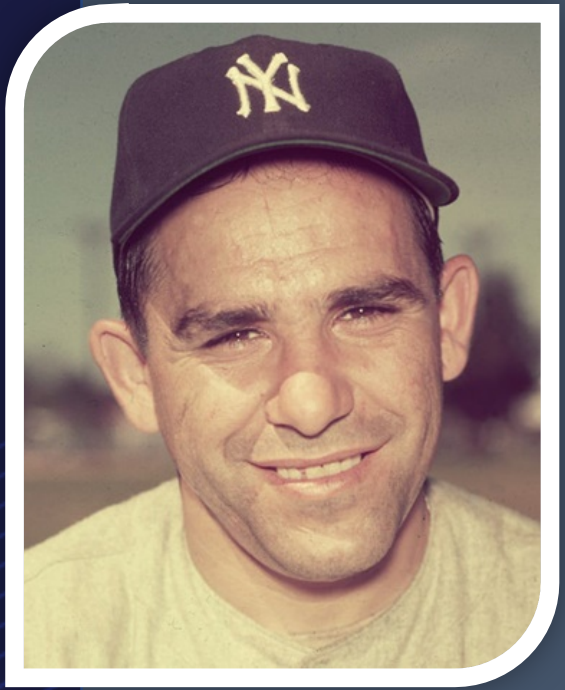
How FAIR Analyses Support Decision-Making at Netflix

Tony Martin-Vegue

Twitter: @tdmv
WWW: tonym-v.com
Email: tony.martinvegue@gmail.com

- Risk team at Netflix
- Been in risk for 11 years (mostly security, some ERM & operational)
- On the board of the Society of Information Risk Analysts (SIRA) and co-Chair of the SF Bay Chapter of the FAIR Institute
- Spoken at RSA, SIRA, FAIRcon, various Bsides, ISACA Fall Conference and others
- Sporadically write on risk topics
- BS, Business Econ from USF & CISSP, CISM, OpenFAIR



“When you come to a fork in the road, take it.”

- Yogi Berra

”We don’t want a risk register…”

Typical risk register

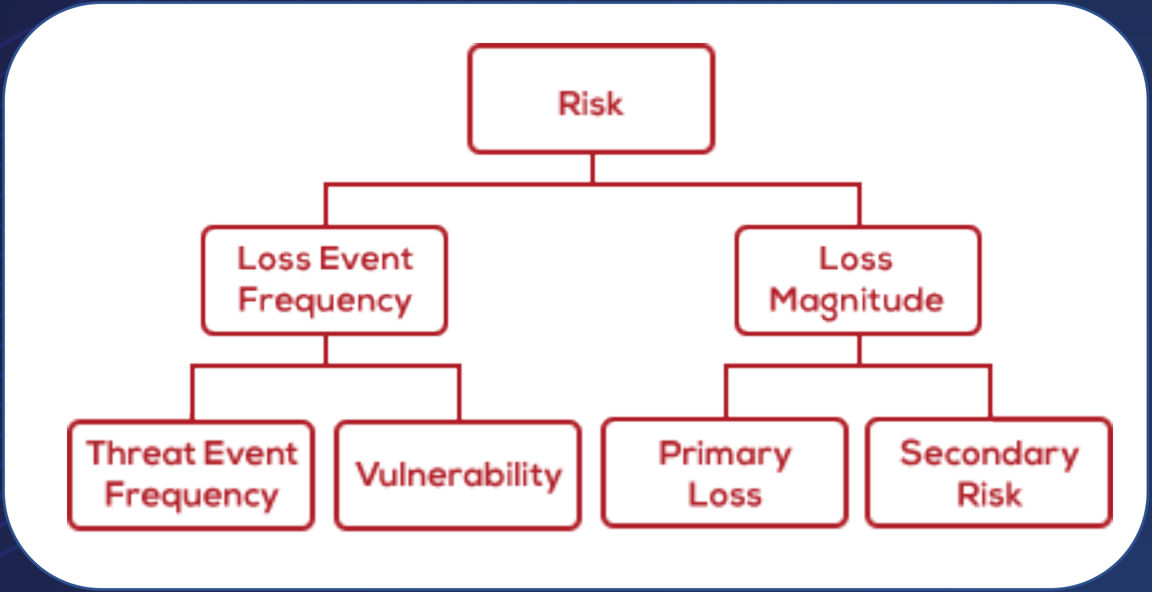
Risk Description	Likelihood	Impact	Risk
Weak admin password on SQL server	High	High	High
30 Windows servers out of patch compliance	Medium	High	High
Data breach	Very High	Very High	Very High
Server room lock is broken	Low	High	Medium

- Difficult to make decisions based on colors (Does the cost of the project reduce enough risk to make it worthwhile?)

