RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

RISK GOVERNANCE

This module introduces and explores some of the foundational concepts of risk governance

- Risk appetite
- Risk tolerance
- Risk capacity
- Risk culture

INTRODUCTION

- Risk governance
  - While pursuing strategic objectives, organizations have to determine
    - How much risk the organization is prepared to undertake
    - How much risk the organization can absorb and tolerate
  - Risk governance sets the appropriate level of risk to optimize operations
  - ISACA definitions
    - *Risk Appetite:* How much risk the enterprise is willing to undertake
    - *Risk Tolerance:* The acceptable range of risk induced deviation from objectives
    - *Risk Capacity:* The maximum risk related losses the enterprise can bear before its viability is threatened
    - *Risk Culture:* The shared values, norms, and behaviors that shape how people in the organization identify, assess, and respond to risk
  - Similar concepts exist across risk standards and frameworks
    - Each standard or framework provides its own formal definition
    - The various definitions restate these ideas, tailored to their specific audiences

RISK APPETITE

- Risk appetite
  - The broad-based amount of risk an entity is willing to accept in pursuit of value
  - For example
    - *"Although the enterprise desires to have no appetite for IT risk, it recognizes that this is impractical in the achievement of its objectives. Therefore, the enterprise will remediate loss scenarios in which aggregate losses of $1 million or more are at risk."*
  - Dimension of risk appetite
    - Objective capacity to absorb loss across multiple asset categories
    - For example: capital adequacy, liquidity, reputation, operational assets
    - Management's predisposition to risk: cautious vs. aggressive culture
    - Nature of business and risk types: operational, cyber, credit
    - Risk appetite can vary across business functions or categories within an organization
  - Best practices
    - Risk appetite must be quantified in order to support risk decisions
    - Reviewed periodically to reflect changes in the organization and/or business environment
    - Integrated into IT governance, investment, and cybersecurity planning

RISK TOLERANCE

- Risk tolerance
  - The acceptable variation in actions relative to objectives that would result from accepting risks
  - Sets “guardrails” to define acceptable levels of risk for specific operations or actions
  - Translates risk appetite into measurable performance indicators such as KPIs or SLA limits
  - Example
    - *“Projects are to be completed within estimated budgets and timeframes, but overruns of 10 percent of budget or 20 percent of time are tolerated.”*
  - Relationship to appetite
    - Risk appetite = strategic-level willingness to take risk at the enterprise level
    - Risk tolerance = operational thresholds of acceptable deviation at the business unit

RISK CAPACITY

- Risk capacity
  - The amount of loss an enterprise can tolerate without risking its continued existence
    - It represents the upper bound beyond which potential losses due to risk threaten survival of the enterprise
  - Sustainable scenario
    - Risk capacity > risk appetite > actual risk
    - When actual risk exceeds capacity, resilience and solvency are threatened
  - Quantitative measurement of operational continuity capability
    - Defines the ceiling within which appetite and tolerance are set
    - Banks often align this with regulatory ratios

RISK CULTURE

- Risk culture
  - The collection of behaviors and values that support open risk discussions and consistent adherence to risk policies
  - A risk-aware culture
    - Promotes open discussion of risk
    - Ensures alignment between policies, appetite, and actual behavior
    - Recognizes risk-taking as necessary for innovation, but within managed limits
  - Key behaviors
    - *Proactive identification:* Early escalation of risk indicators
    - *Ownership and accountability:* All staff own risk, it's not just the responsibility of IT or compliance
    - *Transparent communication:* Avoid hidden agendas and blame culture
    - *Alignment with objectives:* KRIs and decisions aligned with enterprise goals
    - *Learning from negative outcomes:* Post-incident reviews that address root causes

RISK CULTURE

- Risk culture
  - Symptoms of poor risk culture
    - Misalignment between appetite, tolerance, and policy
    - Failure to enforce risk policies
    - A blame culture that discourages transparency and collaboration
- Summary
  - Risk capacity = maximum loss the organization can survive (CFO / CRO)
  - Risk appetite = desired level of risk to achieve strategy (board / exec mgmt)
  - Risk tolerance = operational thresholds of tolerated variation (business units)
  - Risk culture = Norms influencing behavior toward risk (everyone)

CORRELATION WITH RESILIENCE

Risk Concept	DRII Resilience Correlate	Explanation
Risk Capacity	**Impact Tolerance / Maximum Acceptable Outage (MAO)**	Determines the organization's survivability limits — how long critical functions can be interrupted before causing irreversible harm.
Risk Appetite	**Strategic Resilience Objectives**	Defines how much disruption or exposure management is willing to accept to maintain competitiveness (e.g., acceptable downtime, data loss).
Risk Tolerance	**Recovery Time Objectives (RTOs)**	Operational boundaries within which systems must recover; mirrors tolerance thresholds.
Risk Culture	**Resilience Culture & Governance**	A culture that values preparedness, learning from incidents, and cross-functional collaboration ensures resilience integration across the enterprise.

