Flow Down or Fall Down:

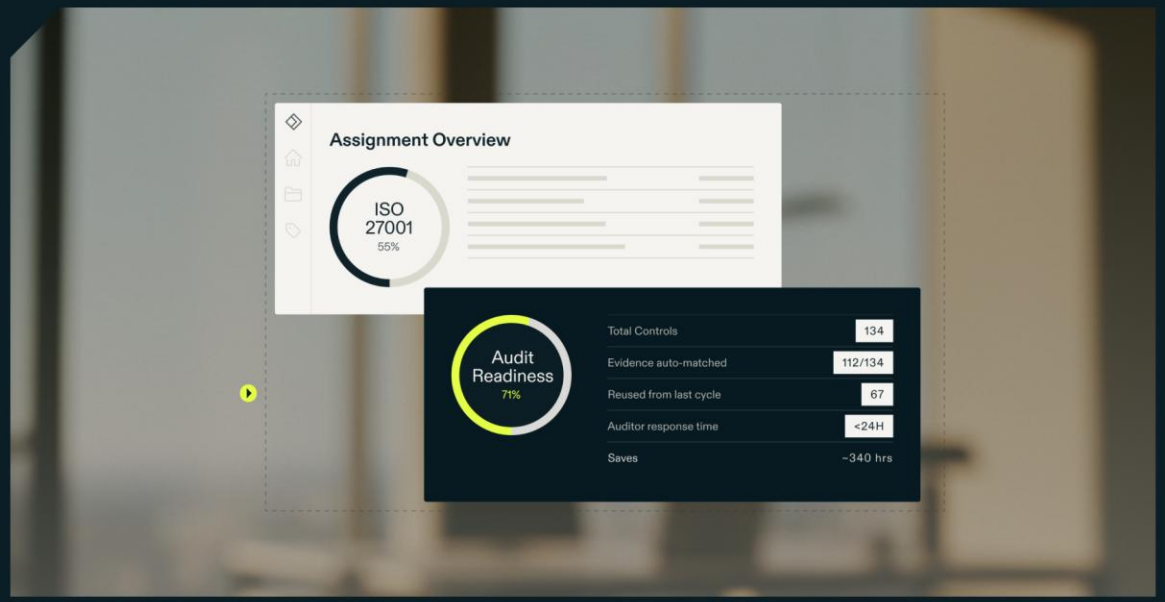
The Affirming Official's Supply Chain Challenge

The Most Important Role in Your CMMC Program Nobody Talks About

Michael Brooks, LCCA, CCI, CISSP

A-LIGN

www.a-lign.com



About me

Michael Brooks

CMMC Strategy and Engagement Director, A-LIGN

CIO | 2X CISO | IT Director | Lt Col, USAF (Ret.)
100+ NIST 800-171 and CMMC L2 Assessments

© 2026 A-LIGN. All Rights Reserved.

Quality reports, every time

A-LIGN is your trusted compliance partner. We are the market leader in efficient, quality compliance.

- Top SOC 2 issuer in the world
- Top ISO certification globally
- Top HITRUST assessor
- Top 3 Federal assessor
- C3PAO for CMMC
- 20+ years of experience

96%

customer satisfaction

A-LIGN

© 2026 A-LIGN. All Rights Reserved.

The One Question?

© 2026 A-LIGN. All Rights Reserved.

How do I know?

This is the most important question an Affirming Official can ask.

Affirming Official. *The Affirming Official is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the specified security requirements for their respective organizations.*

© 2026 A-LIGN. All Rights Reserved.

The 5Ws + How

- What is an Affirming Official?
- Why does it matter?
- Who should it be?
- Where do they sit?
- When should they engage?
- How do they establish confidence?

