RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

RISK AND RESILIENCE

In this module we will

- Define risk and resilience
- We will an intuitive and informal approach
- Introduce related concepts
- Examine some case studies

Image credit: https://skefto.com/blog/resilience-strategy-and-risk/

INFORMAL DEFINITIONS

- Like most terms, risk and resilience have common definitions
- Risk implies the "probability" of some event happening
  - But also with some implication of a negative consequence if the event occurs
    - *"There is a risk of rain today which means I might have to cancel our picnic"*
    - *"The operation has some risk to it, you might lose feeling in your leg.'*
  - In this section, we will create a precise formulation of "risk"
- Resilience implies that something is "tough"
  - In the sense that it can recover from negative events or attacks
    - *"He is a resilient fighter, he took a lot of punches but managed to come back and win the fight."*
    - *"This material is so resilient that no matter how you bend it, it snaps right back to its original shape.*
  - Like risk, we will create a precise formulation of "resilience"

RATING RISK

- Not all risk events are equivalent
  - Events have a range of probability of occurring
    - *"The chance of a hurricane making landfall in Boston MA this year is very unlikely"*
    - *"There is good chance a hurricane will make landfall in Florida this year."*
  - Events also have an outcome which tells us how bad the effects of the event would be
- Either of these can be quantitative or qualitative
  - "There is a 45% chance of a hurricane hitting Miami that would cause between $400 million and $800 million in property damage"
  - "There is a moderate chance of a hurricane hitting Miami that would cause high levels of property damage."
  - Qualitative measures are often good enough for relative risk evaluation
  - Because a primary goal of risk evaluation is to rank the severity of risks to prioritize which ones we should address first.

RANKING RISK

- Our goal in risk analysis is often to rank the risks we face
  - We have to “pick our targets”
    - We can’t do everything, so we will have to ignore some risks
    - The ones we want to ignore are either very unlikely to occur
    - Or they have a very minor impact
  - A typical ranking for risk is a set of ordinal categories like these
    - *Certain* – it definitely will happen
    - *Likely* – the chance the event occurring is greater than it not occurring
    - *Possible* – even odds of it occurring
    - *Unlikely* – the chance the event occurring is less than it not occurring
    - *Rare* – the chance of it happening is very low
    - *Eliminated* – the event cannot occur

RANKING RISK

- A typical ranking for outcomes is a set of ordinal categories like these
  - *Catastrophic* – death or permanent total disability, significant irreversible environmental impact, total loss of equipment
  - *Critical* – accident level injury resulting in hospitalization, permanent partial disability, significant reversible environmental impact, damage to equipment
  - *Marginal* – injury causing lost workdays, reversible moderate environmental impact, minor accident damage level
  - *Minor* – injury not causing lost workdays, minimal environmental impact, damage less than a minor accident level
- If there is no outcome meaning nothing happens when the event occurs
  - Then there is no risk because the event has no impact
- There a variety of different terms used in this sort of ranking

- Once we have an assessment of the likelihood and outcome
  - We can classify the risk of the event as the product of the two
  - This is represented by a risk matrix

