RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

RISK AND RESILIENCE

In this module we will

- Define risk and resilience
- Begin with an intuitive and informal approach
- Introduce related concepts
- Introduce the first case study

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

INFORMAL DEFINITIONS

- *Risk* and *resilience* are often used in an informal sense
- Risk is associated with the *probability* of an event happening
  - But with some implication of a negative consequence if that 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 more formal and precise definition of "risk"
- Resilience implies that something is *tough*
  - Meaning 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 back to its original shape"*
  - Like risk, we will create a precise formulation of "resilience" later

RATING RISK

- Risk events are evaluated along two dimensions
  - Events have a *probability* of occurring
    - *"The chance of a hurricane making landfall in Boston MA this year is very unlikely"*
    - *"There is a good chance a hurricane will make landfall in Florida this year"*
  - Events have *outcomes* that tell us how negative the impacts of the events could be
- Both dimensions 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 informal risk evaluation
  - A primary goal of risk evaluation is to rank the severity of risks in order to prioritize which ones we should address first

RANKING RISK

- To prioritize risks
  - We have to “pick our targets”
    - We can’t do everything, so we will have to ignore some risks
    - The ones we ignore should be either very unlikely to occur or have a very minor impact
  - A typical assessment for risk occurrence is a set of ranked categories
    - *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

- An assessment for outcomes is also a set of ranked categories
  - *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 negative outcome when the event occurs
  - Then there is no risk because the event has no impact
- Once there are rankings of the likelihood and outcome
  - We can classify the overall risk of the event
  - Usually taken as the informal product of the two rankings
- Often represented by a risk matrix

