Scorecard: 11 API Governance Practices

Tick each process you do to find out how you rank.

1. Governance committee

Oversees API strategy and goals; signs off on priorities and approaches.

What to measure:

- Decisions
- Meeting frequency

1. Is membership defined?
2. Are there terms of reference?
3. Are there regular meetings?
4. Is there an agenda?

2. Style guide

Applies API consistency with design guidelines, e.g. how error messages should be returned.

What to measure:

- Number of page views
- Number of APIs built to style guide
- Key categories where APIs are designed outside of agreed style

1. Is there a documented style guide?
2. Is it published to an intranet/portal?
3. Are teams required to use the style guide when designing APIs?

3. OpenAPI specification file

Describes a machine-readable definition of an API that can be used in API design, testing and documentation.

What to measure:

- Proportion of APIs with an OAS or other specification file

1. Do all APIs have an OpenAPI or other specification file?

4. Platform team

Provides consistent resources across the enterprise, e.g. advice on API design lifecycle tooling.

What to measure:

- Number of support calls to platform team
- Platform team response speed to support
- Number of trainings provided

1. Is there a defined platform team with a clear action plan for developing resources?
2. Is there a support desk that tracks calls from business lines?
3. Do platform teams have insight into business line API roadmaps?

5. Security assessment checklist

Embeds security into API design and provides a mechanism for pre-deployment API governance reviews.

What to measure:

- Number of APIs rejected during approval processes due to lack of adherence with security processes

1. Is there a defined checklist?
2. At what stage of API design are security experts involved?
3. Are security measures described in the API specification file?

6. Regulatory assessment checklists

Complies with regulations through API design. It may be built as infrastructure-as-code and included in CI/CD processes.

What to measure:

- Number of APIs rejected during approval processes due to lack of adherence

1. Is there a regulation list for APIs?
2. Are there design guidelines for API regulatory requirements?
3. Are there processes that automatically monitor if regulatory requirements are being met?

7. Enablement team

Supports use of the style guide with capacity to link to key expertise such as risk management, security and data protection.

What to measure:

- Number of requests received
- Resolution speed

1. Is there a process for building an enablement team?
2. Are there clear processes for an enablement team to mentor and support a team developing APIs for the first time?

8. Internal developer portal and API catalog

Publishes a range of self-serve supports such as documentation, notes on API design and roadmaps, access to internal directories of enablement teams.

What to measure:

- Permission denials due to attempts to use APIs without authorization
- Reuse of APIs
- Reduction in duplicative APIs
- Shadow APIs/API discovery risks identified from undocumented APIs

1. Is there an internal-facing developer portal in place?
2. Are there resources for internal teams to understand how to build APIs?
3. Are all APIs described consistently?

9. External developer portal and API catalog

Offers self-serve mechanisms for third parties and partners to access open APIs to build new integrations and products.

What to measure:

- Number of APIs listed
- Number of visits
- Number of support queries resolved by using developer portal
- Time it takes for external developers from first making use of external APIs to applying for production use

1. Is there an external-facing developer portal in place?
2. Are there resources for external developers to get started?
3. Are all APIs described consistently?

10. Automated CI/CD processes

Implements CI/CD automated testing during build and deployments to ensure alignment with specifications, including appropriate security restrictions.

What to measure:

- Proportion of builds rejected
- Time taken to address build rejections
- Common reasons for build rejections

1. Are API specification files built into CI/CD processes?
2. Are there mechanisms to test security and regulatory adherence in CI/CD pipelines?
3. Are there clear triage processes if testing and build are stalled?

11. API standardized templates

Provides standard API patterns to any line of business, which are then extended to meet specific subject matter needs (e.g. loan application form).

What to measure:

- Speed new APIs can be designed and deployed
- Number of errors reviewed during testing and build phases

1. Is there an organization-wide taxonomy of the most common functionalities used in APIs?
2. Are there common patterns for common functions (e.g. search, forms)?

Calculate Reset Form

Score :

What your score means:

Under 15:

Take a step back from API creation to establish a platform team to guide consistent design patterns. Create a style guide and a standard OpenAPI specification file. Build a business case to describe the security, regulatory, and revenue risks that come with not having clear governance processes in place.

16- 25:

You have good governance processes in place. To move away from bureaucratic manual processes, focus on embedding these into the design and build processes.

26-30:

Congratulations! Your institution has strong governance processes. Speak with marketing and other business lines about how to leverage strong governance as a business capability.