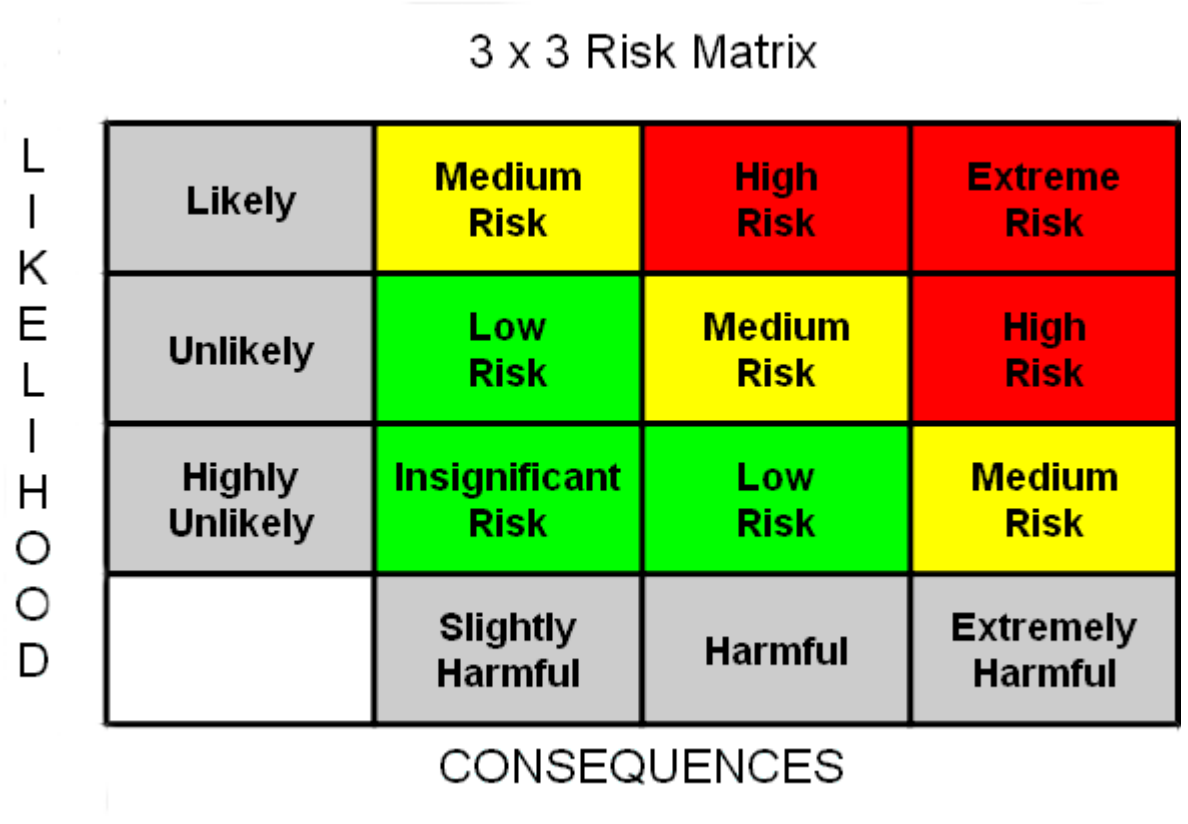
RISK MATRIX

- Each risk can now be ranked
  - Often we would want to deal with the “very high” risk first and urgently
  - These events are certain or likely to happen and will have severe negative impacts
  - We might not want to deal with the “low” risks and then prioritize the “high” risks based on other criteria
  - For example, how easy is it to prevent the risk event from occurring

Likelihood	Harm severity			
	Minor	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

COMMON RISK MATRICES

- A risk matrix is a tool
- There is no “right” form
- On the right is a 3x3 form
- The final risk categories are a subjective assessment
  - Often uses historical data and expert opinions to come to a decision



COMMON RISK MATRICES

- On the right is a 4x4 form
- This also assigns a numerical value for probability and severity
  - This produces a risk score ranging from 16 (4 x 4) to 1 (1 X 1)

COMMON RISK MATRICES

- On the right is a 5x5 form
- This one also shows the action that should be taken
- These examples show there is no "correct" form of a risk matrix
  - The all express the idea of computing risk as combination of likelihood and outcome
  - The actual risks defined will depend on how we choose to classify them
  - That is what we need to get right

Likelihood	Insignificant (A)	Marginal (B)	Moderate (C)	Critical (D)	Catastrophic (E)
Unlikely (1)	Low risk. No further action	Low risk. No further action	Low risk. No further action	Low risk. No further action	Medium risk. Further action optional
Seldom (2)	Low risk. No further action	Low risk. No further action	Medium risk. Further action optional	Medium risk. Further action optional	High risk. Further action necessary
Occasional (3)	Low risk. No further action	Medium risk. Further action optional	Medium risk. Further action optional	High risk. Further action necessary	Extreme risk. Act now
Likely (4)	Medium risk. Further action optional	Medium risk. Further action optional	High risk. Further action necessary	Extreme risk. Act now	Extreme risk. Act now
Definite (5)	Medium risk. Further action optional	High risk. Further action necessary	Extreme risk. Act now	Extreme risk. Act now	Extreme risk. Act now

QUANTITATIVE RISK MATRICES

- We can also use the risk matrix a more detailed risk analysis tool
- One method is to break down the risk into
  - Analysis of historical data as to the likelihood of an event, this might be expressed as an actual probability or the actual odds of the event occurring
  - A set of impacts on different populations of groups
- This results a more comprehensive description of the risk
  - The next page, for example, shows a more detailed risk matrix for the liquid natural gas industry
- The problem is that no matter how detailed the risk matrix
  - It doesn't tell us how to manage risk or reduce the risk
  - We need a standard set of concepts, procedures and strategies for risk management