THEORY VS REALITY

- The concepts presented so far are theoretical
  - But the ability to be effective in each of these areas depends on the process maturity of the organization
  - The maturity definition recap below describes the process of becoming risk culture “mature”

Level	Description	Keywords
1. Initial (Ad Hoc)	Processes are unstructured, reactive, unpredictable.	Firefighting, inconsistent, individual heroics
2. Repeatable	Basic processes exist and are partially documented; some consistency.	Procedural, partially controlled
3. Defined	Processes are standardized, documented, and communicated.	Institutionalized, proactive
4. Managed (Quantitative)	Metrics are used to monitor and control risk and performance.	Data-driven, measured
5. Optimized (Continuous Improvement)	Processes are continuously improved using quantitative feedback.	Predictive, resilient, adaptive

RISK APPETITE AND MATURITY

Maturity Level	Characteristics of Risk Appetite	Capability Impact
1 – Initial	No formal risk appetite statement. Risk decisions made individually or reactively.	Organization cannot articulate acceptable risk; exposure is inconsistent.
2 – Repeatable	Management begins to express appetite qualitatively ("we are risk-averse").	Risk-taking guided by intuition, not metrics. Strategic alignment limited.
3 – Defined	Risk appetite formally approved by board and cascaded through units.	Enables alignment between IT and enterprise strategy. Basic governance established.
4 – Managed	Appetite quantified (e.g., $ thresholds, metrics, KRIs). Linked to capital, compliance, and performance data.	Decisions are consistent, traceable, and auditable. Enables proactive management.
5 – Optimized	Appetite dynamically adjusted based on environmental scanning, predictive analytics, and resilience objectives.	Organization uses risk appetite to guide innovation and resilience investments.

Reliability correlation:

At Levels 4–5, systems are designed with *measurable reliability targets* (e.g., RTOs, SLAs) that align with quantified appetite for downtime or service loss.

RISK TOLERANCE AND MATURITY

Maturity Level	Characteristics of Risk Tolerance	Capability Impact
1 – Initial	No defined tolerance thresholds. Risk responses vary by individual manager.	High volatility in outcomes; compliance and reliability are inconsistent.
2 – Repeatable	Some project-level tolerances defined (e.g., cost/time overruns).	Partial control achieved but no enterprise alignment.
3 – Defined	Enterprise-wide risk tolerance limits approved and documented.	Enables comparison across units; consistent risk reporting.
4 – Managed	Tolerance integrated with KRIs and KPIs; monitored continuously.	Supports data-driven resilience decisions (e.g., automatic triggers for mitigation).
5 – Optimized	Tolerance dynamically linked to risk analytics, AI/ML forecasting, and scenario modeling.	Enables adaptive resilience; organization balances risk and opportunity optimally.

Reliability correlation:

At higher maturity, **risk tolerance thresholds align with reliability objectives** — e.g., "system uptime must not fall below 99.95%" becomes both a tolerance and a reliability metric.

RISK CAPACITY AND MATURITY

Maturity Level	Characteristics of Risk Capacity	Capability Impact
1 – Initial	No clear understanding of maximum risk exposure or loss absorption.	Financial or operational shocks can threaten survival.
2 – Repeatable	Some awareness of limits (e.g., budget, compliance penalties).	Risk capacity treated as static; no link to resilience or capital planning.
3 – Defined	Capacity quantified based on financial, technical, and human resources.	Enables setting realistic risk appetite boundaries.
4 – Managed	Capacity dynamically assessed (e.g., stress testing, scenario planning).	Organization can plan resilience capacity (redundancy, liquidity buffers).
5 – Optimized	Real-time monitoring of operational capacity; integration with resilience indicators (MAO, RTO, MTBF).	Organization operates within its adaptive capacity, ensuring continuity even under duress.

Reliability correlation:

At Level 5, **risk capacity = resilience capacity** — the ability to sustain operations under stress without exceeding failure thresholds.

