedures** and necessary monitoring activities, ensuring the delivery of operational results from software development activities **as planned**.

KIBO practitioners expect a high level of assurance regarding the execution of predefined processes due to the presence of monitored controls, aiming to achieve operational goals.



Mark only one oval.

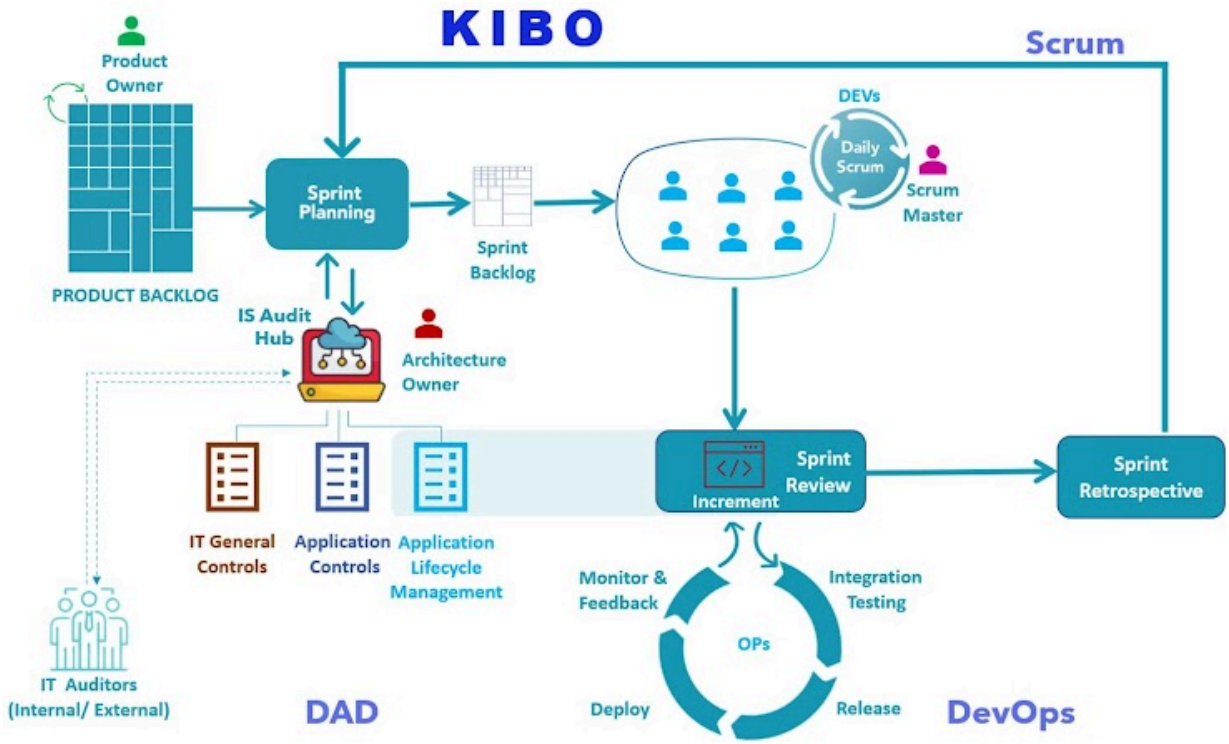
- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

4. Delivery, Service and Support (DSS)

14. **4.2. Managed Continuity (DSS04)** *

COBIT emphasizes the criticality of establishing and maintaining a **plan to enable responding to incidents** and quickly adapt to disruptions.

KIBO practitioners expect that business continuity is tightly secured through the adoption of KIBO, facilitated by the integration of General IT and Application Controls in the solution design, development, and operation.



Mark only one oval.