LNG RISK MATRICES

CONSEQUENCES								INCREASING PROBABILITY (Likelihood) →				
INCREASING SEVERITY ↓		Category						A	B	C	D	E
		People	Asset / Production	Environment	Reputation	Community Relation	Security	Never heard of in the Oil & Gas Industry	Heard of in the Oil & Gas Industry	Has happened in the LNG Industry or more than once per year in the Oil & Gas Industry	Has happened at NLNG or once per year in the LNG Industry	Has happened more than once per year in NLNG
	0	No injury or health effect	No damage	No effect	No impact	No impact	No impact	A0	B0	C0	D0	E0
	1	Slight injury or health effect (FAC)	Slight damage (10k$ & no disruption to operation)	Slight effect (within fence, no exceedance)	Slight impact (E.g. public awareness)	Incidental problem	Minimal impact resolved internally	A1	B1	C1	D1	E1
	2	Minor injury or health effect (MTC, RWC<= 5days, food poisoning & dermatitis)	Minor damage (10k$ - 100k$ & brief disruption)	Minor effect (Minor impact but no lasting effect)	Limited impact (E.g. local / public media)	Threats of bodily harm to personnel, without action; Re-instatement of no go areas	Low impact resolved with Company dedicated GSAs	A2	B2	C2	D2	E2
	3	Major injury or health effect (LTI, RWC >5Days,)	Moderate damage (0.1 - 1.0M$ & partial shutdown)	Moderate effect (Limited Env. Impact that requires clean up)	Considerable impact (E.g.. region / state / public media)	Several days of blockade of local facilities, rivers, water pump station or gas supply station)	Medium impact resolved with support from Local GSAs	A3	B3	C3	D3	E3
	4	Permanent Total Disability (PTD) or up to 3 fatalities	Major damage (1.0 - 10.0M$ & partial operation loss)	Major effect (severe damage recoverable / extended exceedance)	Major Impact (E.g. extensive adverse media)	Severe damage to water supply or gas station reported in Nigerian media	Major impact resolved with support from State GSAs	A4	B4	C4	D4	E4
	5	More than 3 fatalities	Extensive damage (>10M$ & substantial operation loss)	Massive effect (widespread chronic effects / constant high exceedance)	Massive impact (E.g. extensive adverse media)	Impossible to operate without major military support	Massive impact resolved with support from National GSAs	A5	B5	C5	D5	E5

NEGLIGIBLE
LOW
MEDIUM
HIGH

RESILIENCE CONCEPTS

- Resilience generally means
  - How a system deals with negative events and returns to normal
- Resilience is not about avoiding negative events
  - We accept the fact that these event will occur and will impact our system
  - We absorb these events with no or only minimal loss, and recover from them
  - If the system goes down in whole or part, its function can be restored quickly
- Some other related concepts
  - *Continuity*: refers to the idea a business, for example, can continue to function even when there is a failure in a system – although it might be at reduced capacity for a while
  - *Reliability*: refers to the idea that we can count on a system to be consistently resilient

RESILIENCE

- Basic themes in resilience
  - *Anticipate*: Identify the points of failure and dependencies where things could go wrong.
  - *Withstand*: Keep operations running when parts fail
    - Maintain continuity of operations, even at a degraded level
  - *Recover*: Restore full operations quickly
    - Recovery strategies, restore from backups, switch to redundant systems and fail overs
  - *Adapt*: Learn from incidents and improve
    - Improves the reliability of the system
- Like risk, resilience needs
  - Standard concepts, procedures and protocols, including assessment tools
  - We don't want to have to operate from scratch every time we consider resilience
  - We also need to integrate our resilience

ISACA IT RISK FRAMEWORK

- Why do we need a formal risk framework?
  - A framework turns “risk intuition” or gut feelings into repeatable, outcome-driven practices.
- Benefits of a formal framework
  - *Consistency*. Everyone scores, prioritizes, and names risks the same across teams and time.
  - *Comparability*. We can weigh trade-offs across products, systems, and business units apples-to-apples.
  - *Defensibility & auditability*. Clear decision trails; regulators and auditors can trace the logic.
  - *Bias reduction:* Structured steps helps avoid
    - *Recency bias:* too much emphasis on recent data than potentially more relevant historical data
    - *Availability bias:* too much importance on vivid or dramatic data rather than a full analysis of the data
    - *HiPPO effects: Highest Paid Person Opinion* too much emphasis on the most senior person’s opinion

ISACA IT RISK FRAMEWORK

- *Speed with quality:* Templates and best practice allow previous experience to be used to provide faster and better responses in the future
- *Risk appetite:* Actions correlate with the the organization's acceptable risk policies rather than informal gut feelings.
- *Governance integration:* Allows for integration with governance processes, KRIs/KPIs, incident/BC/DR processes.
- *Communication*: Content is packaged for the intended audience
  - Executives get business-impact summaries
  - Engineers get actionable control guidance.