RISK CULTURE AND MATURITY

Maturity Level	Characteristics of Risk Culture	Capability Impact
1 – Initial	Reactive, blame-oriented culture. Risk seen as failure.	Employees hide incidents; low transparency; weak learning from failure.
2 – Repeatable	Some risk awareness, but accountability unclear.	Limited risk communication; siloed IT and business teams.
3 – Defined	Leadership communicates risk values; roles and responsibilities clear.	Collaboration and learning begin; early resilience mindset forms.
4 – Managed	Risk culture measured through surveys, training, and behavioral indicators.	Risk-taking becomes calculated; culture supports adaptive response.
5 – Optimized	Culture of continuous learning and cross-functional trust. Risk and resilience are embedded in decision-making.	Organization achieves *resilience by design* — every level anticipates and adapts to change.

Reliability correlation:

A mature risk culture ensures reliability through **shared accountability, transparent reporting, and a learning orientation**, which reduces recurrence of incidents and accelerates recovery.

MATURITY VS. RESILIENCE CAPABILITY

Maturity Level	Risk Governance State	Resilience Capability
1 – Initial	Reactive, fragmented; no defined appetite or culture.	Fragile — dependent on individual heroics.
2 – Repeatable	Some processes; partial alignment.	Recoverable but inconsistent.
3 – Defined	Policies institutionalized; shared understanding.	Sustainable resilience achievable with structured BCP.
4 – Managed	Quantitative control, predictive monitoring.	Measurable reliability; proactive continuity management.
5 – Optimized	Integrated, adaptive, and learning organization.	Resilient-by-design; reliability engineered into business processes and IT.

MATURITY IMPLICATIONS

- Maturity drives control
  - Without process maturity, risk frameworks remain theoretical
- Quantification enables resilience
  - Risk appetite and tolerance translate into measurable reliability and resilience goals
- Culture amplifies capability
  - A mature risk culture transforms risk awareness into resilient behavior
- Risk capacity defines operational limits
  - Resilience planning begins by understanding the true risk capacity of critical functions
- Integration is the goal
  - Risk and reliability management converge under a unified resilience framework

RISK CULTURE

- The result of combination of external and internal factors
- External or environmental
  - Sets boundaries, incentives, pressures, and references for “acceptable” risk behavior
    - Regulatory environment
    - Legal and compliance pressures
    - Industry norms and peer benchmarking
    - External stakeholder expectations
    - Macro geopolitical environment
    - National culture and societal norms

RISK CULTURE

- Internal or organizational
  - Shape day-to-day behaviors, decision processes, risk escalation, and collective mindsets
    - Leadership behavior and tone from the top
    - Incentives, performance measurement and rewards
    - Governance structure and oversight
    - Communication and information flows
    - Subcultures and functional silos
    - Historical incidents and “lessons learned”
    - HR practices: hiring, onboarding, training
    - Formal systems and control architecture

RISK EXTERNAL CULTURE

- Regulatory
  - Supervisory regime and enforcement intensity
    - Banking and financial services regulators often impose culture and conduct expectations as part of regulatory guidance or exams
    - For example *"culture of compliance"* and "*risk culture expectations"*
  - Threat of regulatory penalties, fines, or reputational sanctions motivates organizations to embed risk culture more robustly
  - In environments with weak enforcement, organizations may pay lip service to "risk culture" while focusing compliance efforts on ticking boxes
  - Example
    - A bank subject to regular regulatory audits may emphasize rigorous risk escalation and whistleblower frameworks
    - A non-regulated technology firm might have more latitude to undertake risk without triggering external attention or investigations

RISK EXTERNAL CULTURE

- Industry norms
  - Peer benchmarking and competitive pressures
    - Peer benchmarking: comparing an organization's performance, processes, or risk posture against similar organizations
  - Industries with high reputational risk have peer expectations that create norms
    - High reputation risk example, banking, insurance, pharmaceuticals, energy
    - Fore example: *"Every major bank must have a 'first-line, second-line, third-line' risk culture*."
  - Benchmarking reports create aspirational pressure
    - For example: *"Top-tier banks have X maturity level in risk culture"*
  - If competitors tolerate more risk or cut corners
    - Can either erode culture by triggering a "race to the bottom"
    - Or provoke stronger counter-measures to differentiate on trust

