



EDINBURGH  
JUNE 16-21  
**2019**

# Common Tabletop Exercise Failures

Michael Murray

Robert Lelewski

# Michael Murray

Senior Manager, Incident Response Consulting

## Secureworks' Security and Risk Consulting Incident Response (SRC-IR) Team



### About

- Over 15 years of experience in cyber security.
- Focused on delivering proactive incident response services that prepare our clients to act when an incident strikes by ensuring that they have defined, implemented, and exercised the necessary plans and processes, and by augmenting client incident management capabilities during an incident response event.
- Previously Technical Manager for the CSIRT Operations Team at the CERT Coordination Center, Carnegie Mellon University.
- Provided on-site support to U.S. national-level cyber centers to include US-CERT, the Department of Defense Cyber Crime Center (DC3), and Joint Task Force Global Network Operations (JTF-GNO).

### Previous Focus Areas

- Public / Private sector information sharing
- International cooperation, National-level CSIRT capability development
- Analysis infrastructure development and deployment
- Operational process and tooling improvements

### Passion for Security

- Coordinated collaboration amongst global network of CSIRTs with National Responsibility.
- Served on the Forum of Incident Response and Security Teams (FIRST) Board of Directors.
- North America FIRST membership committee representative.
- Has played a number of roles, starting as junior analyst triaging tickets and answering the CERT/CC hotline.
- “Team sport” focus – community, collaboration, information sharing.

# Robert Lelewski

Team Lead and Senior Consultant, Incident Response Consulting

## Secureworks' Security and Risk Consulting Incident Response (SRC-IR) Team



### About

- 15+ years in Information Security in a variety of client facing and management roles.
- Developed several incident response practices from the ground up.
- Expert witness testimony in state and federal courts on computer forensic issues.
- International consulting experience, enabling a wide view of unique cultural and legal issues.
- In-depth experience in applying the Incident Response Lifecycle to preparing for incidents via the development and review of incident response plans, facilitation of tabletop exercises, and the facilitation of lessons learned events.

### Previous Focus Areas

- Managed a flyaway incident response team, participating in high-profile breaches around the world.
- Primary investigator for the Colorado Public Defenders specializing in computer crimes and electronic evidence.
- Adjunct professor teaching courses on network security, computer forensics, and other topics.

### Passion for Security

- Possesses several security-related certifications including: SANS GCIH, CIPM, CISA, CISM, CRISC, CISSP-ISSMP, EnCE, CCE, CASP.
- MBA – University of Northern Iowa, MS – University of Denver, BS – Syracuse University.
- Speaker for major industry events including the IBM Security Summit in Mexico City, ISACA's CSX in Ghana, FIRST Annual Conference in Edinburgh.
- Regular featured contributor to ISACA's *The Nexus* journal on cyber security and risk management topics.
- Presented to boards and leadership circles on cybersecurity risks and the changing threat landscape.

# Background

Proactive IR consulting:

What we do,  
why we do this,  
why we care...

Why tabletops?

Where do they go wrong?