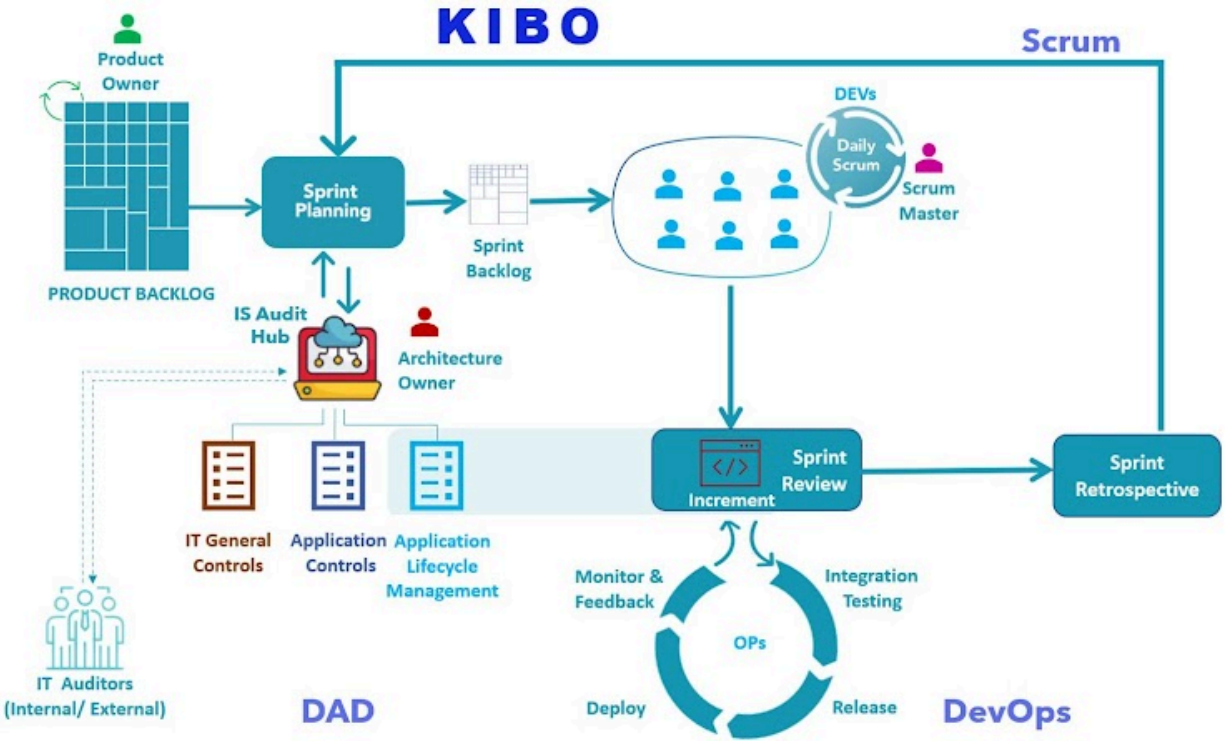
- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

4. Delivery, Service and Support (DSS)

15. **4.3. Managed Security Services *(DSS05)*** *

Effective IT Governance requires establishing and maintaining **information security roles** and **access privileges,** performing **security monitoring** during **software development** and **IT operations**.

KIBO practitioners expect that KIBO encapsulates continuous management of role access privileges, monitoring security issues, and control during development and operations.



Mark only one oval.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

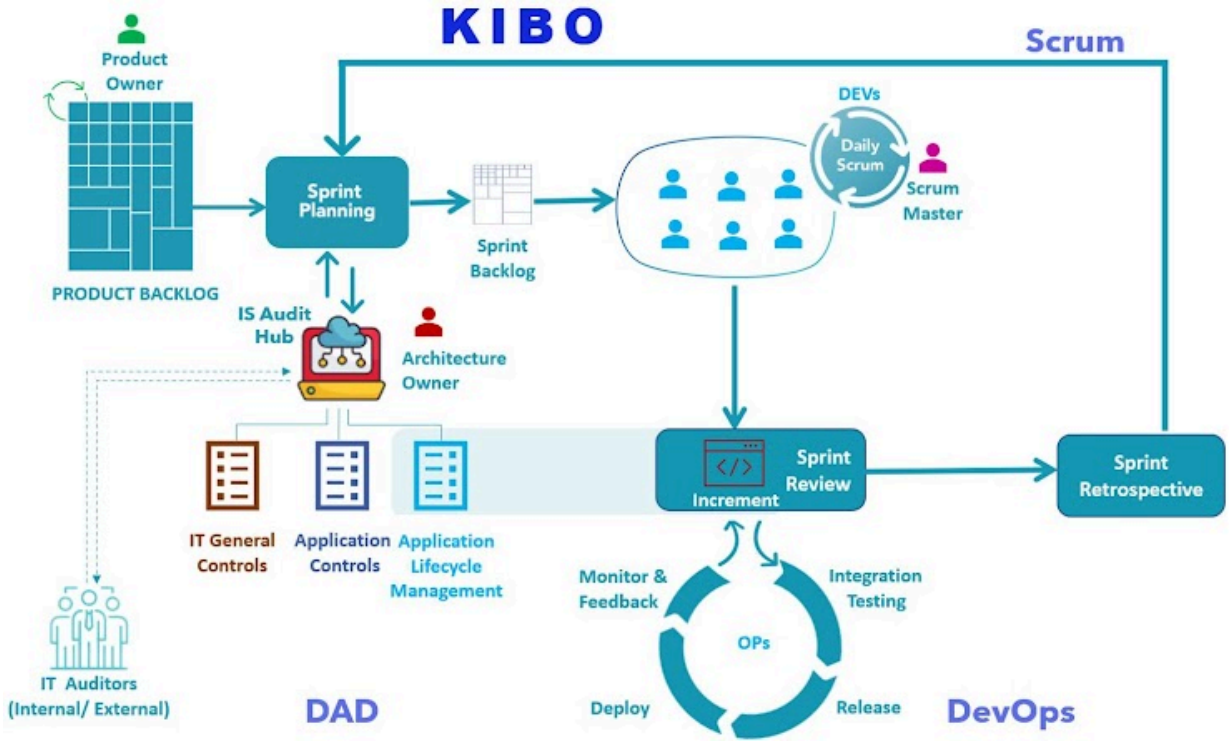
5. Monitor, Evaluate and Assess (MEA)

