Category

Digital Transformation

Cybersecurity & Digital Risk Management Playbook

A structured method for mapping digital risk exposure to business impact and building a board-ready risk treatment plan.

- Executive
- Intermediate
- Template Included
- Workshop Ready

- Mithun A. Sridharan

- 27 January 2023
- 8 minute(s)

Overview

A practical framework for CIOs and CISOs to quantify digital risk in business terms, prioritize remediation with limited budget, and report exposure to the board with confidence.

How is this different from a standard penetration test or compliance audit?

A pen test or audit produces a list of technical findings scored by severity. This playbook adds the missing layer: translating those findings into business impact so leadership can prioritize a finite budget against the risks that actually threaten revenue, safety, or regulatory standing, rather than treating every finding as equally urgent.

Do we need a mature security program before we can run this workshop?

No. The workshop works with whatever findings you already have, even an incomplete vulnerability scan and a rough asset list. The first pass will be imperfect; its value is in creating a shared, prioritized starting point rather than waiting for a perfect data set that never arrives.

Who should own the Digital Risk Register after the workshop?

The CISO owns the operational upkeep, but risk acceptance decisions belong to the business unit leader whose process or system carries the risk, ratified by the Digital Risk Committee. Ownership sitting solely with IT security is the most common reason registers go stale.

How do we handle risk from third-party vendors and SaaS platforms?

Include vendor and SaaS-hosted systems in the asset-to-process map on equal footing with internally hosted systems, and score them using vendor security questionnaires, SOC 2 reports, or breach history in place of internal scan data. Vendor risk is frequently under-scored because it's invisible to internal vulnerability scanners.

How often should the heat map actually change the remediation roadmap?

Expect meaningful movement each quarter as remediation closes out top-quadrant items and new findings enter the register. If the heat map looks identical quarter over quarter, that's a signal the refresh session isn't rigorous enough, not that risk has stabilized.

{ "@context": "https://schema.org", "@type": "FAQPage", "mainEntity": [{ "@type": "Question", "name": "How is this different from a standard penetration test or compliance audit?", "acceptedAnswer": { "@type": "Answer", "text": "A pen test or audit produces a list of technical findings scored by severity. This playbook adds the missing layer: translating those findings into business impact so leadership can prioritize a finite budget against the risks that actually threaten revenue, safety, or regulatory standing, rather than treating every finding as equally urgent." } }, { "@type": "Question", "name": "Do we need a mature security program before we can run this workshop?", "acceptedAnswer": { "@type": "Answer", "text": "No. The workshop works with whatever findings you already have, even an incomplete vulnerability scan and a rough asset list. The first pass will be imperfect; its value is in creating a shared, prioritized starting point rather than waiting for a perfect data set that never arrives." } }, { "@type": "Question", "name": "Who should own the Digital Risk Register after the workshop?", "acceptedAnswer": { "@type": "Answer", "text": "The CISO owns the operational upkeep, but risk acceptance decisions belong to the business unit leader whose process or system carries the risk, ratified by the Digital Risk Committee. Ownership sitting solely with IT security is the most common reason registers go stale." } }, { "@type": "Question", "name": "How do we handle risk from third-party vendors and SaaS platforms?", "acceptedAnswer": { "@type": "Answer", "text": "Include vendor and SaaS-

hosted systems in the asset-to-process map on equal footing with internally hosted systems, and score them using vendor security questionnaires, SOC 2 reports, or breach history in place of internal scan data. Vendor risk is frequently under-scored because it's invisible to internal vulnerability scanners." } }, { "@type": "Question", "name": "How often should the heat map actually change the remediation roadmap?", "acceptedAnswer": { "@type": "Answer", "text": "Expect meaningful movement each quarter as remediation closes out top-quadrant items and new findings enter the register. If the heat map looks identical quarter over quarter, that's a signal the refresh session isn't rigorous enough, not that risk has stabilized." } }] }

- [ ] I agree to data processing in accordance with GDPR

Submit

Leave this field blank

References

Related playbooks

Digital Transformation

Telco Network & 5G/Edge Services Digital Transformation Playbook

A framework for telecommunications network and 5G/edge services digital transformation that identifies genuine new revenue and service opportunities enabled by

- Executive

- Advanced
- Template Included

Read playbook

Digital Transformation

AI & Digital Transformation Talent, Skills & Capability Building Playbook

A framework for building AI and digital transformation talent and capability deliberately — targeted skills assessment, structured capability building, and tale

- Executive
- Intermediate
- Template Included

Read playbook

Digital Transformation

Digital Transformation Risk, Resilience & Business Continuity Playbook

A framework for digital transformation risk, resilience, and business continuity planning that treats the transformation program itself as a source of operation

- Executive
- Advanced
- Template Included

Read playbook

Talk to our digital transformation team

Author

Mithun A. Sridharan

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.