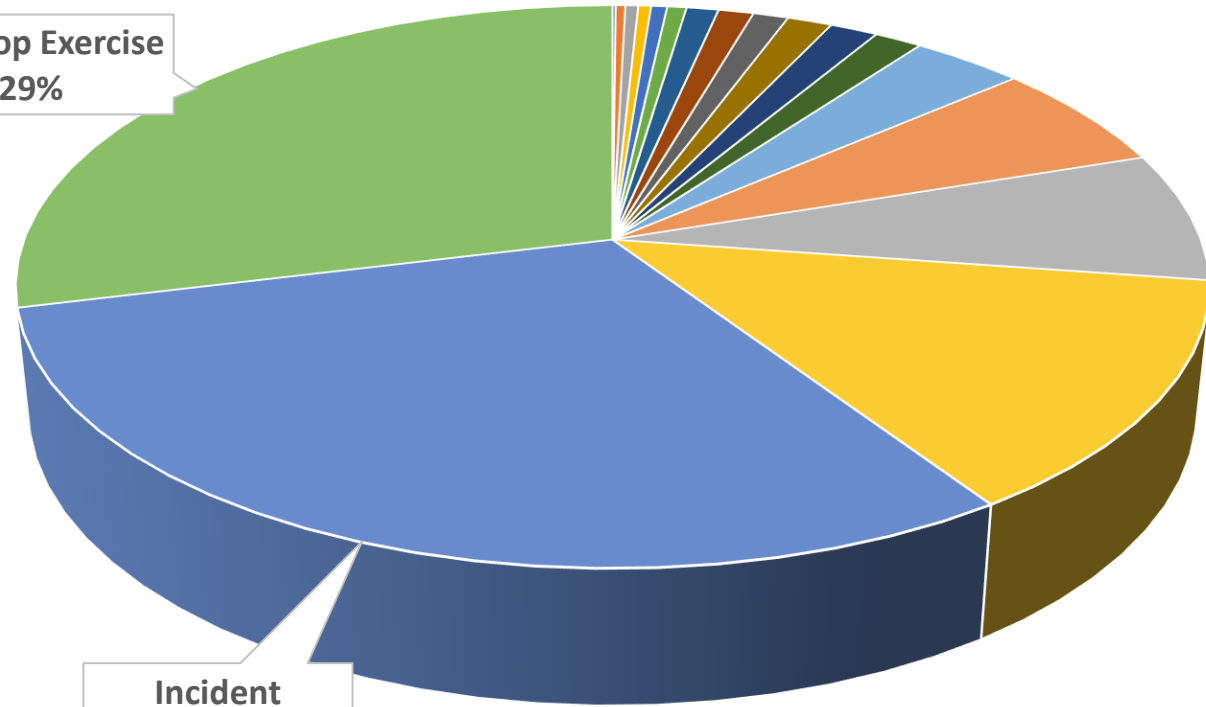


<https://www.zapiro.com/110120mg>

# RE: Secureworks Proactive IR Services

*We strive to prepare our clients to act when an incident strikes by ensuring that they having defined, implemented, and exercised the necessary plans and processes to respond to such events, and by supplementing their incident management capability during an incident response activity.*