WHAT: Affirming Official

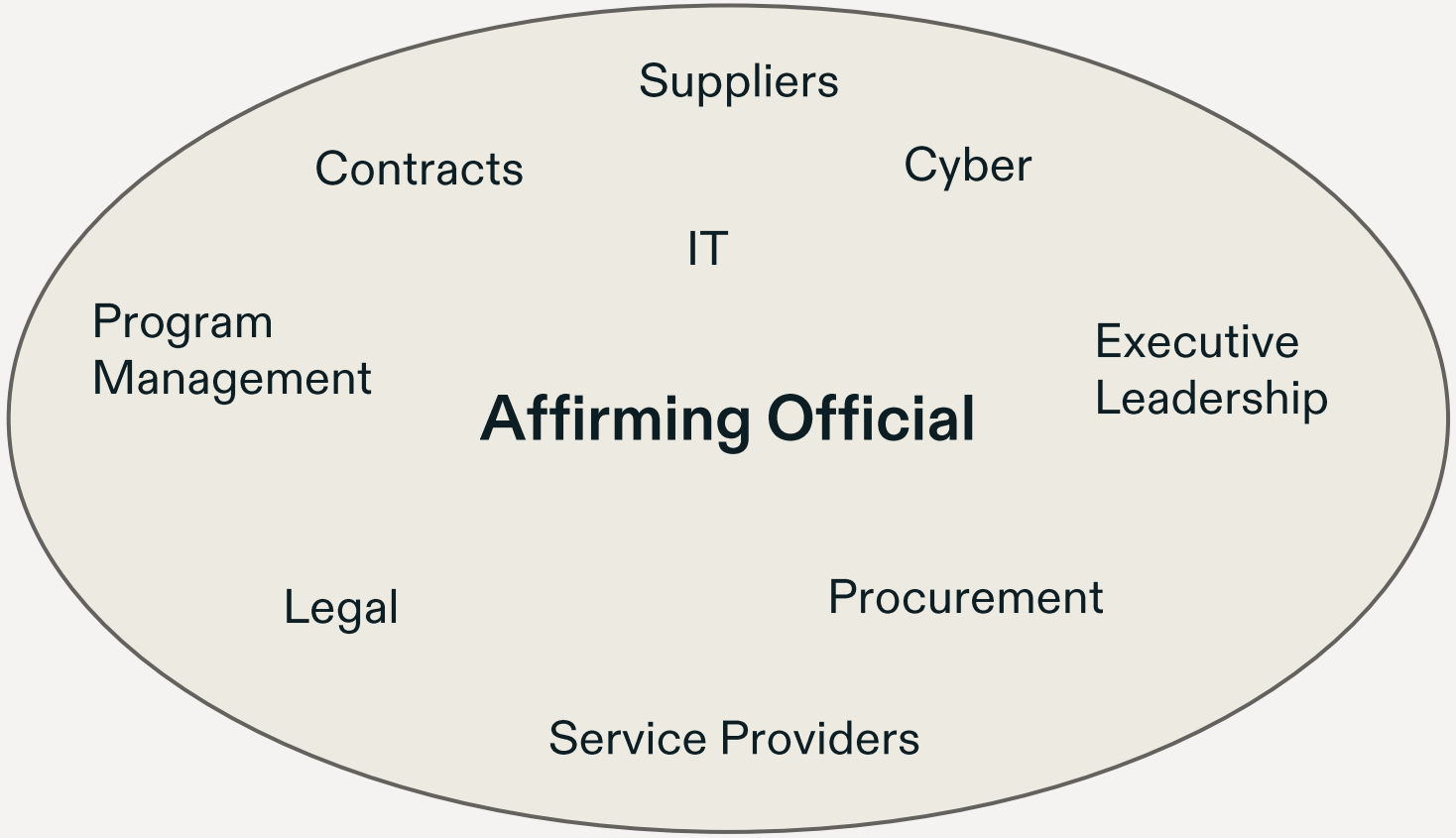
- **Assessment:** Did we meet the requirements? Self or third-party evaluation.
- **Affirmation:** Can we defend our continuous compliance posture? Leadership decision and declaration.

§ 170.22 Affirmation.

(a) ***General.*** The OSA must affirm continuing compliance with the appropriate level self-assessment or certification assessment. An Affirming Official from each OSA, whether a prime or subcontractor, must affirm the continuing compliance of their respective organizations with the specified security requirement after every assessment, including POA&M closeout, and annually thereafter. Affirmations are entered electronically in SPRS. The affirmation shall be submitted in accordance with the following requirements:

(1) ***Affirming Official.*** The Affirming Official is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the specified security requirements for their respective organizations.