PEER BENCHMARKING

- Peer benchmarking
  - Measuring the organization against comparable institutions
    - For example, banks compare their incident response times, cybersecurity controls, recovery objectives, or capital/risk exposure to other banks of similar size and complexity
  - Identifying gaps and leading practices
    - If peers have stronger resilience testing, stricter third-party oversight, or faster notification capabilities, regulators may expect the organization to close the gap
  - Providing evidence to regulators and auditors
    - Benchmarks help show that the organization's risk posture is not only internally acceptable but also aligned with industry norms and supervisory expectations
  - Supporting KRIs, governance, and strategic decisions
    - Metrics like RTOs, vendor performance, staffing levels, or breach frequency are benchmarked to evaluate whether the organization's targets and thresholds are realistic and defensible

PEER BENCHMARKING

- Goals of peer benchmarking
  - To ensure firms don’t fall significantly behind industry norms
  - To encourage consistent practices across institutions
  - To identify systemic weaknesses across a sector
  - To justify improvements, resources, or investments in controls

RISK EXTERNAL CULTURE

- Legal
  - Occurs in jurisdictions with strict liability, class-action exposure, or heavy litigation
  - Organizations may become excessively risk-averse and suppress open discussion of near misses
  - In environments with weak liability, there is less external pressure to report or escalate issues
- Macro-economic
  - Volatility in the economy forces more frequent, severe stress events
    - For example: volatility in financial markets, cyber threat landscape or geopolitical risk
    - Organizations in volatile environments often develop “risk hardiness” or more conservative cultures
    - More stable environments might breed complacency, overconfidence, or “it won’t happen to us” attitudes

RISK EXTERNAL CULTURE

- Societal culture
  - Differences in national culture shape
    - How people interpret authority
    - Whether they feel safe reporting bad news
    - Whether questioning the chain of command is acceptable, etc.
  - An empirical study found that national culture, industry type, and organizational security culture significantly influence individuals' security behavior

RISK INTERNAL CULTURE

- Tone from the top
  - Leadership actions speak louder than policies
    - If senior executives bypass controls, dominate decisions without discussion, or penalize risk disclosure, they undermine culture
    - When the board or CEO publicly demands risk transparency, participates in discussions, and visibly supports risk escalation, that sets a cultural anchor
  - In studies of ERM sophistication, organizations where leaders push for stronger oversight show higher maturity in risk culture

RISK INTERNAL CULTURE

- Incentives
  - Misaligned incentives generate cultural tension between actions mitigating risk
    - For example: rewarding revenue growth without penalizing risk overruns
  - Risk management failure arises when short-term individual incentives conflict with long-term enterprise risk appetite.
  - If risk controllers or compliance units are not part of performance evaluations, their voice may be sidelined

RISK INTERNAL CULTURE

- Governance structure
  - Where risk governance is weak culture is less capable of intervening
    - For example: Risk committees that never challenge or risk functions under powered
  - Clear accountability lines and escalation paths matter: who owns risk, who can override, who judges exceptions
  - Frequency and seriousness of oversight affect how risk culture stays alive day to day

RISK INTERNAL CULTURE

- Information flow
  - A “speak-up” environment where there are channels for escalation, anomaly reporting, whistleblowing
  - If information is hoarded in silos or filtered upward aggressively, senior leadership gets distorted views
  - Informal networks, like power centers and shadow communication channels, can override formal governance.
    - McKinsey notes that informal networks often influence how formal risk channels operate in practice

RISK INTERNAL CULTURE

- Functional silos
  - Large organizations often have multiple micro-cultures
    - For example: development, operations, risk, audit
  - These different micro-cultures may have varying attitudes to risk
  - This can create subculture conflict
    - For example: DevOps striving for rapid release conflicts with security requiring cautious rollout
- Historical memory
  - Past failures, “near misses,” or regulatory fines leave cultural legacies
    - Either fear-based suppression or learning orientation based on transparent root cause reviews
  - Organizations that do after-action reviews, “lessons learned” loops, and close the loop by changing practices build a stronger risk culture over time

RISK INTERNAL CULTURE

- Control systems
  - The architecture of controls, systems, metrics, dashboards, and analytics reinforce or weaken culture
  - If control systems are opaque, overburdensome, or disconnected from decision-making, they may generate bypassing or cynicism
  - The strength of risk measurement, like KRIs and predictive analytics, can influence how visible risks are, and how credible the risk function is