Tabletop Exercise  
29%



Incident  
Response /  
Digital Forensics  
30%

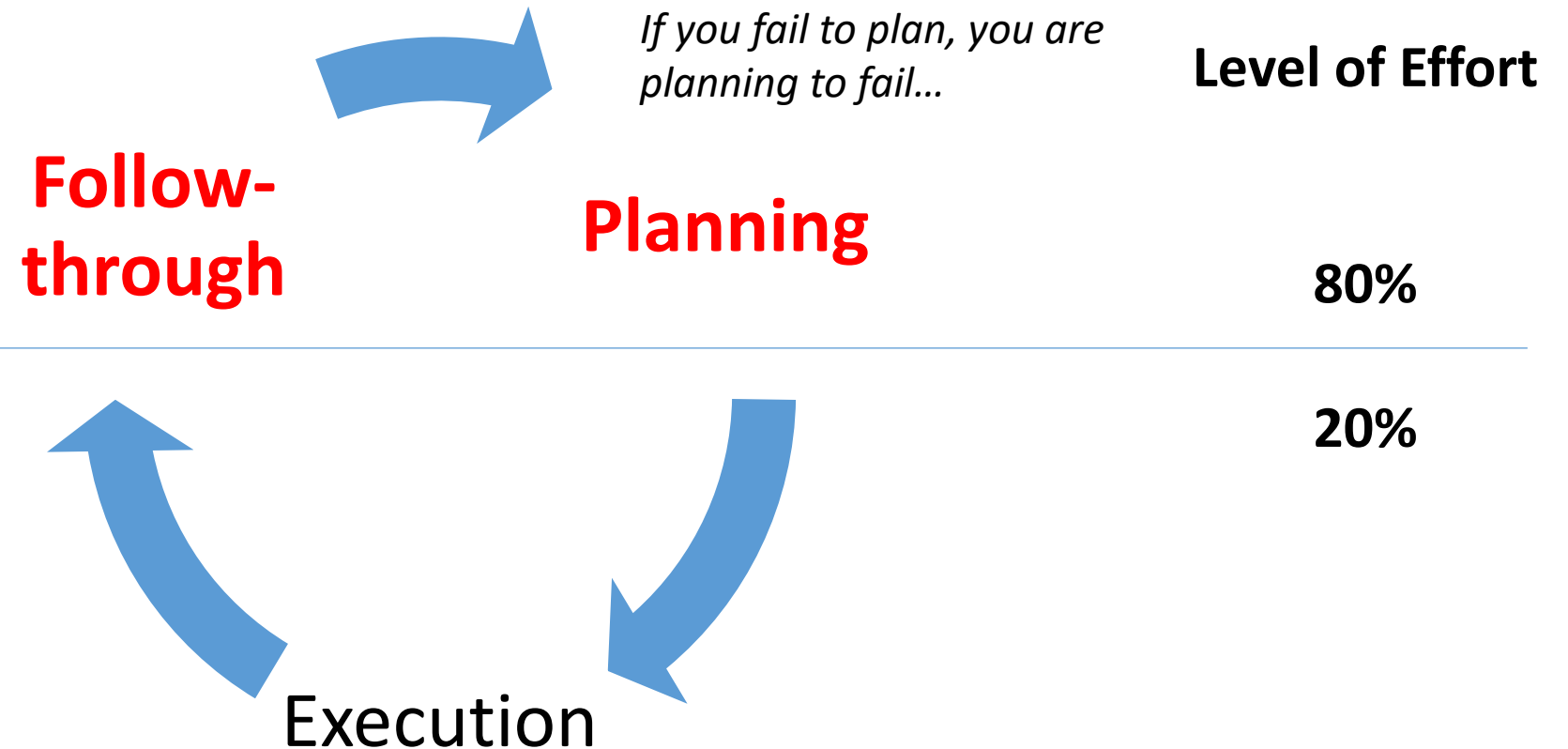


# Why Tabletops?

- Whether a plan and program is old or new, there is a need to regularly review and validate.
- Looking for unknown unknowns.
- Increasingly, clients/customers, insurers, and regulators requesting or requiring evidence of preparedness, or weighing repercussions on proof thereof.
- Building cross-organizational relationships and raising awareness / gaining support.
- Low-impact / high-ROI



# Where Exercises Go Wrong



**Let's get into some specifics...**





# Failure 1: The Need to Find the “Right” Answer

Take Off Those Blinders!

The value of a tabletop is not getting to a final answer. It is:

- getting everyone in the same room,
- discussing individual interests,
- taking time to explore unforeseen issues, and
- fostering communication paths.

When your sight is set on the “right” answer, you may lose the real value to be gained from a tabletop.



1

2

3

4

5

6

7

8



# Failure 2: Not Performing Cross-Functional Tabletops

It's not a party unless somebody invites Legal.



Typically the most valuable tabletop exercise.

Do prior-relationships exist between cross-functional roles?

Resistance to performing cross-functional tabletops.

Each function should be defined within the incident response plan.

Cross-functional tabletops  $\neq$  technical scenarios.

1

2

3

4

5

6

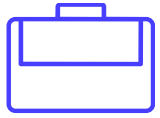
7

8



# Failure 2: Not Performing Cross-Functional Tabletops

It's not a party unless somebody invites Legal.



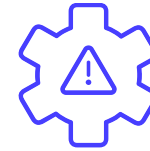
Legal



Media



Finance



Risk  
Management



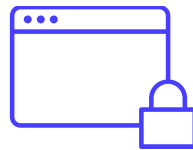
Physical  
Security



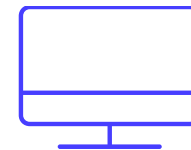
Executive  
Management



Audit



Information  
Security



Information  
Technology



Vendors

1

2

3

4

5

6

7

8

# Failure 3: Not Defining Tabletop Goals

What are you *really* trying to accomplish?

Tabletops may experience diminished value due to a lack of defined goals.

Before getting started, consider what are your goals for the tabletop?

Based on your goals, what is the most appropriate style of tabletop?



1

2

3

4

5

6

7

8



# Failure 3: Not Defining Tabletop Goals

What are you *really* trying to accomplish?