WHY: CMMC is a Business Posture



Organization Seeking Certification

- Cross functional leadership
- Organizational focus
- Not a control implementer

(2) ***Affirmation content.*** Each CMMC affirmation shall include the following information:

(i) Name, title, and contact information for the Affirming Official; and

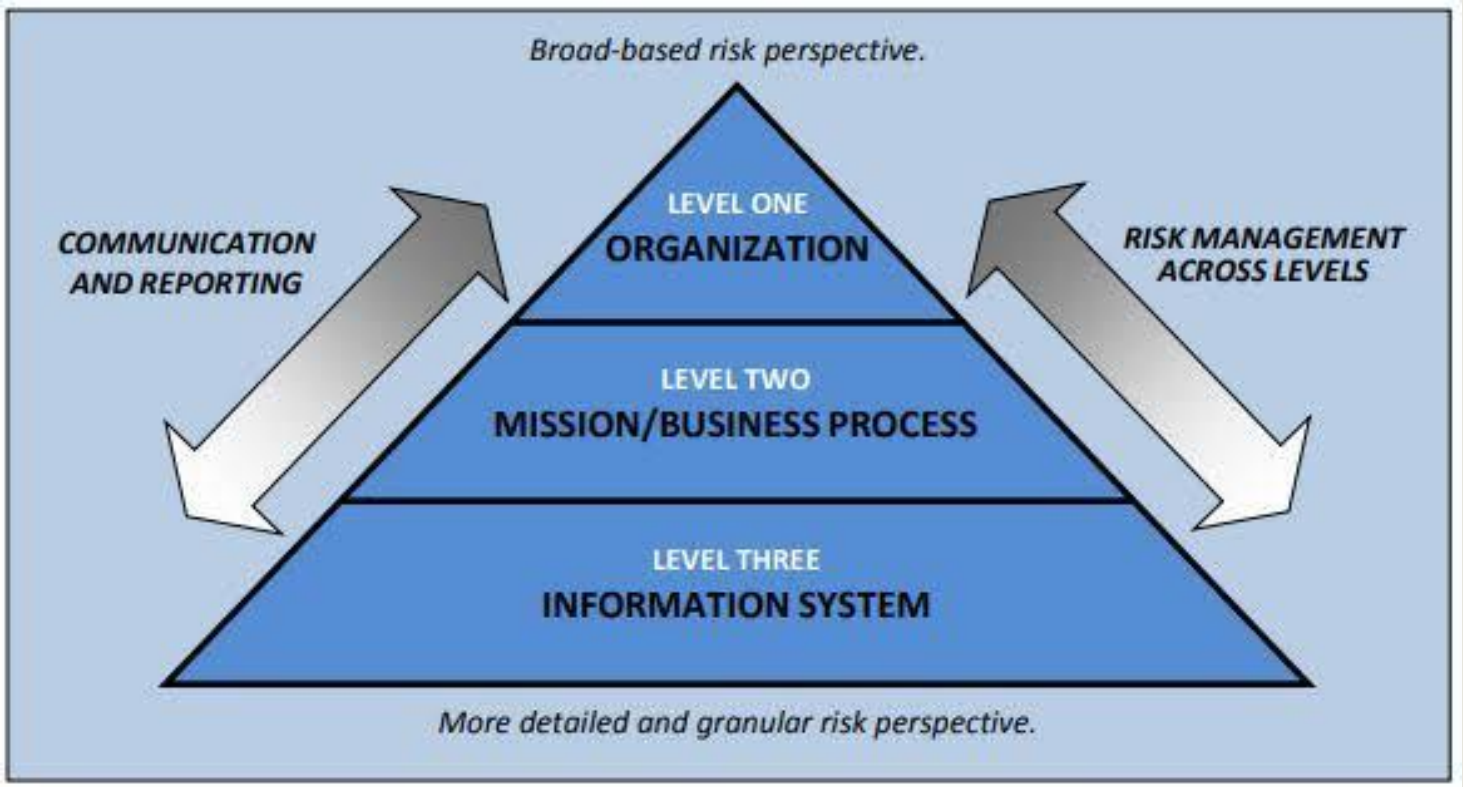
(ii) Affirmation statement attesting that the OSA has implemented and will maintain implementation of all applicable CMMC security requirements to their CMMC Status for all information systems within the relevant CMMC Assessment Scope.

