Shadow IT

Assets that lurk in the dark!

- David Kohrell, NECERT 19FEB2025

Definitions and References

Risk = Threat x Vulnerability x Asset

ISSA, Managing Risk in Information Systems, 2022
Gibson & Igonor

FFIEC (banking) – Shadow IT

- Shadow IT refers to IT devices, software, or services operating within the entity's environment without the knowledge, approval, or control of IT management. Shadow IT can also be identified within a third-party service provider's environment. Unapproved devices, software, or services should not be running at the entity, but they could be placed there by the following:
  - Business units to support their specific needs in contravention to the enterprise's needs.
  - Third-party service providers to support services provided to the entity or to collect data for the service providers.
  - Individuals (internal or external) for convenience to allow them to use entity resources (e.g., wireless network) or for malicious purposes (e.g., to steal data or processing power).
  - Incomplete decommissioning process for legacy.

FFIEC Information Technology Examination Handbook Architecture, Infrastructure, and Operations JUNE 2021. III.B.3 Shadow IT

Failure to address the risks of shadow IT may lead to an unknown attack vector due to management's lack of awareness of unapproved devices, software, or services. Therefore, management should understand and communicate the following risks of shadow IT to the entity's personnel:

FFIEC Information Technology Examination Handbook Architecture, Infrastructure, and Operations JUNE 2021. III.B.3 Shadow IT

FFIEC (banking) – Shadow IT

- Security weaknesses, data breaches, or data loss from using unapproved devices, software, or services.
- Inability to maintain or update (e.g., apply patches to) unknown devices or software resulting in vulnerable devices or software.
- Costs related to identifying, diagnosing, and mitigating security issues. • Inability to back up and recover unknown devices or software.
- Unintentionally performing automatic backups of unapproved and possibly infected devices or software leading to the spread of malware.
- Penalties for using software or services without a license.
- Legal risks related to data use or data ownership.
- Potential nullification of cyber insurance.

FFIEC Information Technology Examination Handbook Architecture, Infrastructure, and Operations JUNE 2021. III.B.3 Shadow IT

“Navigating the Shadows” ISACA

Shadow IT must be distinguished from business-managed IT. The former involves IT solutions adopted without the IT department’s knowledge, while the latter refers to sanctioned but externally managed IT solutions.

Navigating the Shadows: A Comprehensive Framework for Anticipating, Identifying, and Managing Shadow IT, Spivey and Mcilveene 1NOV24, ISACA

Practice

Shadow and Light IT- 2019-22

IS/IS Pilot – Application Focus

- Over 600 Apps ID
- CASB ID up to 6,000

Asset Management was “MEH”

- Focus had been on top 200
- Things that were purchased
- Assumption Black- and Whitelist did it

Aha’s

- “Light” was biggest offender
- People use What’s App, Survey Monkey and all sorts of things they’re not supposed to
- 10% coverage allows for a lot of improvement!
- Meld into Cyber clean and longer-term efforts

BANK OF THE WEST
BNP PARIBAS

Shadow IT for an Insurance Company Not in Nebraska - 2022

Internal Audit (3LOD) said do it

- Board level issue
- Concerns about risk

1LOD ran with Business Led IT

- Wasted effort on Visual Basic use from 2014-22
- Ignored and didn't understand IoT, OT, Servers, 3rd Party
- Went back to comfort zone

