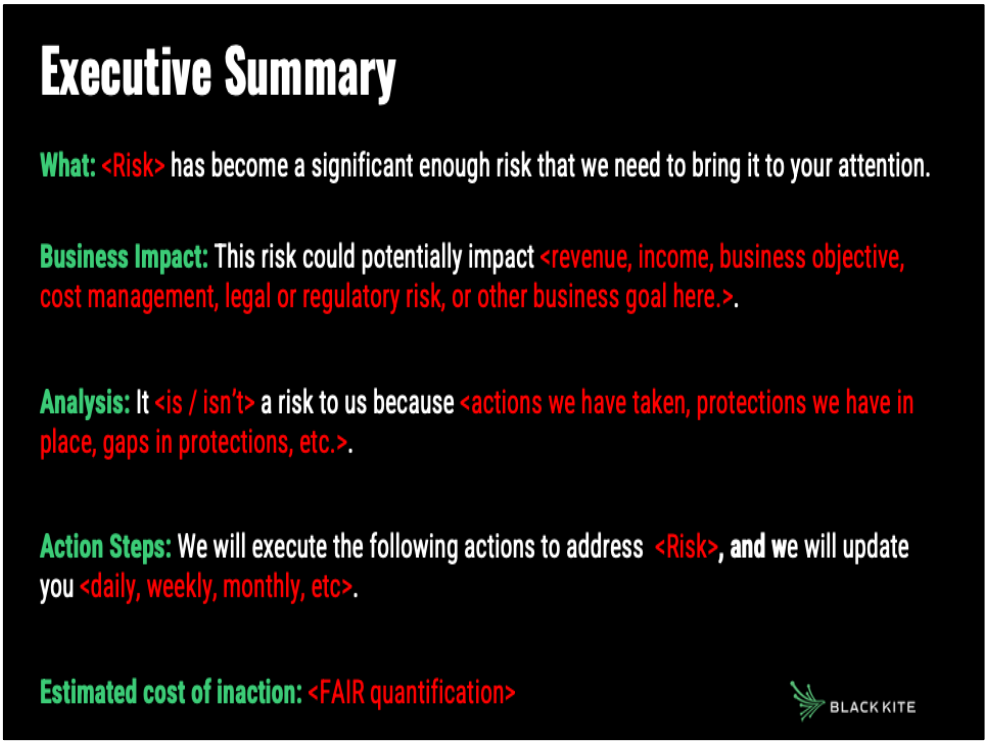
BLACK KITE

GET MORE THAN A SCORE

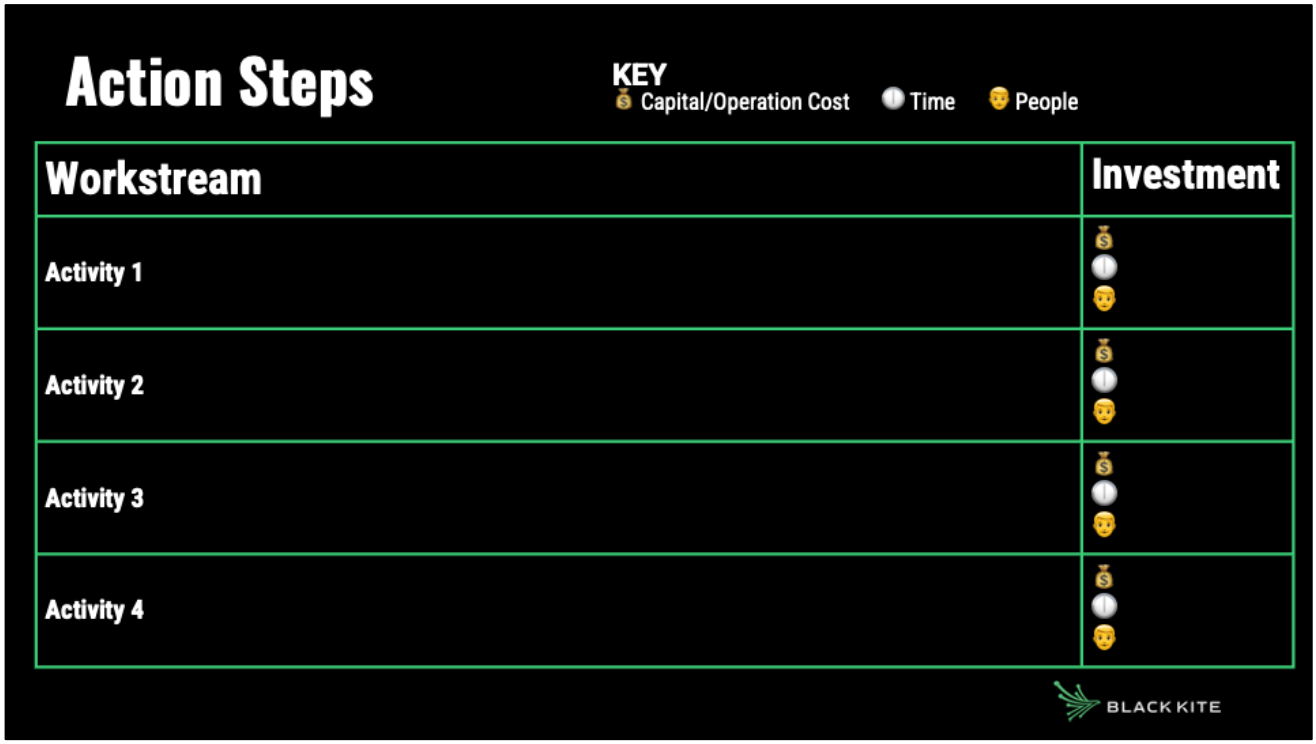
Reporting Risk to the Board (Template Slides)



Instructions:
Give stakeholders a 1-page overview of the problem and solution. (See example on Slide 8.)