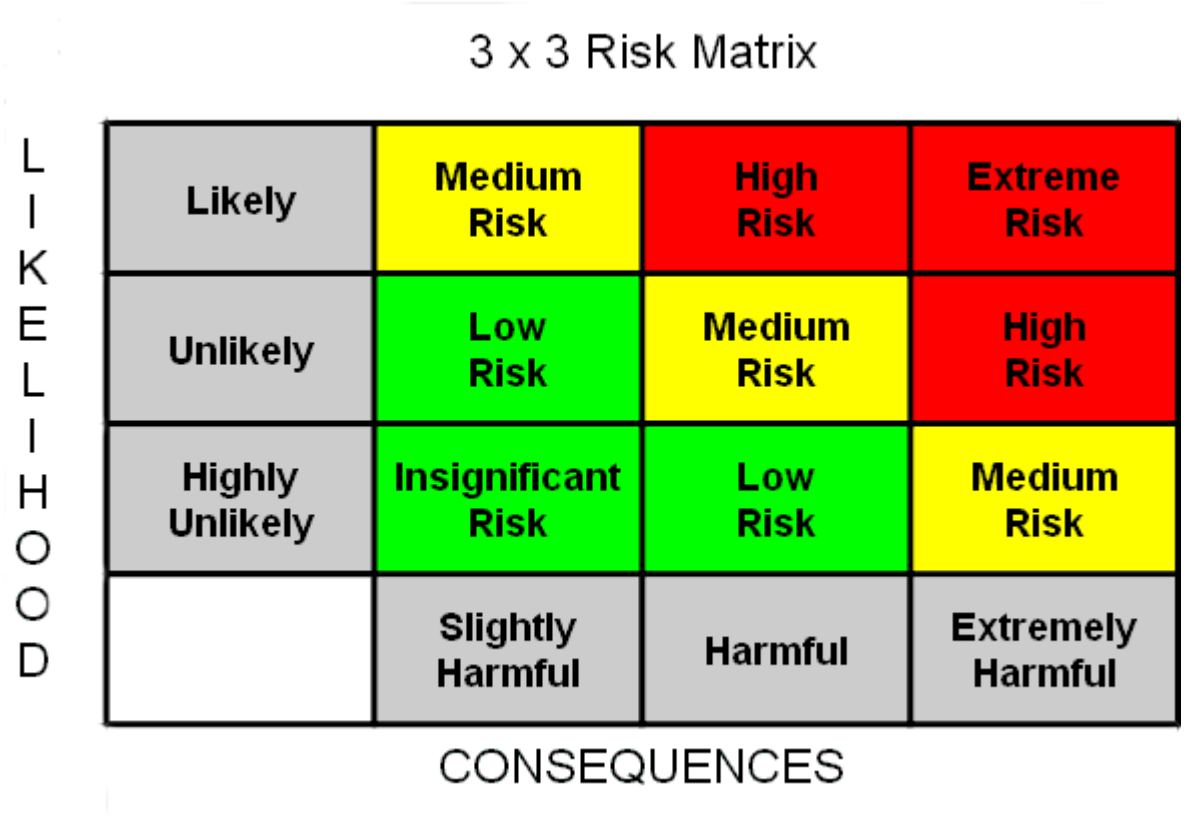
RISK MATRIX

- Each risk can now be prioritized
- The *very high* risks are dealt with first
  - These events are certain or likely to happen and will have severe negative impacts
  - These generally need to be done urgently
- We might not manage with the *low* risks
- We can prioritize management of the mid-range risks based on other criteria
  - For example, costs of a *high* risk mitigation may have to be deferred because of costs
  - Or a *medium* risk may be deferred because the skill sets to mitigate it might not be available.
- Establishes a way to triage risks

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 visual tool
  - There is no official format
  - On the right is a common 3x3 form
- The example is qualitative
  - Useful as a first analysis
  - Often uses historical data and expert opinions to come to a preliminary decision

