Category

Enterprise Transformation

Data Privacy, Security & Compliance in Digital Programs Playbook

Building privacy and security in from day one, not retrofitting it after the program is already built

- Executive
- Advanced
- Template Included

- Mithun A. Sridharan

- 19 August 2021
- 4 minute(s)

Overview

A framework for embedding data privacy, security, and regulatory compliance into digital transformation programs from the outset — privacy-by-design and security-by-design practices that avoid the far higher cost and risk of retrofitting compliance after systems are already built and live.

Can't privacy and security compliance be added later once the

digital program proves its value? Retrofitting privacy and security into a live system is significantly more expensive and riskier than building it in from the start — data flows, architecture decisions, and vendor relationships already established are often difficult and

costly to unwind once compliance gaps are discovered.

Who should own privacy and security in a digital transformation

program — legal, IT, or the program team? All three need genuine involvement, but the program team needs to treat privacy and security as design requirements from the outset, not issues to hand off to legal or security for review at the end.

{ "@context": "https://schema.org", "@type": "FAQPage", "mainEntity": [{ "@type": "Question", "name": "Can't privacy and security compliance be added later once the", "acceptedAnswer": { "@type": "Answer", "text": "digital program proves its value?\nRetrofitting privacy and security into a live system is significantly\nmore expensive and riskier than building it in from the start — data\nflows, architecture decisions, and vendor relationships already\nestablished are often difficult and costly to unwind once compliance\ngaps are discovered." } }, { "@type": "Question", "name": "Who should own privacy and security in a digital transformation", "acceptedAnswer": { "@type": "Answer", "text": "program — legal, IT, or the program team?\nAll three need genuine involvement, but the program team needs to treat\nprivacy and security as design requirements from the outset, not issues\nto hand off to legal or security for review at the end." } }] }

Subscriber access

Unlock this playbook

This playbook — including every framework, template, and step-by-step section — is available free to Think Insights subscribers. Enter your email to unlock it instantly and get our weekly insights newsletter. No account needed, and access is remembered on this device.

First Name

Last Name

Email

Country - Select -

■ I agree to data processing in accordance with GDPR

Submit

Leave this field blank

References

Related playbooks

Enterprise Transformation

AI-Driven Digital Transformation Strategy (Beyond Efficiency) Playbook

A framework for AI-driven digital transformation strategy that pursues genuine capability and business model change — new products, new customer experiences, ne

- Executive
- Advanced
- Template Included

Read playbook

Enterprise Transformation

Cloud FinOps & Digital Cost Management Playbook

A framework for establishing FinOps practice — visibility, accountability, and optimization — so cloud and digital infrastructure costs scale predictably with b

- Practitioner
- Intermediate
- Template Included

Read playbook

Enterprise Transformation

Data-Driven Product & Subscription Business Transformation Playbook

A framework for transforming toward data-driven product and subscription business models — using usage data to continuously improve the offering and justify rec

- Executive
- Advanced
- Template Included

Read playbook

Talk to us about privacy-by-design

Tags

- Data Privacy
- Security
- Compliance

Author

Mithun A. Sridharan Thought Leader

I'm Mithun A. Sridharan, Founder of this website - Think Insights - on Strategy, Management Consulting, Leadership, Digital Transformation, and Data Literacy. Follow me on social media or connect with me on LinkedIn for updates.