WHO: The Four Tests

- ✓ **Authority** – Can they decide and direct?
- ✓ **Visibility** – Can they make informed decisions?
- ✓ **Access** – Can they engage where and when needed?
- ✓ **Accountability** – Can they own and defend the outcome?

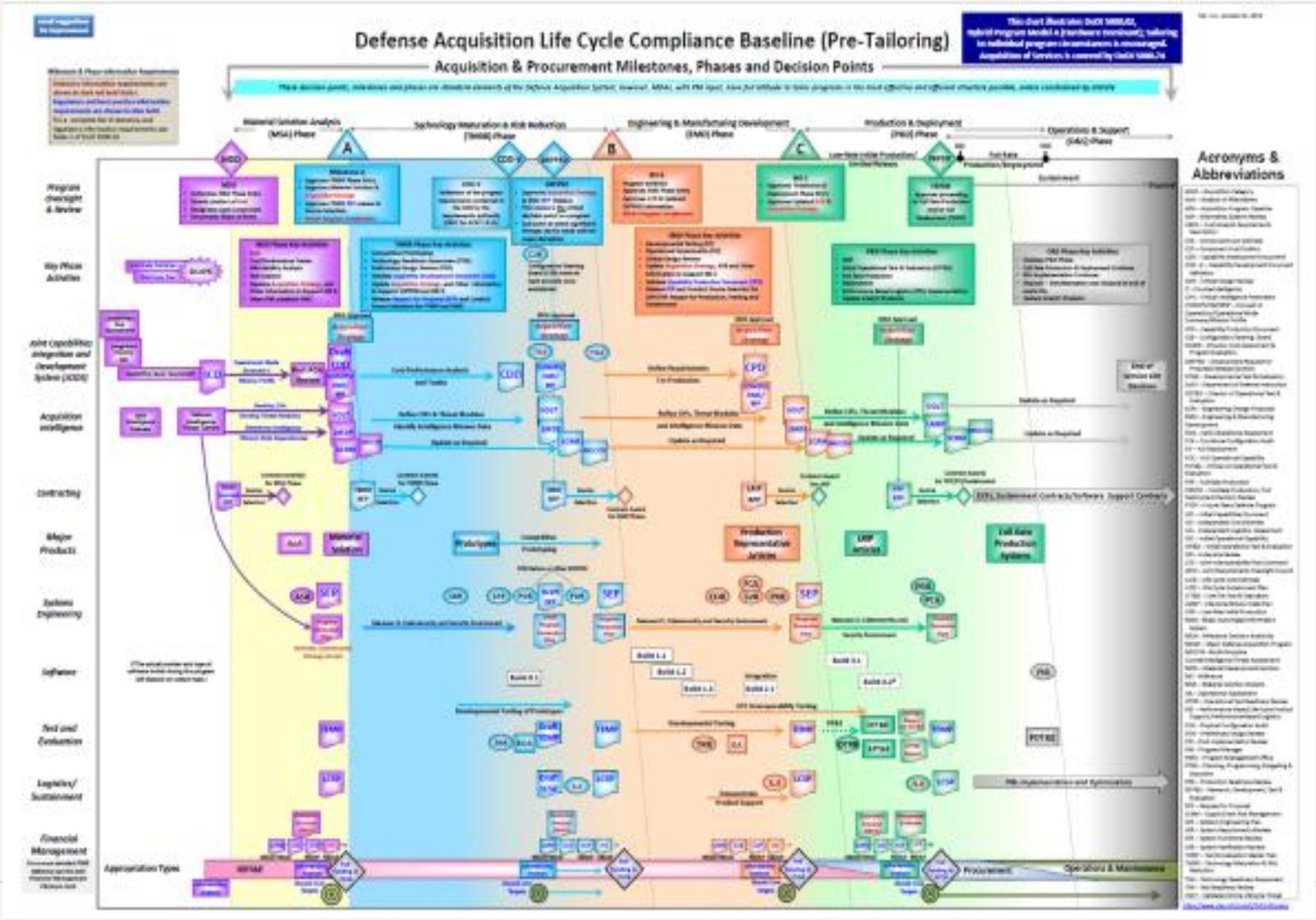
WHERE: Above the Program

- Governance function
- Not administration
- Executive accountability
- Ability to challenge
- Allocate resources / priority