APPETITE VS. TOLERANCE

- Risk Appetite
  - Strategic-level statement of how much risk and of what types an organization is willing to accept in pursuit of its objectives
    - Forward-looking, aspirational, and reflects the risk culture
- Risk Tolerance
  - Translates risk appetite into operational thresholds or boundaries of acceptable deviation
  - Quantifies appetite within a framework of real world constraints

FACTORS INFLUENCING RISK APPETITE

Factor	How It Shapes Appetite	IT / Banking / Security Implications
Strategic Objectives & Growth Ambitions	If an organization is targeting aggressive growth, innovation, or market disruption, its appetite must allow for higher volatility. Conversely, if strategy is preservation, risk appetite is more constrained.	A bank pushing into fintech, open banking, or new digital services may adopt higher appetite for cybersecurity and technology risk to compete.
Financial Strength / Capital Buffer	Organizations with robust capital, liquidity reserves, and strong balance sheets can more comfortably absorb losses and thus support higher appetite.	In banking, regulatory capital (Basel, stress testing) constrains how much risk you can take. Appetite must respect capital adequacy.
Risk Capacity / Loss Absorption Capability	Honest assessment of maximum tolerable loss (financial, reputational, operational) acts as an upper bound on appetite. If capacity is low, appetite must be modest.	Security failures, data breaches, outages, or compliance fines can push appetite downward—if remediation budgets are limited, appetite must be conservative.
Stakeholder Expectations & Risk Tolerance	Investors, regulators, rating agencies, customers, and board members all have implicit or explicit expectations about acceptable risk. Their attitudes can pull appetite higher or lower.	A bank's board may demand "zero tolerance" for certain risks (e.g. AML, data privacy), constraining appetite in those domains even if other domains allow more risk.
Regulatory and Compliance Regime	Strict regulatory frameworks, exposure to sanctions, oversight intensity, and enforcement actions push appetite downward (i.e. risk of penalty is a deterrent).	In banking, rules like Dodd-Frank, FFIEC, GDPR, consumer protection, and examination regimes force more conservative appetite in many risk domains.

FACTORS INFLUENCING RISK APPETITE

Industry Norms & Competitive Pressure	If peers or competitors are taking bold moves or embracing new technologies, an organization may feel pressure to take on more risk to remain competitive.	In banking and fintech, being "too conservative" might mean losing ground to more aggressive digital banks or fintech challengers.
Leadership Mindset, Risk Attitudes, and Board Culture	The risk appetite is often set or strongly influenced by CxOs and the board. Their personal risk propensities, tolerances for uncertainty, and biases (e.g. overconfidence) will shape the appetite.	A CEO with a strong growth orientation might push for higher appetite, while a risk-averse board chair might constrain it. The RARA model (risk appetite + risk attitude) speaks to this interplay. Project Manage...
Past Experience, Loss History & Organizational Memory	Prior bad events or near-misses tend to dampen appetite (more conservatism). Conversely, a legacy of success in navigating risk can foster confidence to take more.	A bank that survived a cyberattack may reset appetite lower in security domains; or conversely, if it handled the attack well, it may push forward with more ambitious security innovations.
Macroeconomic / Market / Environmental Conditions	External uncertainty, volatility, macro shocks, geopolitical risks, or emerging threats can cause appetite to shrink. During "boom times", appetite often expands.	In times of credit stress or market turbulence, banks often scale back risk appetite (e.g. reduce lending exposures, tighten cybersecurity posture).
Technology / Innovation Imperative	If technological disruption is a competitive necessity, appetite must allow for experimentation, testing, and tolerance of failure.	A bank adopting AI, blockchain, or open banking APIs must accept more risk, particularly in data, privacy, integration, and vendor risk.
Reputational / Brand Risk Sensitivity	If brand damage is especially costly, appetite in areas that affect customer trust or regulatory standing will be more constrained.	A large bank is very sensitive to brand; a security breach or scandal can erode customer and regulatory trust, so appetite in cyber / data