- We will formally introduce the ISACA framework in the next section

FORMAL VS INFORMAL DEFINITIONS

- Risk
  - Informal
    - “Something bad might happen because…”
    - eg. “It would be terrible if someone could break into our system with administrator privileges”
  - Formal Definition
    - A potential event/condition with likelihood and impact on objectives.
- Issue
  - Informal
    - “Something bad could happen if we don’t fix this”
    - e.g “The administrator account login has not been disabled for external logins over the Internet”
  - Formal Definition
    - A current problem (realized risk) requiring remediation .

ISACA IT RISK DEFINITIONS

- Control
  - Informal:
    - "Things we put this security feature into place or bad things will happen"
    - eg. "We need to ensure administrators can only log in from inside our IT department network."
  - Formal Definition
    - A policy/process/technical measure to reduce likelihood/impact or detect/recover.
- Incident
  - Informal
    - "That issue we didn't address, it just caused a bad thing to happen."
    - eg. "Someone hacked in as administrator and deleted the entire code base for our next release."
  - Formal Definition
    - A disruptive event affecting confidentiality, integrity, availability, or operations.

ISACA IT RISK DEFINITIONS

- Remediation
  - Informal:
    - “We need to fix this issue”
    - eg. “We need to ensure administrators can only log in from inside our IT department network.”
  - Formal Definition
    - Actions to resolve an issue or strengthen controls to reduce risk.
- Recovery
  - Informal
    - “Get it back up.”
    - eg. “We were able to restore the deleted code base from the last backup with minimal loss so we can continue development.”
  - Formal Definition
    - Activities to restore services/data to an acceptable state and service level agreements

ISACA IT RISK DEFINITIONS

- Inherent risk
  - Informal:
    - “Raw risk before we do anything.”
    - eg. “Literally anyone can log into our system from anywhere as administrator and use a brute force attack to get full system access”
  - Formal Definition
    - The level of risk before considering existing controls.
- Residual risk
  - Informal
    - “What risk is left over after we apply controls.”
    - eg. “No one can get administrator access from outside, but we still have to worry about social engineering attacks on our existing staff to gain internal access.”
  - Formal Definition
    - The level of risk after controls are applied.

ISACA IT RISK DEFINITIONS

- Risk appetite
  - Informal:
    - “How much pain we’ll accept because we can’t eliminate all risk and still get our jobs done.”
    - eg. “Because we are committed to developing AI tools, we are willing to accept the risks inherent in new technology development ”
  - Formal Definition
    - The amount of risk an organization is willing to accept in pursuit of its objectives.
- Risk tolerance
  - Informal:
    - “How much risk we are willing to accept as acceptable before we start to panic”
    - eg. “No more than 2% of transactions per year may fail due to IT issues.”
  - Formal Definition
    - The acceptable level of variation in outcomes related to specific risks, often expressed in measurable thresholds.

RISK TOLERANCE EXAMPLE

- UNIX operating system and C programming language
  - Have a reputation for being “risky”
  - You could do things in a UNIX system that would brick the system or cause damage
  - There was a high tolerance for risk,
- Doug Gwyn explained why
  - *“Unix was not designed to stop you from doing stupid things, because that would also stop you from doing clever things.”*
  - Risk management was the programmer’s responsibility, not the operating system’s responsibility

RISK CATEGORIES

- There are a number of risk categories defined by various groups
  - We will explore these in more detail later
  - We will focus mostly on the financial services industry
- Enterprise Risk Management identifies the following general categories
  - *Strategic* – risks that affect achievement of high-level goals aligned with mission/strategy (e.g., poor tech bets, failed transformations).
  - *Operations* – risks from day-to-day processes, people, systems, or external events that impair effective and efficient operations (e.g., outages, control breakdowns).
  - *Reporting* – risks that financial or non-financial reports are unreliable, incomplete, or untimely (e.g., data quality, ITGC/SOX failures).
  - *Compliance* – risks of violating laws, regulations, or internal policies (e.g., privacy, AML, consumer-compliance tech issues).