WHEN: Earlier Than You Think

- Across the lifecycle and supply chain
- Bid -> Award -> Performance
- Continuous compliance
- Condition of performance
- Contractual obligation



CMMC Is A Business Decision

- ✓ Can we win it?
- ✓ Can we perform it?
- ✓ Can we protect it?
- ✓ Can we defend our position?
- ✓ Trust and investment not bolt on

Photo: Air Force Research Laboratory

Flow Down

- Validated CUI data flow
- Supplier access model
- Requirements focus (investment)
- Verified status
- Performance and Change Mgmt
- Engaged AO

Fall Down

- Unknown CUI data flow
- Supplier access uncontrolled
- Compliance focus (cost)
- Unverified status
- Ad hoc Performance and Change Mgmt
- AO ambiguity / not engaged

© 2026 A-LIGN. All Rights Reserved.

The Affirming Official Origin Story

Modeled after RMF Authorizing Official.

The most important thing to know about the AO is **accountability**. If the system gets hacked or loses data later on, the AO is the person who has to answer for it. Because this job is so important, they cannot pass this final decision-making power to anyone else.

Prepare	Essential activities to **prepare** the organization to manage security and privacy risks
Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis
Select	**Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
Implement	**Implement** the controls and document how controls are deployed
Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to **authorize** the system (to operate)
Monitor	Continuously **monitor** control implementation and risks to the system

© 2026 A-LIGN. All Rights Reserved.

Legal and regulatory implications

© 2026 A-LIGN. All Rights Reserved.

The False Claims Act is Active

Companies have faced penalties for overstating their cybersecurity compliance. Examples:

$4.6M

Amount Morse Corp paid after failing to meet NIST SP 800-171 standards and **reporting false SPRS scores**[1]

+

$11M

Amount Health Net Federal Services settled for over **false cybersecurity claims.**

[1]Source: US Attorney's Office, 2025 ; Office of Public Affairs, 2025

Where affirmation lives

Affirmation sits at the intersection of:

- Contracts
- Regulatory compliance
- Prime contractor trust
- DoD mission assurance

Affirmation is not an internal memo

It informs:

- Contract eligibility
- Prime contractor risk decisions
- Government confidence
- FCA exposure

© 2026 A-LIGN. All Rights Reserved.

When affirmation applies

Affirmation is required:

- After self assessment or certification
- After POA&M closeout (if applicable)
- Every year thereafter

© 2026 A-LIGN. All Rights Reserved.

When affirmation applies

If the score submitted to the government is incorrect, the consequences are severe:

- Legal exposure under the False Claims Act, a powerful federal law that holds individuals and organizations accountable for defrauding federal programs
- Contract risk, reputational damage, and financial penalties
- Personal risk for you as the Affirming Official

© 2026 A-LIGN. All Rights Reserved.

Common mistakes

© 2026 A-LIGN. All Rights Reserved.

Common mistakes

The mistakes are rarely technical. They're about ownership, timing, and how much the person signing actually knows.

- **Mistake 1:** Treating affirmation as a signature, not a decision
- **Mistake 2:** Assuming last year's assessment still holds
- **Mistake 3:** No process between assessments
- **Mistake 4:** Waiting until the deadline to look

© 2026 A-LIGN. All Rights Reserved.

