DECISION RECORD

OPERATION SILK HARVEST · FILL IN AS YOU PLAY, READ IN THE DEBRIEF

INCIDENT NAME _____ DATE _____ INCIDENT MASTER _____

THE THREE EXECUTIVE DECISIONS

1 WHAT STOPS TODAY, AND WHAT EXPOSURE DO WE BUY?

OPTION CHOSEN ◯ A ◯ B ◯ C ◯ No resolution (wait outcome) VOTE _____ OF ___

ROLL target __+ d20 ___ backers +__ specialty +__ total ___ ◯ Full ◯ Partial ◯ Failure ◯ No roll

WHAT IT LED TO _____

2 WHOSE TIME, AND WHAT EXPOSURE DO WE CARRY?

OPTION CHOSEN ◯ A ◯ B ◯ C ◯ No resolution (wait outcome) VOTE _____ OF ___

ROLL target __+ d20 ___ backers +__ specialty +__ total ___ ◯ Full ◯ Partial ◯ Failure ◯ No roll

WHAT IT LED TO _____

3 WHAT DO WE SAY, TO WHOM, AND WHEN?

OPTION CHOSEN ◯ A ◯ B ◯ C ◯ No resolution (wait outcome) VOTE _____ OF ___

ROLL target __+ d20 ___ backers +__ specialty +__ total ___ ◯ Full ◯ Partial ◯ Failure ◯ No roll

WHAT IT LED TO _____

THE LEADERSHIP CALLS

THE FIRST CALL

Incident lead _____

Owner of the old system _____

CSIRT contact _____

☐ Nobody named

RESTART BEFORE CERTIFICATION

◯ Reopen ◯ Wait ◯ Not asked

Vote _____ of 4. Roll (15+) _____

It led to _____

THE CONSULTANT

◯ Bought ◯ Not bought

Vote _____ of 4

Financial one step worse to the end of the session when bought.

WHAT THE TABLE FOUND

A	**Fast-track exception**	☐ Found	☐ Missed
B	**Nobody owned the trade-off**	☐ Found	☐ Missed
C	**Speed again and again**	☐ Found	☐ Missed

THE RISK BOARD, AT THE END

SECURITY	STEADY	STRAINED	SERIOUS	CRITICAL
FINANCIAL	STEADY	STRAINED	SERIOUS	CRITICAL
REPUTATIONAL	STEADY	STRAINED	SERIOUS	CRITICAL

Circle the step each marker ended on.

THE VERDICT

THE TWO MARKS ☐ Ways in shut ☐ Leak stopped

CONTAINMENT ◯ Reached ◯ Not yet reached

THE COST, ONE SENTENCE

_____

_____

WHAT WE TAKE BACK: ONE LINE PER SEAT

CEO When _____ I will _____ by _____

CFO When _____ I will _____ by _____

CIO When _____ I will _____ by _____

CISO When _____ I will _____ by _____

CEO Accountable for fixing what this showed _____ by _____