## Common Goals:

- Increase plan familiarity
- Determine the impact of incident response on a new process
- Regulatory compliance
- Highlight a known deficiency
- Test process against a new threat or involving a new stakeholder
- Rekindle / forge communication paths
- “Stress test”



1

2

3

4

5

6

7

8

# Failure 4: Not Capturing and Addressing Deficiencies

We're done. Off to the pub, right?



Capture feedback early – “hot wash” at the end to gather comments, solicit feedback via questionnaires, and provide your own assessment while it’s fresh in everyone’s mind. Remember – people get very busy again upon return to \$DAY\_JOB.

Reconvene the participants to discuss areas for improvement, assign, and track actions.

1

2

3

4

5

6

7

8

# Failure 4: Not Capturing and Addressing Deficiencies

We're done. Off to the pub, right?

Create a report that clearly identifies:

- What was observed
- Potential impact of the observation
- Recommended actions
- Assignee(s) to take action
- Priority / Due Dates
- Follow up on actions, host working sessions to discuss progress

Set check points to track progress.  
Re-exercise those areas.



1

2

3

4

5

6

7

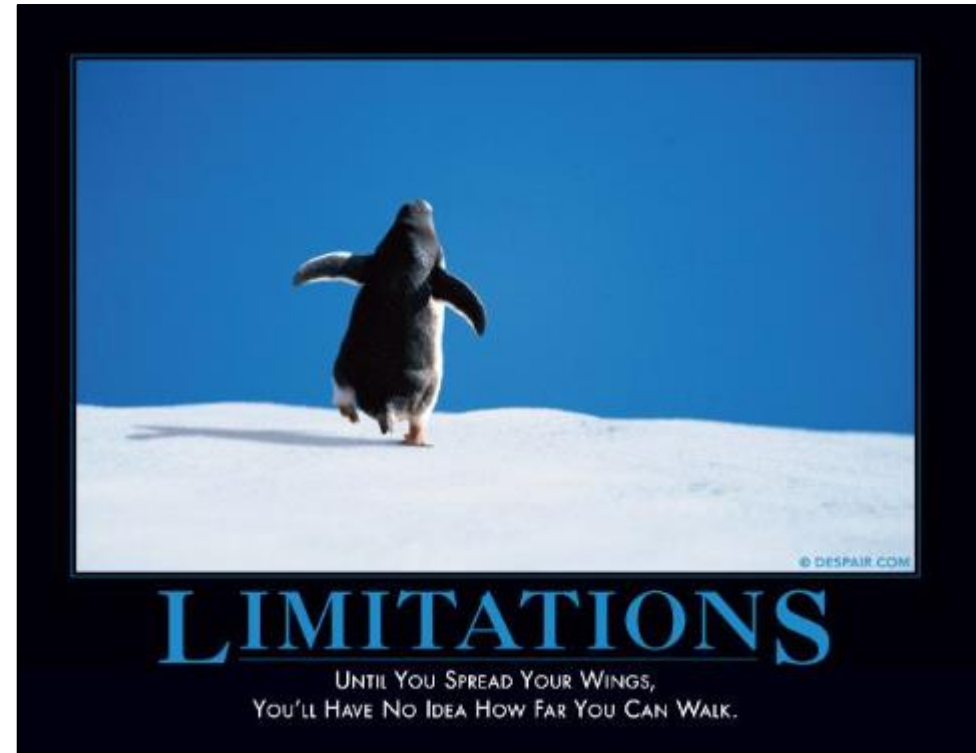
8

# Failure 5: Not Pushing Boundaries

Stop me if you've been in this exercise before...

Exercises are a means to expand the scope of your people, process, and technology assets.

For technologists, the prospect of a several hour long meeting may not be all that exciting, so it is important to drive interest in exercises by making them more interesting.



1

2

3

4

5

6

7

8





# Failure 5: Not Pushing Boundaries

Stop me if you've been in this exercise before...

## Easy to make it exciting...

- Take the “table” out of tabletop
- Valid domain account logging into many systems in a few seconds
- Introduce a non-trusted device
- Disable \$SECURITY\_COTROL on a box
- Simulate data exfiltration
- Call someone and report a “found device”
- Leverage Red Teamers
- Exercise known deficiencies to raise awareness and seek support

## Utilize disposable infrastructure

- Easier than ever to spin up and tear down infrastructure for exercises, education, etc.