- Sometimes, there is no decision to be made – policy says servers must be patched within a tolerance and server room must be locked – why do you need a risk analysis?

- Last, what would you like to know about data breaches? Are we covered? Overexposed? Underexposed?

“We want help making business decisions”


Risk
Loss Event Frequency
Loss Magnitude
Threat Event Frequency
Vulnerability
Primary Loss
Secondary Risk

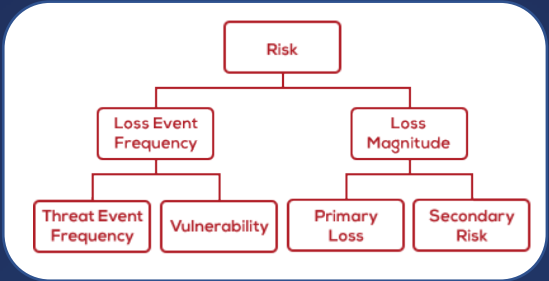
Decision

Should the company invest in a DLP project?

Opportunity cost → The loss of potential gain from other alternatives

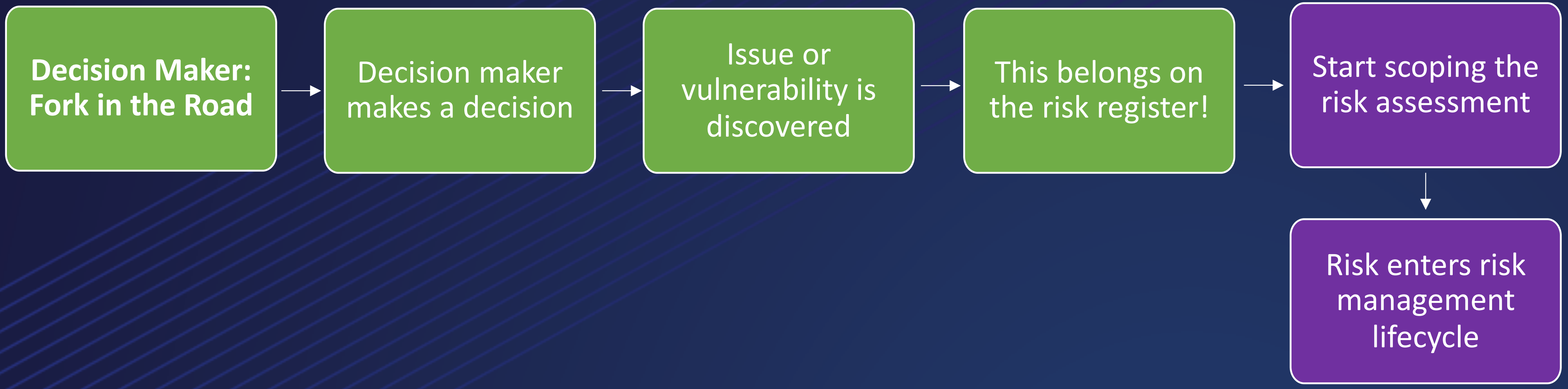
Current risk exposure

Projected risk exposure reduction →



Project cost → Is it worth it?

Conceptualize the risk lifecycle differently



Decision Maker: Fork in the Road

Decision maker makes a decision

Issue or vulnerability is discovered

This belongs on the risk register!