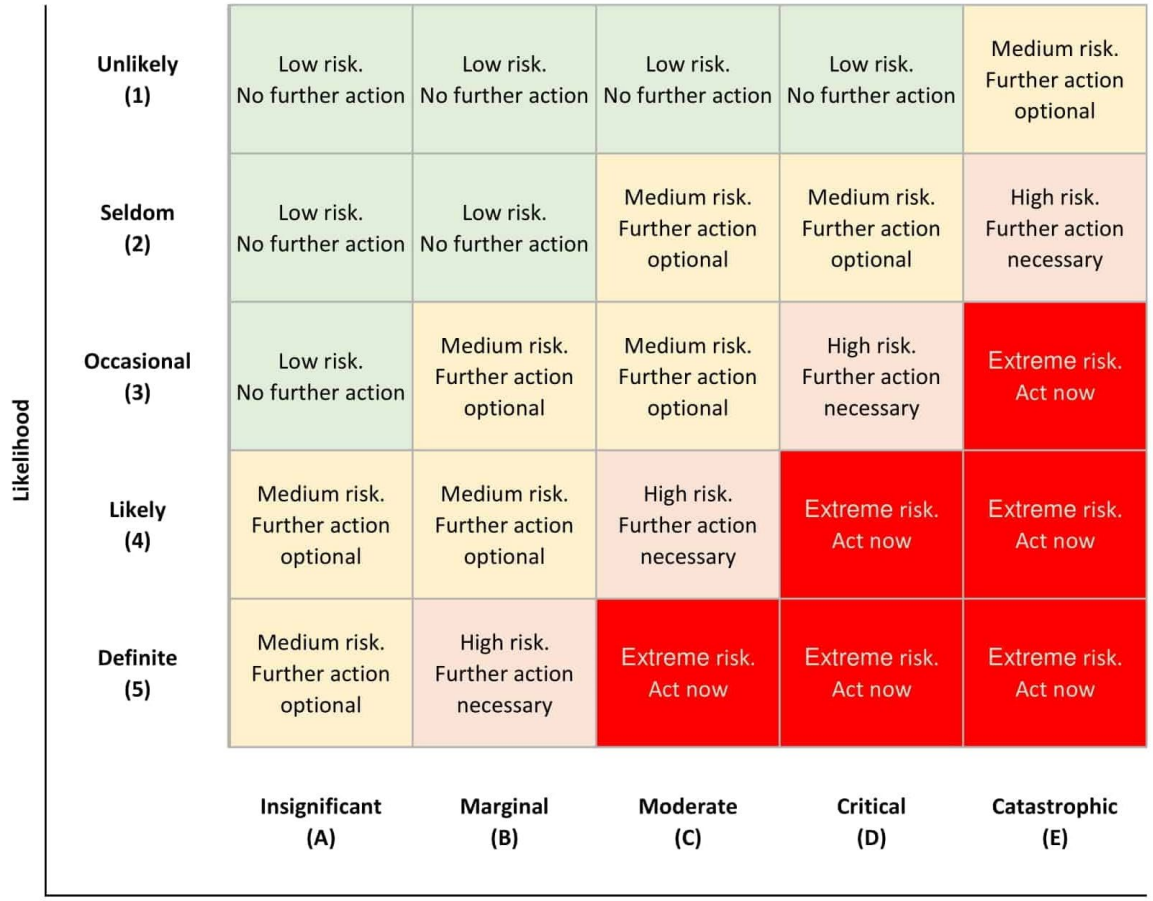


COMMON RISK MATRICES

- Another variant is the 4x4
- This matrix assigns a numerical value for both probability and severity
  - This produces a risk score ranging from 16 (4 x 4) to 1 (1 X 1)
- This is still qualitative
  - The values are not computed from data
  - They are still ordinal
  - Often used to support automation and data analysis

COMMON RISK MATRICES

- This is a 5x5 matrix
- Incorporates a risk management decision to prioritize responses
- These examples show there is no "correct" form of a risk matrix
  - They all express the idea of computing risk as a combination of likelihood and outcome
  - The actual risks will depend on how we choose to define and classify them
  - That is what we need to get right in a risk assessment



QUANTITATIVE RISK MATRICES

- Quantitative matrices use data to assign the frequency and outcome values
  - These values are derived from existing data
  - Often based on some mathematical model; a regression analysis for example
- The model might incorporate
  - Analyses of historical data to predict the likelihood of an event
    - This could be expressed as a probability of the event occurring
  - A set of impacts on affected populations based on historical occurrences
    - For example, historical records of the dollar value of damage for similar events
  - Results in a more comprehensive description of the risk
  - The next page shows a quantified risk matrix from the liquid natural gas industry
- No matter how detailed or precise the risk matrix is
  - It doesn't tell us how to manage risk or reduce the risk
  - Requires a standard set of concepts, procedures and strategies for responding to risk

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

ALTERNATIVE TERMINOLOGY

- Our discussion so far
  - Has used the idea of events that could occur and the likelihood of occurance
- Another way of describing this:
  - There exist *threats* to the organization
    - These are still events but emphasizes the negative nature of the event
    - A power outage is a threat, so is a hacker attache
  - Threats are exploited through vulnerabilities
    - A vulnerability represents the outcome
    - The more vulnerable we are correlates with the negative impact of the threat
    - Mitigating the vulnerability reduces the effect of the threat
  - For example
    - An earthquake represents a threat to our data center
    - Locating the data center near a fault line is a vulnerability

RESILIENCE CONCEPTS

- Resilience refers to how a system deals with negative events and returns to normal operations
- Resilience is not about avoiding negative events
  - Accepts the fact that negative events will occur and will impact the system
  - The system absorbs these events with no or only minimal loss
  - The system recovers from the event with minimal effects
    - If the system goes down in whole or part, its function can be restored quickly
- 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 the resilience of the system ensures it is consistently available and operational

RESILIENCE

- Basic themes in resilience operations
  - *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 execute failover plans
  - *Adapt*: Learn from incidents and improve
    - Improves the reliability of the system
- Like risk management, resilience needs
  - Standard concepts, procedures and protocols, including assessment tools
  - Constant improvement in the resilience processes and procedures
  - To be integrated across systems and coordinated with other functional areas

ISACA IT RISK FRAMEWORK

- Purpose of a framework
  - Turns risk intuition into repeatable, outcome driven practices
- Benefits of a formal framework
  - *Consistency*. Everyone scores, prioritizes, and responds to risks in a standardized manner across teams and over time
  - *Comparability*. Trade-offs can be evaluated across products, systems, and business units
  - *Defensibility & auditability*. Clear decision trails
    - Regulators and auditors can trace the logic and the actions taken
  - *Bias reduction:* Structured steps help avoid bias such as:
    - *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

- Benefits of a formal framework (cont)
  - *Speed with quality:* Templates and best practice allow previous experience to be leveraged to provide faster, more efficient and effective responses in the future
  - *Risk appetite:* Actions taken correlate with the organization's acceptable risk policies rather than informal gut feelings or individual one-off decisions
  - *Governance integration:* Allows for integration with governance processes, KRIs/KPIs, incident/BC/DR processes (business continuity and disaster recovery)
  - *Communication*: Content is packaged appropriately for the different audiences
    - Executives get business-impact summaries
    - Engineers get actionable control guidance
    - Regulators get standardized compliance reports