## Engage external entities

- Providers (more to come on this one)
- Partners
- Clients / stakeholders

1

2

3

4

5

6

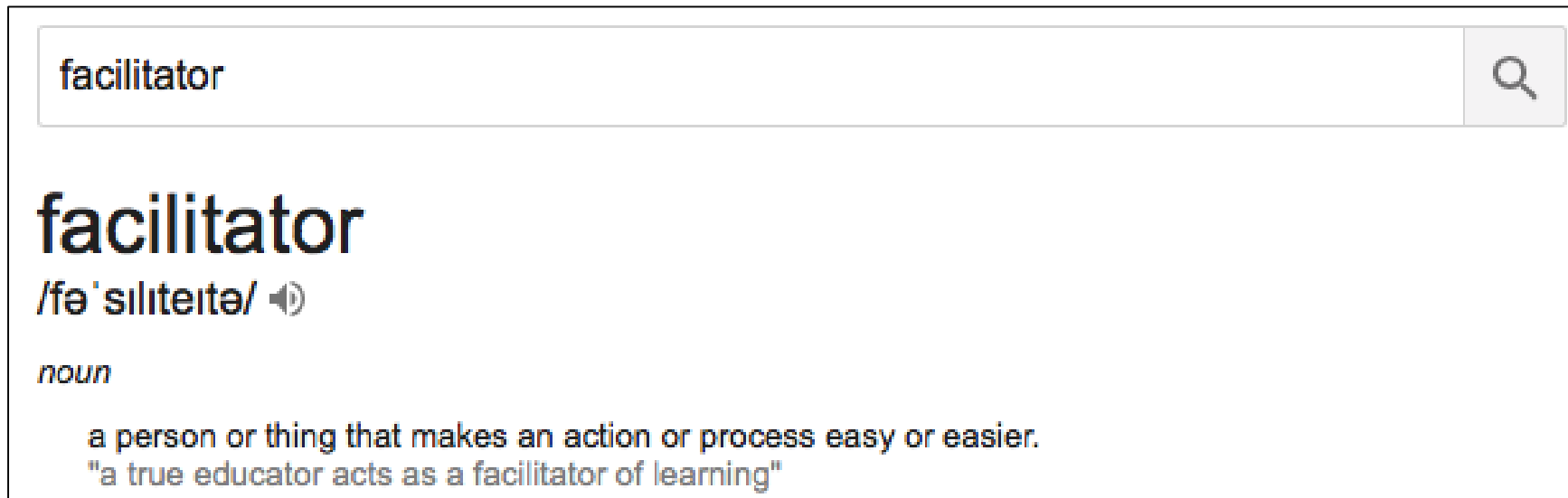
7

8

# Failure 6: Always Building and Facilitating Internally

Plug for the consultants in the room!

Internally facilitated tabletops are perfectly acceptable but should periodically be combined with leveraging external facilitators.



A screenshot of a search engine results page for the word "facilitator". The search bar at the top contains the word "facilitator" and a magnifying glass icon. Below the search bar, the word "facilitator" is displayed in a large, bold, blue font. Underneath, the phonetic transcription "/fə'silitetə/" is shown with a speaker icon. The word is identified as a "noun". The definition provided is "a person or thing that makes an action or process easy or easier." A quote is included: "a true educator acts as a facilitator of learning".

1

2

3

4

5

6

7

8

# Failure 6: Always Building and Facilitating Internally

Plug for the consultants in the room!

An external facilitator:

- Brings a wider perspective.
- Provides independent reporting to management.
- May help discover unknown points of failure.
- Is less likely to “sugarcoat” observations.
- Allows the usual event planners to participate.