Start scoping the risk assessment

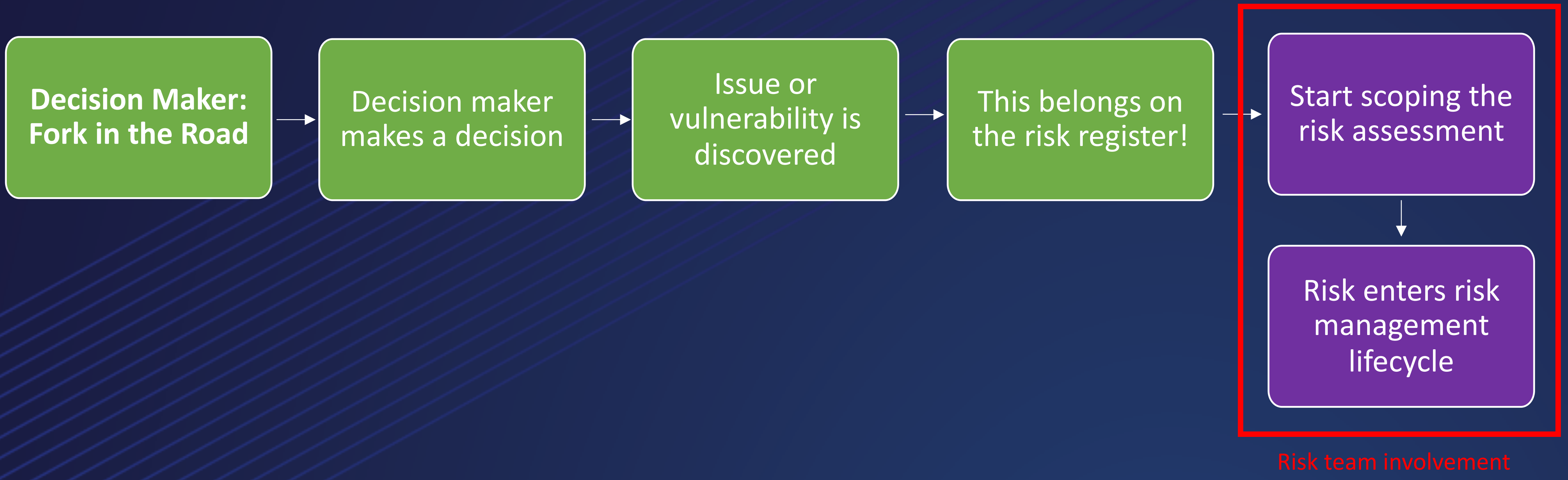
Risk enters risk management lifecycle

Compliance-focused risk program

🟪 Risk team

🟩 Decision maker (or risk owner)