RISK CATEGORIES

- ISACA's Risk IT framework groups I&T-related risk into four main categories
- Benefit/value enablement risk:
  - The risk that technology-enabled initiatives don't deliver the expected business value (missed benefits, poor adoption, bad ROI).
- Program & project delivery risk:
  - The risk that change efforts (programs, projects) fail on scope, time, cost, or quality, causing business disruption or lost opportunity.
- Operations & service-delivery risk:
  - The risk that day-to-day IT services underperform or fail (outages, capacity shortfalls, process/control breakdowns).
- Cyber and information security risk
  - The risk from threats to information and technology (confidentiality, integrity, availability), including cyberattacks and control weaknesses.

RISK CATEGORIES

- We will explore these definitions in more detail later
- And how the various definitions relate to each other

RESILIENCE

- Differences between risk and reliability/resilience
  - Risk is about preventing things from going wrong
  - Reliability is about continuing to function normally without failing even when things go wrong
    - For example, systems that reject bad data that could crash operations are reliable, they continue to function even given corrupted input
  - Resilience is about absorbing bad events and getting back to normal fast
  - Resilience is about expecting failure, limiting the fallout, and returning to service predictably so customers and the business keep moving.
- Reliability tries to avoid failure; resilience assumes failure will happen
  - Systems are designed to absorb and recover from failure

RESILIENCE

- Security vs. Resilience
  - Security reduces the likelihood of problems deliberately caused by an adversary
  - Resilience reduces the impact and duration when a system is attacked
- Redundancy vs. Resilience
  - Redundancy is a tool (extra capacity, backups).
  - Resilience is the strategy that decides where and how to use those tools.
- Resilience (recall)
  - *Anticipate* — Spot what could go wrong (single points of failure, dependencies).
  - *Withstand* — Keep core services running when parts fail (graceful degradation).
  - *Recover* — Restore full service quickly (clear roles, practised runbooks, tested backups).
  - *Adapt* — Learn from incidents and improve so the same issue hurts less next time.

RESILIENCE DEFINITIONS

- Organizational resilience
  - *"Ability of an organization to absorb and adapt in a changing environment to deliver objectives and to survive and prosper."*
- RTO (recovery time objective)
  - How fast you must restore an activity/service to an acceptable level after a disruption. Think "clock time to be back up enough to matter."
- RPO (recovery point objective)
  - How much data you can afford to lose, expressed as a point in time you must be able to roll back to (e.g., "no more than 5 minutes of orders lost").

RESILIENCY DEFINITIONS

- MTPD (maximum tolerable period of disruption)
  - Beyond this duration, the impact becomes unacceptable.
  - This is the outer limit for a disruption
  - RTO must always be set inside this boundary.
  - Also called MAO Maximum Acceptable Outage
- MBCO (minimum business continuity objective)
  - The minimum acceptable performance level during disruption
  - (e.g., “process 20% of payments”).
  - Your RTO is the time to reach at least the MBCO.
- BIA (business impact analysis)
  - Analysis step that quantifies impact over time and helps calculate realistic RTO/RPO per activity/application.

BANK EXAMPLE

- Payments process routing:
  - MTPD: 2 hours (beyond that: regulatory, reputational impact unacceptable).
  - RTO: 15 minutes to MBCO (route 30% of traffic through secondary processor).
  - RPO: 1 minute (can’t lose more than 1 minute of auth logs/transactions).
  - Resilience Planning: synchronous replication for auth logs, hot-hot routing, automated failover playbook.
- Trade confirmations portal
  - MTPD: 24 hours.
  - RTO: 4 hours (read-only mode acceptable initially).
  - RPO: 15 minutes (replayable from upstream book of record).
  - Resilience Planning: frequent backups + near-real-time replicas; runbook for read-only mode.