Instructions:
Add relevant information about Constraints, Considerations, and Gaps to bolster your recommendation
Scripting Advice
Be clear and concise. Do not over promise or state your recommendations will result in absolute protection.

(See example on Slide 9.)



Instructions:
1 - Add the specific steps you need to complete in order to move the capability scaling to the targeted level.
2 - Add the details around your anticipated time horizon and investment. Icons for financial, time, and personnel effort give a visual impact of the anticipated investment.
Scripting Advice:
Acknowledge that not all investments are financial. Furthermore, being that controls maturity is tied to the breadth of coverage, process rigor and the strength of protection, there are other non-financial levers to pull to move the needle.
Acknowledge that there is no such thing as perfect or indefensible protection, and that by considering these actions you a lower risk.
Cybersecurity is a business decision. The board and executives could forgo this plan, and most will be willing to accept the consequences.

(See example on Slide 10.)

Instructions:
When reporting a risk found in your Black Kite dashboard, grab a screenshot of the OpenFAIR risk quantification screen to emphasize the business risk of not taking action. Include any other data points that will help your stakeholders understand what is at risk.

(See example on Slide 11.)

Instructions:
Let your board members know exactly what you are asking them to do.

(See example on Slide 12.)

BLACK KITE

GET MORE THAN A SCORE

Reporting Risk to the Board (Real-life Example)

Executive Summary

What: Third-Party Risk to our organization is **significant** enough that we need to bring it to your attention.

Business Impact: This risk could potentially impact our organization in three material ways-

1. **Loss of regulated data**
2. **An outage in one of our key vendors leading to operational disruption**
3. **Contractual obligations with our customers/partners**

Analysis: This represents a **CRITICAL** risk to us - we do not actively monitor potential cybersecurity exposure in our third-parties. We do assess cybersecurity posture during onboarding and annually thereafter (for partners deemed critical. Our criticality assessment is based upon how how much we spend with a vendor. Business owners are not involved in discussions around the impact of cybersecurity incidents in critical partners.

Action Steps: (1) We will be updating our onboarding process to account for financial and operational impact of Cybersecurity incidents in our supply chain; (2) We will be enhancing our governance to involve business owners in cyber risk discussions; (3) We will be implementing a third-party risk intelligence platform to provide real time visibility into our risk; and (4) We will update you monthly and at regular board meetings.

Analysis

Our current risk exposure to Cybersecurity incidents in our Third-party ecosystem partners is **CRITICAL**

Current State:

- Sending out questionnaires prior to onboarding new vendors
- Collecting and manually reviewing assessment/audit collateral
  - SOC 2, ISO 27001, High Trust, etc.

Gap Analysis:

- No continuous monitoring
- Minimal technical validation
- No business impact analysis
- No business involvement
- No outward focused assessment of cybersecurity exposures in our partners
- No real time risk or threat intelligence in our third party ecosystem

BLACK KITE

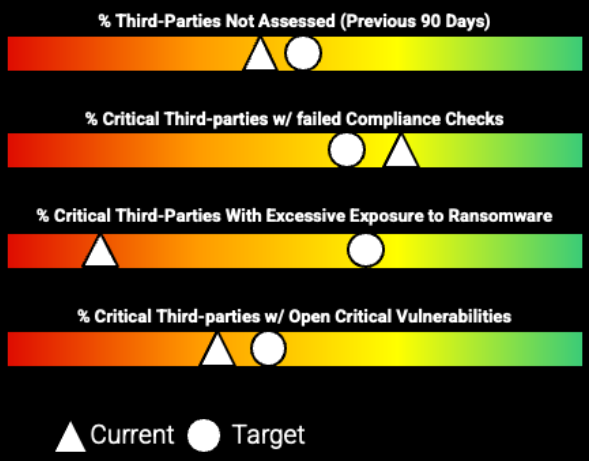
Action Steps

KEY
💰 Capital/Operation Cost 🌓 Time 👨 People

Workstream	Investment
Update partner onboarding to assess or financial/operational impact of Cybersecurity incidents	💰 🌓🌓🌓 👨👨
Enhance/mature governance to involve business owners in cyber risk discussions	💰 🌓🌓 👨👨👨
Implement a third-party risk intelligence platform to provide real time risk visibility	💰💰💰 🌓 👨👨
Update board monthly and at regular board meetings	💰 🌓 👨

BLACK KITE

What and Where is the Business Impact/Risk?



Riskiest Critical Vendors ($MM)

Third-Party	Impact
Vendor 'A'	1.5 - 1.7
Vendor 'B'	1.3 - 1.6
Vendor 'C'	.9 - 1.2
Vendor 'D'	.9 - 1.0
Vendor '*n*'	.8 - .9

Annualized Impact Across Third-Party Ecosystem

$275k	$9.5MM	$41MM
Minimum (10th%)	Most Likely (50th%)	Maximum (90th%)

BLACK KITE

What We Need From You

To Be Successful, We Need:

- Sign-off/authorize on project charter
- Provide support via engagement with executive leadership
- Authorize appropriate level of investment
- Support and ensure alignment with business objectives

BLACK KITE