Aha's

- Program abandoned and awaits another audit finding

Pharma and OTC

OT and IT

- I want to run a plant is strong #1
- Manage IT yes, but see #1

Systems and applications

- Often missed in traditional IT
- OT Segmentation challenges

Aha’s

- Clarody is sweet
- Shadow Asset Management lives in a much bigger world

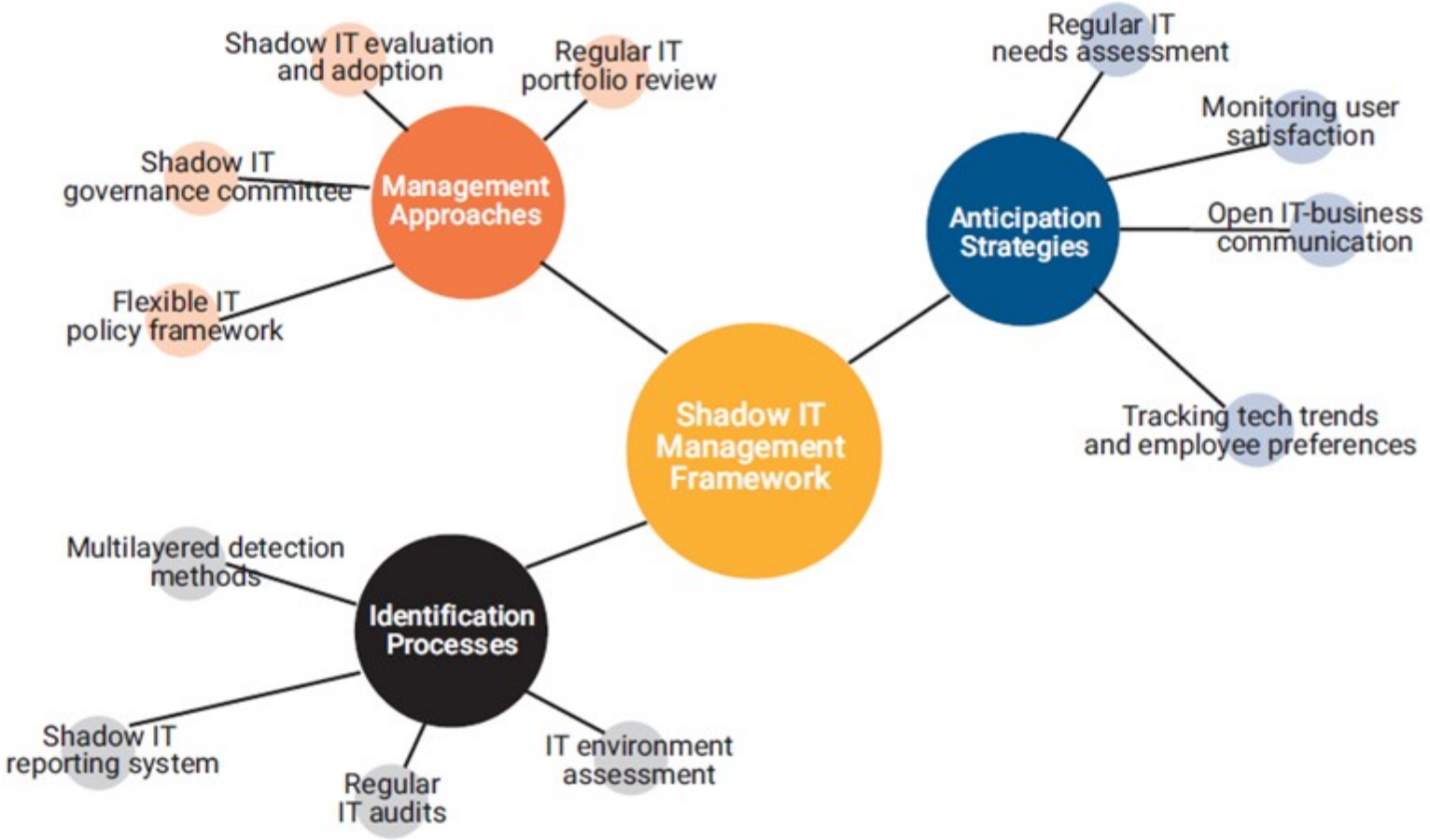
Solutions

Navigating the Shadows

KOHRELL
Strategy and Delivery

FIGURE 1

Proposed Shadow IT Management Framework



Navigating the Shadows: A Comprehensive Framework for Anticipating, Identifying, and Managing Shadow IT, Spivey and Mcilveene 1NOV24, ISACA

Checklist

Business purpose and understanding

Show me your configuration management database CMBD: SNOW, Cherwell, HP, etc.

Show me your Splunk, SharePoint, Spreadsheet or other if your managed assets there as well

List of third party, vendors and cloud

AI and the Gen’s

I’ll inspect as well. CASB, Clarody

Let’s organize, prioritize and solve!

NEbraskaCERT's Wisdom

Contact

Shadow IT is Risky Business. Not the good kind either!

LINKEDIN – DKOHRELL
OR
1-402-429-9805

DAVID KOHRELL – DAVID@KOHRELL.ORG

HTTPS://WWW.KOHRELL.ORG

KOHRELL
Strategy and Delivery