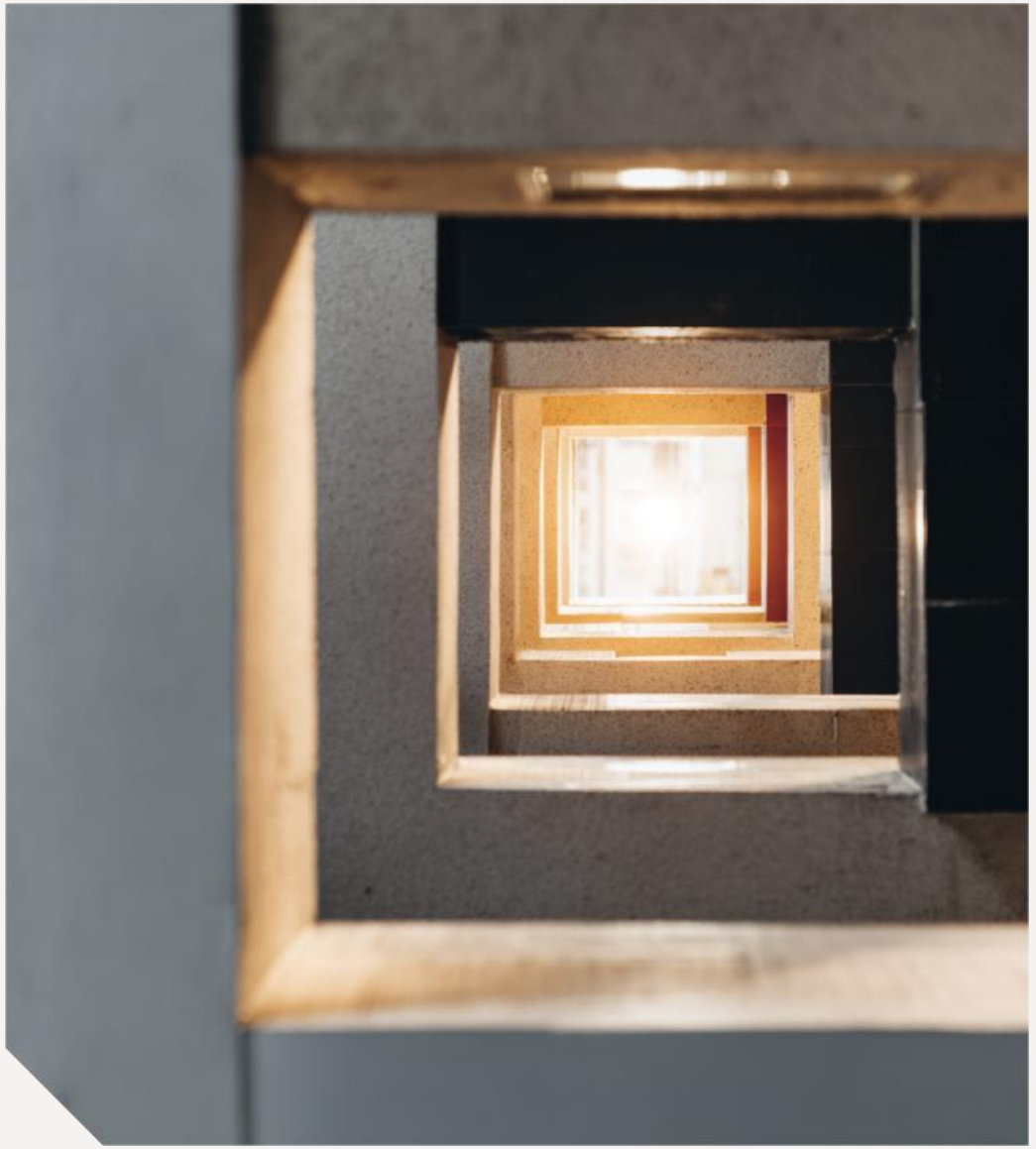
Establishing a sustainable annual process

© 2026 A-LIGN. All Rights Reserved.

How to establish an annual process

A sustainable process turns affirmation from an annual scramble into a routine checkpoint.

- Build an affirmation cadence
- Establish clear ownership before you need it
- Monitor continuously, not just annually
- Run an internal review before you affirm
- Brief the affirming official properly
- Partner for ongoing assurance



© 2026 A-LIGN. All Rights Reserved.

Thank you!

© 2026 A-LIGN. All Rights Reserved.