BUSINESS IMPACT ANALYSIS

- Structured way to assess how bad things get over time when a business activity or IT service is disrupted.
  - Quantifies the impact (financial, customer, regulatory, operational)
  - Uses that to set targets a resilience plan must meet
    - MTPD/MAO (how long you can be down at most),
    - RTO (how fast you must be back to a minimum level), and
    - RPO (how much data you can afford to lose).
  - Identifies which services matter most, how quickly does pain escalate, and what recovery promises do have to be keep?
  - Also useful for identifying various types of risks
- We will drill down into doing a BIA in future sections
  - But for now, just enough to do the analysis exercise
  - Also, our first look at the terminology

BUSINESS IMPACT ANALYSIS

- BIA key outputs
  - Criticality tier for each activity/service
    - e.g., Tier 1 “mission critical,” Tier 2, etc.)
    - Essentially an evaluation of how important each service is to maintaining business continuity
  - Impact curve over time
    - e.g., tolerable degrades to severe degrades unacceptable after X hours)
    - Generally a measure of how the impact to the business gets worse over time
  - MTPD/MAO for each activity
    - We have to know the outer limit for what is acceptable
  - RTO and RPO targets:
    - We have to know what the targets are that are to be designed to and tested against.

BUSINESS IMPACT ANALYSIS

- Minimum Business Continuity Objective (MBCO):
  - The minimum acceptable service level during disruption.
  - Although service might be degraded, how much can be tolerated before it all fails
- Dependency map
  - Where are the people, locations, technology, data and third parties who are involved
- Regulatory/contractual constraints that tighten targets.
  - What are the legal and compliance issues that we have to take into account
  - What we might be able to tolerate as MBCO might not be acceptable to regulators
- Prioritized recovery order and data protection needs.
  - What needs to be done first
  - How do we protect our data assets
- Assumptions and residual risks
  - What could still go wrong even if we recover
  - For example, was an outage was a planned diversion by someone hacking the system

HOW TO RUN A BIA

- Phase 1: Prepare (1–2 weeks)
  - Define scope: Which business activities to analyze
  - Identify the underlying IT services (applications, databases, payment rails, call center, branches) are in-scope.
  - Pick impact criteria describing the impact of failure on various areas
    - Financial (per hour/day),
    - Customer (volume affected, VIP segments),
    - Regulatory (reporting deadlines, penalties),
    - Operational (manual workarounds),
    - Reputation (media/social triggers).
  - Use a quantified scale with concrete thresholds (e.g., “Regulatory breach likely” = level 4).
  - Collect reference data: Past incidents, SLAs, volumes, cutoffs, market windows (e.g., payment settlement times), control test results, known issues.

HOW TO RUN A BIA

- Phase 1: Prepare (1–2 weeks)
  - Example impact criteria for a bank
    - Financial: revenue loss, fees/penalties, trading P&L, cost of manual work.
    - Customer: Number of customers unable to transact, VIP/segment impact, queue/abandon rates.
    - Regulatory & Legal: reportable incidents, filing deadlines missed, consent order exposure, fines.
    - Operational: throughput drop, backlog growth, staff hours for workaround, dependency breakage.
    - Reputation: media/social escalation, complaints, NPS drop, executive attention.
    - (Optional) Safety/People: rarely primary in IT-only outages, but include if relevant to branch/ATM physical operations.

HOW TO RUN A BIA

- Phase 1: Prepare (1–2 weeks)
  - Example ranked impact criteria for a bank

Criterion	1 – Low	3 – Moderate	5 – Intolerable
Financial (per day)	<$10k	$250k–$1M	>$5M
Customer blocked	<100	5k–50k or VIPs impacted	>250k or nationwide
Regulatory	None	Filing delay/notice	Reportable breach or fine likely
Operational	Minor workaround	Sustained manual backlog	No viable workaround
Reputation	Internal noise	Social/media chatter	National coverage/Board-level

HOW TO RUN A BIA

- Phase 2: Elicit & validate (2–4 weeks)
  - Interviews/workshops: With business owners and tech leads (Dev/SRE/DBA/Network/IAM), using the same questionnaire to ensure comparability.
    - What does the activity produce? Who depends on it?
    - What happens at 15m / 1h / 4h / 24h / 3d of downtime?
    - What data would be lost at different points? How hard is reconciliation or restoration?
    - What's the minimum acceptable level (MBCO)?
    - Any hard deadlines (market close, clearing windows, regulatory submissions)?
  - Map dependencies: Applications, data stores, identity, networks, endpoints, facilities, vendors, SLAs
  - Quantify impact over time:
    - Convert narratives into scores and impact curves.
    - Identify the time when impact becomes unacceptable, that's becomes the MTPD/MAO.