FORMAL VS INFORMAL DEFINITIONS

- Risk
  - Informal
    - "Something bad might happen because…"
    - *"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"
    - *" 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
    - "Unless we put this security feature into place, bad things will happen"
    - *"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"
    - *"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 deal with this security issue"
    - *"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
    - "We dodged a bullet this time"
    - *"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:
    - "All the risk we face before we do anything"
    - *"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
    - "The risk left over after we apply controls"
    - *"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"
    - *"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 before we start to panic"
    - *"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”
  - Programmers can write C code on a UNIX system that would crash or brick the system
  - This requires a high risk tolerance
- Doug Gwyn explains why
  - *“Unix was not designed to stop you from doing stupid things, because that would also stop you from doing clever things”*
  - Risk management is the programmer’s responsibility, not the operating system’s responsibility

RISK CATEGORIES

- Different industries have different risk categories
  - But there are commonalities across industries
  - The focus in this course is on the financial services industry
- Enterprise Risk Management (ERM) categories
  - *Strategic:* risks that affect achievement of high-level goals aligned with mission/strategy
    - For example: Deploying AI tools that negatively impact the core business processes
    - For example: Transforming the IT infrastructure produces deadlocks in developments
  - *Operations:* risks from day-to-day processes, people, systems, or external events that impair effective and efficient operations
    - For example: Outages, control breakdowns, failure to respond to security events
    - For example: Failed updates to production systems, configuration errors

RISK CATEGORIES

- Enterprise Risk Management (cont)
  - *Reporting:* risks that reports are unreliable, incomplete, or untimely
    - For example: delayed suspicious activity reporting (SAR)
    - For example: data quality errors in financial consolidation reporting
  - *Compliance:* risks of compliance failures with regulators
    - *For example:* risks of violating laws, regulations, or internal policies about privacy, AML, or consumer-compliance technology issues

RISK CATEGORIES

- ISACA has four main categories
- Benefit enablement risk:
  - The risk that technology-enabled initiatives don't deliver the expected business value
    - For example: customer loss because of difficult to use automated systems
    - For example: operations monitoring tools do not improve efficiency in the production operations environment
- Program and project delivery risk:
  - The risk that programs or projects fail on scope, time, cost, or quality
  - Causes business disruption or lost opportunities
    - For example: The development process for new applications is disorganized and inefficient
    - For example: Rolling out a new application is overdue and is unusable for some users

RISK CATEGORIES

- Operations and service-delivery risk:
  - The risk that day-to-day IT services underperform or fail
    - For example: the new customer relations system regularly hangs, annoying customers
    - For example: data required for executives decisions is late or inaccurate
- Cyber and information security risk
  - The risk from threats to information and technology
    - For example: confidentiality, integrity, availability
    - For example: cyberattacks and unintended exposure of confidential data

RESILIENCE

- Differences between risk and reliability/resilience
  - Risk management focuses on preventing things from going wrong
  - Reliability focuses on maintaining normal operations when things go wrong
    - For example, systems that reject bad data that has the potential to crash operations are reliable because they continue to function even when given corrupted input
  - Resilience is about absorbing bad events and getting back to normal fast
    - If bad data does crash the system, it reboots and is online with minimal downtime
  - Resilience is about expecting failure, limiting the fallout, and returning to service predictably so customers and the business keep operating
  - Reliability tries to avoid failure
  - Resilience assumes failure will happen and focuses on recovery from the failure

RESILIENCE

- Security vs. Resilience
  - Security reduces the likelihood of attacks by an adversary will succeed
  - Resilience reduces the impact and duration of the effects of an attack on the system
- Redundancy vs. Resilience
  - Redundancy is a tool (extra capacity, backups)
  - Resilience is the strategy that decides where and how to use redundancy 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 the organization must restore an activity/service to an acceptable level after a disruption
  - The amount of down time needed to be back up enough to continue operations
- RPO (recovery point objective)
  - How much data the organization can afford to lose
  - Expressed as a point in time that the process must be able to roll back to
    - For example: "no more than 5 minutes of orders lost"