This domain addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements.

16. **5.1. Managed Performance and Conformance Monitoring *(MEA01)*** *

COBIT emphasizes the criticality of **collecting**, **validating**, and **evaluating** enterprise goals and metrics related to the SDLC.

KIBO practitioners expect a significant improvement in the validation and evaluation of goals, aligning with standard Scrum and DevOps practices. This is ensured by the Application and General IT controls set by the Architecture Owner, in harmony with the organization's business goals as brought in by the Product Owner.



Mark only one oval.

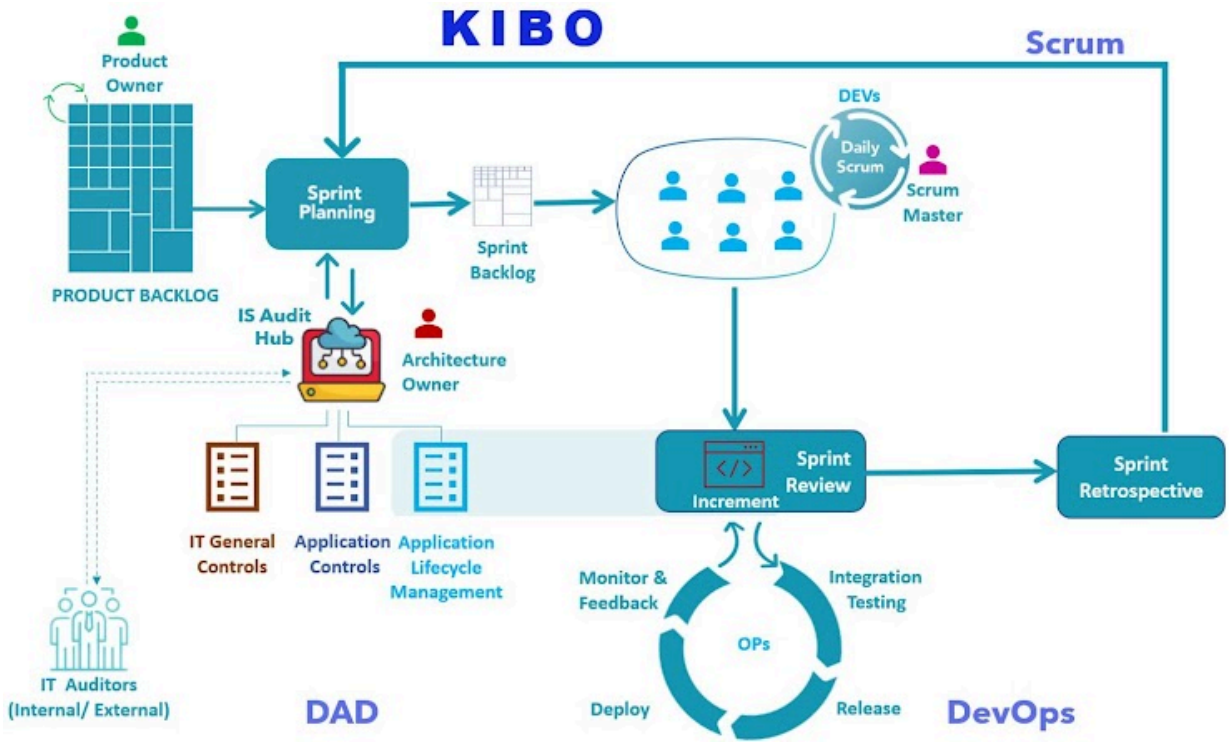
- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

5. Monitor, Evaluate and Assess (MEA)

17. **5.2. Managed System of Internal Control (MEA02)** *

COBIT recommends enabling management to **identify control shortcomings** and **initiate improvement actions**.