Conceptualize the risk lifecycle differently

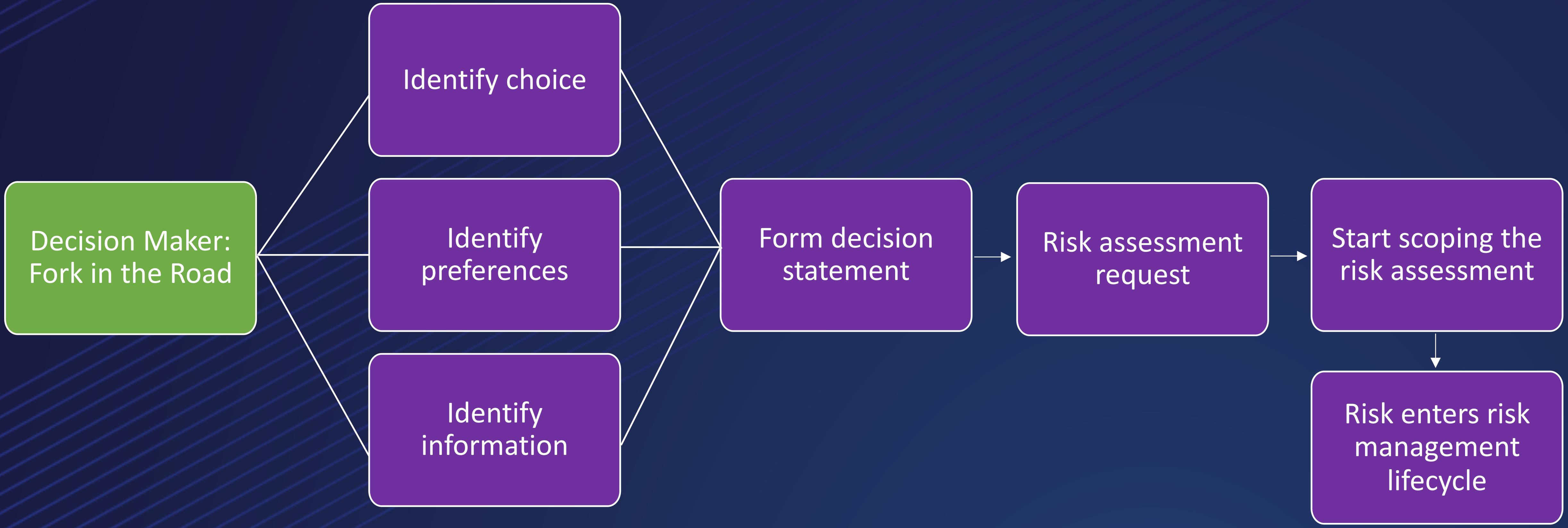

Decision Maker: Fork in the Road
Decision maker makes a decision
Issue or vulnerability is discovered
This belongs on the risk register!
Start scoping the risk assessment
Risk enters risk management lifecycle
Risk team involvement

Compliance-focused risk program

🟪 Risk team

🟩 Decision maker (or risk owner)

Conceptualize the risk lifecycle differently

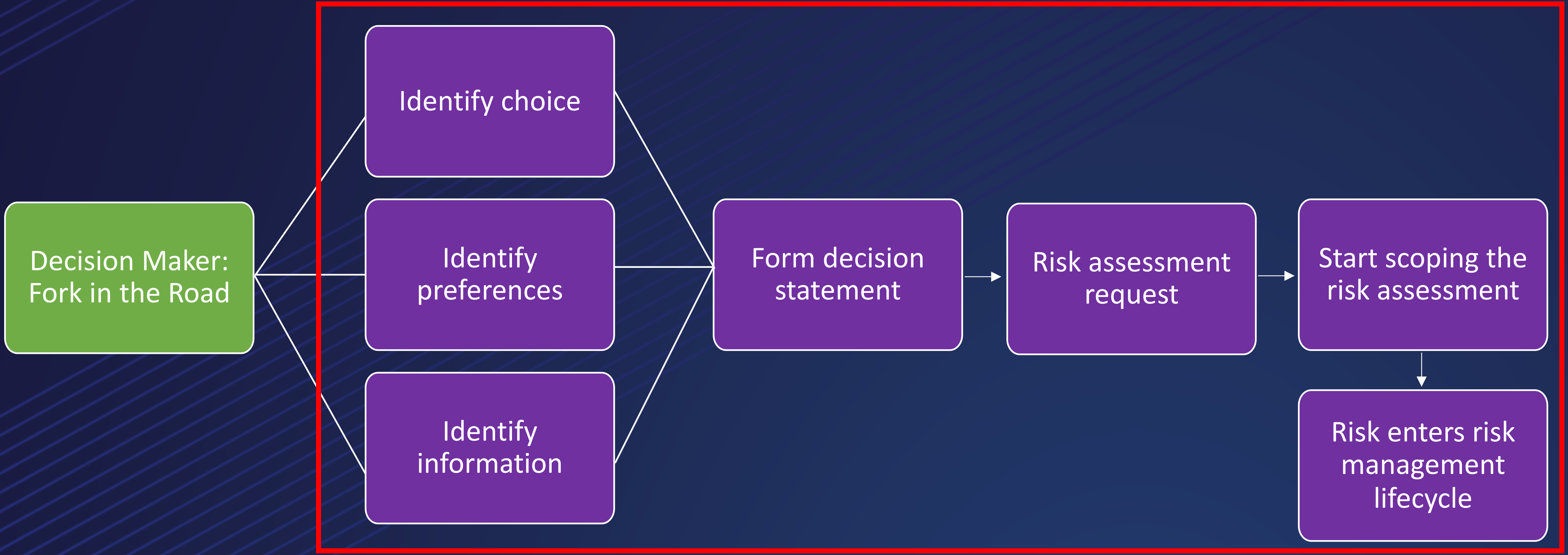

Decision Maker: Fork in the Road
Identify choice
Identify preferences
Identify information
Form decision statement
Risk assessment request
Start scoping the risk assessment
Risk enters risk management lifecycle

Decision-focused risk program

🟪 Risk team

🟩 Decision maker (or risk owner)