RESILIENCE DEFINITIONS

- MTPD (maximum tolerable period of disruption)
  - Beyond this duration, the impact on the business becomes unacceptable
  - Outer limit for a disruption before the the business suffers loss
  - 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
    - For example: “process 20% of payments during system recovery”
  - The 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 is 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:
    - Ssynchronous replication for auth logs, hot-hot routing, automated failover playbook

BANK EXAMPLE

- Trade confirmations portal:
  - MTPD: 24 hours
  - RTO: 4 hours
    - Read-only mode acceptable initially
  - RPO: 15 minutes
    - Rreplayable from upstream book of record
  - Resilience Planning:
    - Ffrequent backups + near-real-time replicas; runbook for read-only mode

BUSINESS IMPACT ANALYSIS

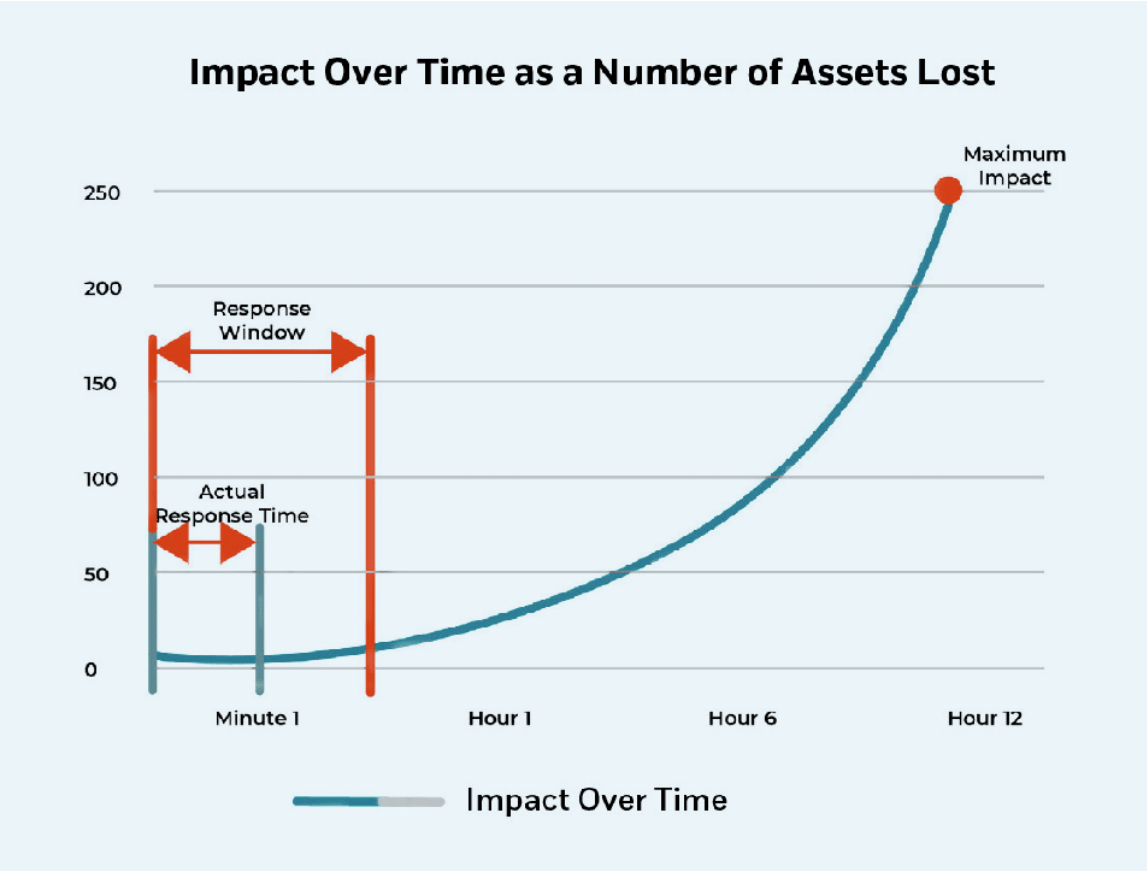
- Structured way to assess how bad things get over time when a business activity or IT service is disrupted
  - Quantifies the impact: financial, customer, regulatory, operational dimensions
  - Used to set targets for resilience planning, specifically
    - RTO: How fast the system must be back to a minimum level
    - RPO: How much data the business can afford to lose
  - Identifies
    - Which services matter most
    - How quickly does pain escalate
    - What recovery promises have to be kept
  - Also useful for discovering risks