KIBO practitioners expect that the setup and maintenance of General IT and Application Controls serve to secure SDLC and deployment activities by identifying and addressing deficiencies and inefficiencies.



Mark only one oval.

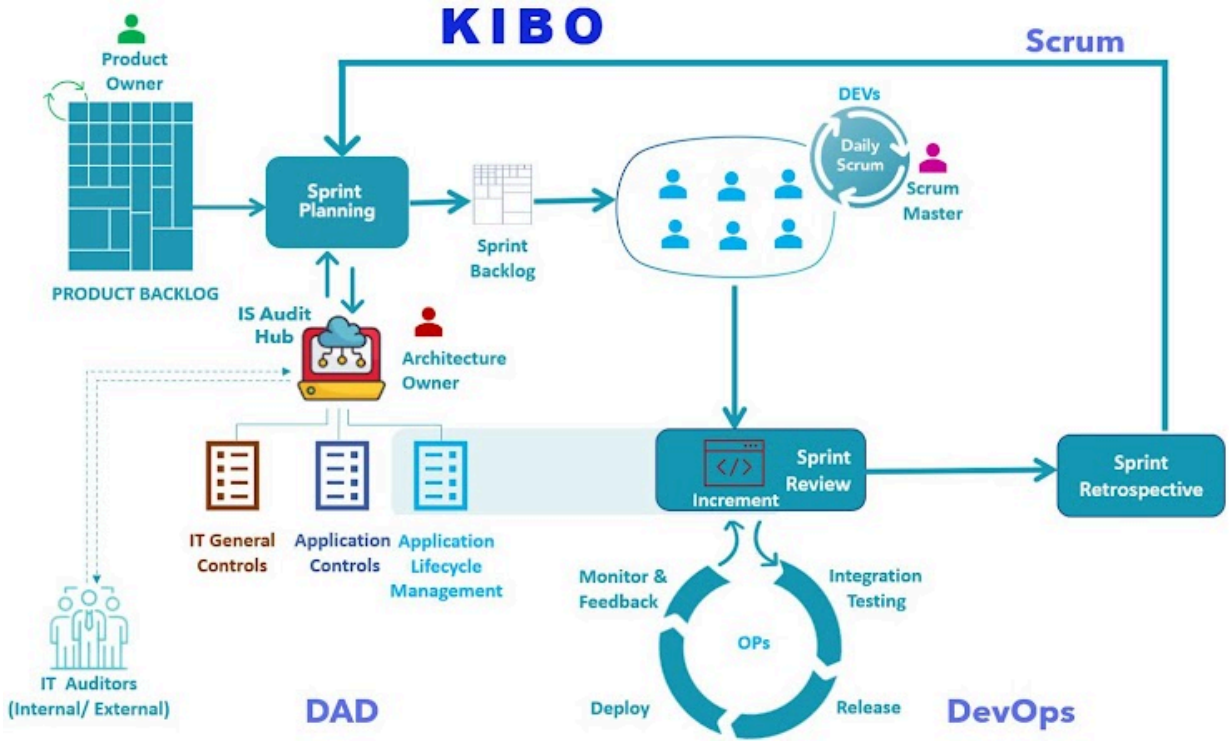
- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

5. Monitor, Evaluate and Assess (MEA)

18. **5.3. Managed Compliance with External Requirements** ***(MEA03)*** *

IT Governance indicates that SDLC processes and IT-supported business processes are **compliant with laws**, **regulations**, and **contractual requirements**.

KIBO practitioners expect that KIBO provides greater assurance of compliance with laws and regulations compared to stand-alone agile methods, given the pivotal role of the Architecture Owner in setting up and maintaining conformance to General IT and Application Controls.



Mark only one oval.

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

Please help us to better understand your background

19. Which role is more representative to your background? *

Mark only one oval.

- Business Analyst
- Project Manager
- Product Owner
- Scrum Master
- Software Developer
- IT Auditor/ Controller
- Security Engineer
- Delivery Lead
- Business Consultant
- Agile Coach
- DevOps Practitioner
- QA Engineer
- C-Level Executive
- Researcher/Academic
- Student
- Other: _____

20. How many years of professional experience do you have in your field? *

Mark only one oval.

- 0 years
- 1-3 years
- 4-6 years
- 7 years or more

21. What is your Academic background?

Mark only one oval.

- ◯ Graduate
- ◯ Postgraduate
- ◯ Doctorate
- ◯ Professor
- ◯ Other: _____

22. Please leave here any extra comment or remark you may have. (Optional)

_____

_____

_____

_____

_____