1

2

3

4

5

6

7

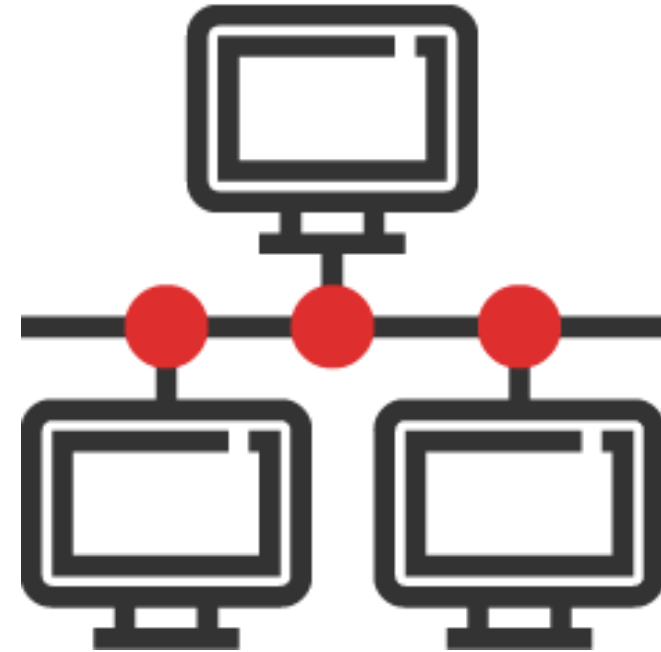
8



# Failure 7: Not Testing Vendors

Vendors always adhere to their SLAs. Always.

- Vendors are increasingly used to fulfill a variety of roles.
- Security compromises involving vendors are well known.
- Must be integrated into your incident response process.
- Starts with the SLAs.



1

2

3

4

5

6

7

8

# Failure 7: Not Testing Vendors

Vendors always adhere to their SLAs. Always.

Simple Vendor Exercise:

Pick a non-critical system operated by a vendor. Contact the vendor and state that, due to a security concern, the following data sets are requested:

- OS Event Logs
- RAM
- Disk Image

1

2

3

4

5

6

7

8



# Failure 8: Lack of Senior Leadership Participation

When the highest ranking person in the room is the intern, something went wrong.



Sometimes you need their help...

- ~~People~~
- ~~Process~~
- ~~Technology~~



You need their perspective on what matters and why to inform how and where you focus your efforts.

1

2

3

4

5

6

7

8

# Failure 8: Lack of Senior Leadership Participation

When the highest ranking person in the room is the intern, something went wrong.

Also an opportunity to showcase your team's capabilities...

Make sure that there is an appreciation for where you become reliant on other parts of the organization.

You are going to be "invited" to the board meeting one of these days.

<b>ONE ..WEEK.. ONLY.</b>	<b>Eighteenth and Douglas</b> One Week, Starting <b>MONDAY, JUNE 11</b>	<b>SEATS FOR ...2,000...</b>
<b>'PROF. GENTRY'S FAMOUS Dog and Pony Show.</b>		
		
The World's Best Trained Animal Exhibition. Every- thing New This Year.		
<b>275</b> <b>ARISTOCRATIC</b> <b>275</b> <b>ANIMAL ACTORS.</b>		
See Pinto and Nero, the Smallest Performing Elephants in Cap- tivity. Watch for the Grand Free Street Parade, Daily 10:30a.m		
<b>Matinee</b> <b>ADMISSION</b> <b>EVERY</b> <b>Daily</b> <b>CHILDREN, 15 Cents.</b> <b>NIGHT</b>		
<b>Monday</b> <b>ADULTS, 25 Cents</b> <b>at 8 P. M.</b>		

1

2

3

4

5

6

7

8

# Key Takeaways

---

## When Planning A Tabletop...

1

***Consider who needs to be involved and how you will involve them.*** (hint: it's not just technologists)

2

***Invest in exercising & push your team.*** Make it an open and honest dialogue and discuss a realistic and concerning threat to the constituency.

3

***Have some fun doing it.*** People are engaged when the subject matter is pertinent and challenging.





# Thank you! Questions?

**Michael Murray**

MMurray@secureworks.com

**Robert Lelewski**

RLelewski@secureworks.com

The Need to Find the 'Right' Answer

1

Not Performing Cross-Functional Tabletops

2

Not Defining Tabletop Goals

3

Not Capturing and Addressing Deficiencies

4

Not Pushing Boundaries

5

Always Building and Facilitating Internally

6

Not Testing Vendors

7

Lack of Senior Leadership Participation

8