HOW TO RUN A BIA

- Phase 3: Set targets & align (1–2 weeks)
  - Derive targets:
    - RTO = time to resume to at least the MBCO, and always < MTPD.
    - RPO = max tolerable data loss window based on data volatility and reconciliation cost.
  - Prioritize recovery order
    - If many services are down, what starts first?
  - Validate feasibility with IT:
    - Can the current architecture meet RTO/RPO?
    - If not, document gaps, options, and cost.

HOW TO RUN A BIA

- Phase 4: Publish & embed (1 week)
  - Deliver the BIA register/report: Criticality tiers, impact curves, targets, dependencies, assumptions.
  - Flow targets into plans & tests: Update DR runbooks, exercise calendar, monitoring dashboards (RTO/RPO/MTPD).
  - Set review cadence: Re-run or refresh annually or after major changes (mergers, platform shifts, new regulations).

HOW TO DETERMINE RTO

- Scope the “activity”
  - Name the business service (e.g., Card Authorizations) and the IT stack behind it (apps, DBs, networks, vendors).
- Run/refresh a BIA (Business Impact Analysis)
  - Quantify impact (financial, customer, regulatory, operational) as a function of outage time. Identify the MTPD/MAO—the point at which impact becomes unacceptable.
- Set a measurable target
  - Pick the RTO inside the MTPD that reflects the minimum acceptable level of service (MBCO). Example: “15 minutes to read-only balances, 60 minutes to full function.”
- Check external constraints
  - Regulatory rules, customer SLAs, market hours, cutoffs (e.g., payment settlement windows) may force a tighter RTO.

HOW TO DETERMINE RTO

- Design to the number
  - Choose strategies that can actually meet it (active-active, hot standby, autoscaling, automated failover, pre-provisioned capacity).
- Cost–risk tradeoff
  - Compare business benefit of a shorter RTO vs. added run costs and complexity. Adjust if the economics don’t justify “minutes.”
- Codify & test
  - Put RTO in runbooks and DR plans. Validate with timed exercises; record actual recovery time and fix gaps.

HOW TO DETERMINE RPO

- Understand the data
  - What records are affected (orders, trades, auth logs)?
  - What's their change rate and reconciliation cost if lost?
- Establish the tolerance
  - With business owners, set the largest acceptable loss window
    - e.g., "≤ 5 minutes of orders lost"
- Map to data protection options
  - RPO ≈ 0: synchronous replication, dual-write, commit-quorum.
  - RPO in minutes: asynchronous replication + frequent log shipping/snapshots.
  - RPO in hours: periodic backups are sufficient.

HOW TO DETERMINE RPO

- Check downstream dependencies
  - If systems feed each other, the strictest RPO in the chain often governs.
- Prove recoverability
  - Run point-in-time restores and message replays to show you can land at or before the RPO. Keep logs as evidence.

REAL WORLD ISSUES

- Feasibility loop
  - If architecture can’t meet the chosen RTO/RPO, either invest (hotter standby, faster replication) or revise targets with signed risk acceptance.
- Tiering:
  - Not every component needs the same target
  - Design graceful degradation
  - eg. Read-only mode meets RTO while other features catch up.

RISK CONTRIBUTION

- Implicit in the discussion of resilience
  - The assumption we understand the risks involved in outages of any type
  - Essential in doing a BIA
- In developing a BIA, it might be discovered that some failures cannot be recovered from
- For example:
  - A critical system is a legacy system which no one really understands anymore
  - The in house expertise to perform the recovery operations does not exist
  - The IT dependencies are so complex that a single failure might result in a cascading total failure of the entire IT infrastructure

RISK CONTRIBUTION

- This creates a risk profile that might not have been obvious before
- Risk management then has to assess the various types of risks discovered
- Generally uses the following categories
  - *Operational risk:* Risk of loss from inadequate or failed processes, people, and systems or from external events; includes legal risk, excludes strategic and reputational risk.
  - *Information security & privacy risk:* Risk to organizational operations/assets and individuals from the operation and use of information systems (security and privacy).
  - *Strategic risk:* Risk to achieving strategy and business objectives (e.g., tech choices that hinder strategy execution).
  - *Compliance risk:* Risk of violations of existing laws/regulations or internal policy requirements.

CASE STUDY: AI

For the provided case studies of failed AI implementation, provide an informal risk and resiliency analysis

EXERCISE: BIA

Perform a BIA for a provided IT project

Q&A AND OPEN DISCUSSION