Conceptualize the risk lifecycle differently


Decision Maker: Fork in the Road
Identify choice
Identify preferences
Identify information
Form decision statement
Risk assessment request
Start scoping the risk assessment
Risk enters risk management lifecycle

Decision-focused risk program

🟪 Risk team

🟩 Decision maker (or risk owner)

Components of a Decision

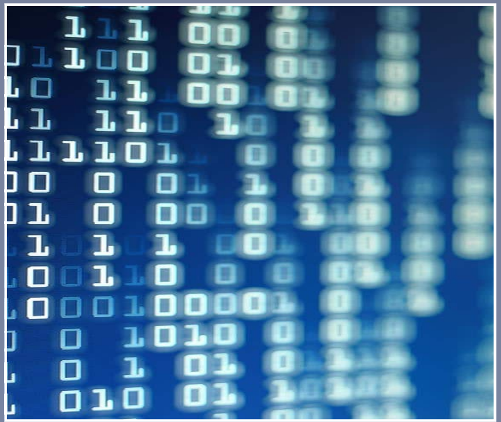
Choice

What the decision-maker can do

Preference

Preference for a desired outcome

Information



Information that can be applied

Source: *Foundations of Decision Analysis* by Ron Howard

Components of a Decision

Logic

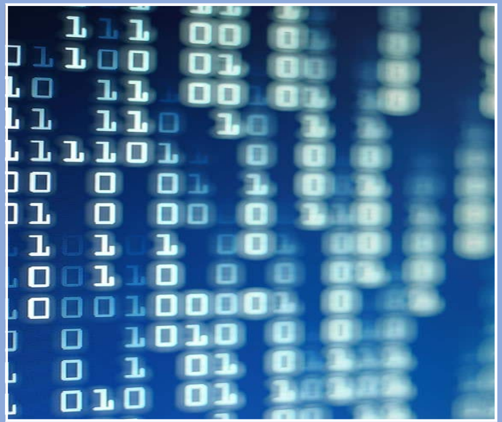
Choice

What the decision-maker can do

Preference

Preference for a desired outcome

Information



Information that can be applied

Source: *Foundations of Decision Analysis* by Ron Howard

“What kinds of decisions?”

“What kinds of decisions?”

Depends on your management point of view.

Levels of Risk Abstraction

Tier 1:

Supports Strategic Decision Making

Tier 2:

Supports Tactical Decision Making

Tier 3:

Supports Operational Decision Making

Tier 1: Strategic Decision Making

Scope

- Short list of systemic, existential or persistent company risks that senior leadership needs to be aware of.

How it’s used

- Portfolio view of risk that C-level leadership uses to make strategic investment decisions ~5 years out

Tier 1: Strategic Decision Making

Decision Examples

- Analysis of in-house versus outsourced code development
- Analysis of deploying services to cloud versus in-house hosting
- Analysis of selling product x over product y & how it impacts security
- Security and tech risk associated with M&A activity

Tier 2: Tactical Decision Making

Scope

- Risks across platforms, technologies, threat actors, departments and asset classes.

How it's used

- Cost/benefit analysis of proposed initiatives, budget and headcount planning, see how security investments are working

Tier 2: Tactical Decision Making

Decision Examples

- Enterprise architecture decisions (e.g. how to backup data, types of disk storage to use, servers running Linux versus Windows)
- Do we employ server virtualization?
- Model risk, risk of unassessed risk, risk of poor risk analysis methodologies
- Third party / service provider choices

Tier 3: Operational Decision Making

Scope

- Eventually thousands of risks; detailed analysis of individual assets.

How its used

- Aids in operational decisions: compare control x versus control y; prioritize or compare projects

Tier 3: Operational Decision Making

Decision Examples

- Endpoint protection: antivirus software, full disk encryption, DLP, full disk backup
- Which physical security controls are most effective to mitigate insider threats?
- Remediate pen test finding #31 or #12 first?

Comparisons

Potential risks of doing business

Security project

Increased security

Rewards of business (profit)

Opportunity cost

End-user friction

Key Takeaways

- Move FAIR analysis closer to decision makers
- Don’t perform FAIR analyses on issues – only risks
- Scope the analysis to fit the decision
- Higher level of abstractions = longer term, strategic decisions (know your audience)
- It’s always a balance between risk and reward (and risk isn’t bad)

Thank you!