BUSINESS IMPACT ANALYSIS

- BIA key outputs
  - Criticality tier for each related or dependant service or application
    - An evaluation of how important each service is to maintaining business continuity
    - Tier 1 “mission critical,” Tier 2, etc.
  - Impact curve over time
    - Scale of tolerable service degradation to severe service degradation that are unacceptable after X hours
    - A measure of how the impact to the business gets worse over time
  - MTPD/MAO for each activity
    - Defines the outer limit for what is acceptable
  - RTO and RPO targets:
    - Defines the targets are that are to be designed to and tested against

BUSINESS IMPACT ANALYSIS

- BIA key outputs
  - Criticality tier for each related or dependant service or application
    - An evaluation of how important each service is to maintaining business continuity
    - Tier 1 "mission critical," Tier 2, etc.
  - Impact curve
    - Scale tracking service degradation over time from tolerable service degradation to unacceptable
    - Measure of how the impact to the business gets worse over time



BUSINESS IMPACT ANALYSIS

- Minimum Business Continuity Objective (MBCO):
  - The minimum acceptable service level during disruption
  - Although service might be degraded, defines how much can be tolerated before business failure
- Dependency map
  - Identifies the people, locations, technology, data and third parties that are involved
- Regulatory/contractual constraints
  - Identifies the legal and compliance issues that have to be taken into account
  - What the business can tolerate as MBCO might not be acceptable to regulators
- Prioritized recovery order and data protection needs
  - What needs to be done first
  - How to protect the data assets
- Assumptions and residual risks
  - Identifies what could still go wrong even if after recovery
  - For example, determining if an outage 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 that are involved
    - Applications, databases, payment rails, call center, branches systems
  - Pick impact criteria describing the impact of failure along various dimensions
    - 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
    - For example: "Regulatory breach likely" = level 4
  - Collect reference data:
    - Past incidents, SLAs, volumes, cutoffs, market windows
    - For example : payment settlement times, control test results, known issues

HOW TO RUN A BIA

- Phase 1: Prepare (cont)
  - 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, net promoter score drop, executive attention
    - *(Optional) Safety/People*: rarely used in IT-only outages, but included if relevant

HOW TO RUN A BIA

- Phase 1: Prepare (cont)
  - 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 and validate (2–4 weeks)
  - Interviews/workshops: With business owners and tech leads (Dev/SRE/DBA/Network/IAM)
  - Use 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 and 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 multiple services are down, identify the order in which they should be restarted
  - Validate feasibility with IT:
    - Can the current architecture meet RTO/RPO?
    - If not, document the gaps, options, and costs to make it compliant

HOW TO RUN A BIA

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

HOW TO DETERMINE RTO

- Scope the activity
  - Name the business service
    - For example: card authorizations
  - And the IT stack that supports it
    - For example: apps, DBs, networks, vendors
- Execute a BIA
  - Quantify impact as a function of outage time
    - For example: financial, customer, regulatory, operational
  - Identify the MTPD/MAO: the point at which impact becomes unacceptable
- Set a measurable target
  - Pick the RTO < MTPD that reflects the minimum acceptable level of service (MBCO).
    - Example: “15 minutes to read-only balances, 60 minutes to full function”

HOW TO DETERMINE RTO

- Check external constraints
  - Regulatory rules, customer SLAs, market hours, and cutoffs like payment settlement windows may force a tighter RTO
- Design to the number
  - Choose strategies that can actually meet the RTO
    - For example, 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
  - The records that are affected
    - For example: orders, trades, auth logs
  - How often they are updated – rate of change
  - How they are reconciled if the data is lost
- Establish the tolerance
  - With business owners, set the largest acceptable loss window
    - For example: "≤ 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 dictates the RPO for all the other related systems
- Prove recoverability
  - Run point-in-time restores and message replays to show you can recover on before the specified 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
- Tiers
  - Not every component needs the same target
  - Design graceful degradation
  - For example, read-only mode meets RTO for one components while other features catch up on meeting their RTO

RISK CONTRIBUTION

- Implicit in the discussion of resilience
  - The assumption is that 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 for discovered risk
    - *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

Q&A AND OPEN DISCUSSION