FACTORS INFLUENCING RISK TOLERANCE

Factor	How It Shapes Tolerance/Thresholds	IT / Security / Banking Implications
Risk Appetite Boundary / Strategic Direction	Tolerance must be consistent with appetite; it operationalizes the broad appetite into measurable limits.	If appetite is "moderate risk in fintech experimentation," tolerance may allow up to X% downtime, X breach incidents, etc.
Quantitative Analysis & Historical Data	Analytics, loss distributions, scenario modeling, stress testing, historical incident frequency/severity help calibrate what tolerances are credible.	Security teams may model expected incidence rates, mean time between failures, and set tolerances (e.g. "10 medium vulnerabilities open at any time").
Measurement Capability / Data Quality	Tolerance requires good metrics, data collection, dashboards, and reporting. Without measurement, you can't set informed tolerances.	A bank with mature security telemetry and SIEM / dashboarding can set tighter, more responsive tolerance thresholds; immature organizations must set loose tolerances.
Risk Capacity / Buffer Margins	The more "buffer" you have (financial, operational, reserve), the more slack you can allow in tolerance. Conversely, tight capacity means stricter tolerance.	In a stressed liquidity scenario, tolerance for losses might shrink; capacity-driven constraints force tighter tolerances in security investments.
Operational Constraints & Dependencies	Interdependencies (between systems, business units) and technical constraints limit how much deviation can be tolerated.	For core banking transaction systems, tolerance for downtime is extremely strict; for less critical systems it might be more relaxed.
Cost / Cost of Control / Remediation Costs	Increasingly strict tolerances often require expensive controls or remediation; the marginal cost of tightening tolerance affects where tolerance lines are drawn.	If lowering tolerance for certain vulnerabilities demands heavy investment in tools or architecture, risk leaders must balance cost vs reduction in risk.

FACTORS INFLUENCING RISK TOLERANCE

Remediation Costs	remediation; the marginal cost of tightening tolerance affects where tolerance lines are drawn.	investment in tools or architecture, risk leaders must balance cost vs reduction in risk.
Escalation / Governance Mechanisms	Tolerance must be aligned with governance structures: who can approve exceptions, who responds when threshold is breached, and how quickly remediation must happen.	If tolerances are too strict but governance is weak, many breaches might be elevated constantly — leading to "alert fatigue" and erosion.
Stakeholder / Regulatory Mandates	Some tolerance thresholds may be externally mandated (e.g. regulatory limits, capital ratios, downtime SLAs).	E.g. banking regulators may require zero tolerance for certain kinds of operational or compliance breaches; these become non-negotiable tolerances.
Cultural / Behavioral Tolerance for Deviation	The "wiggle room" allowed by culture — some organizations are more comfortable with deviations and exceptions; others believe in tight compliance.	If an organization has been tolerant historically of "bending rules," its operational tolerance thresholds may be looser (for better or worse).
Coordination with Resilience / Business Continuity Goals	Tolerance should reflect recoverability objectives (RTOs, RPOs, MAO) — i.e. how long or how much deviation can be absorbed before harm is unacceptable.	Tolerance for system downtime must align with derived business impact tolerances — e.g. no more than X hours.
Time Horizon / Exposure Window	Tolerance may vary depending on short-term vs long-term exposures. A higher short-term deviation might be accepted if expected long-term trend is acceptable.	E.g. temporary performance degradation may be tolerated if long-run security posture remains below certain risk thresholds.

RISK TOLERANCE

- Tolerance is often expressed in dual limits
  - Minimum and maximum, or multi-dimensional thresholds like financial, time and severity dimensions
    - Minimum limits prevent total risk avoidance policies and behaviors
- Tolerances must be reviewed and recalibrated periodically
  - As systems evolve and threat profiles shift, tolerances that were once acceptable may become dangerous
- Measurement or monitoring may be immature
  - Organizations may define coarse tolerances like low/medium/high bands rather than quantified numerical thresholds

RISK TRADE-OFFS

- Appetite vs capacity constraints
  - No matter how ambitious appetite is, it must not exceed capacity or the organization becomes in danger of insolvency or collapse
- Tolerance cost vs benefit
  - Tightening tolerance with smaller deviations often increases control and remediation costs
- Strategic ambition vs regulatory constraints
  - Appetite to innovate might push for looser tolerance
  - But regulators or standards may force stricter tolerance in certain domains, like data privacy
- Measurement maturity vs precision of tolerance
  - Immature measurement capabilities force broader tolerances that may allow more risk
- Culture and behavior vs tolerance enforcement
  - If the culture routinely grants exceptions or ignores breaches, tolerance has little real effect

UNCERTAINTY

- The amount of unavoidable variance in future predictions of external factors
  - Essentially, the risk of not being able to predict the future with certainty
    - For example: The impact of AI on the economy and banking
    - For example: Inconsistent or changing positions on major regulatory issues
- Uncertainty options
  - Commit to one possible outcome
    - High level of risk but potentially high level of returns
  - Spread the risk
    - Make investments in the different alternatives, hedging bets
  - Ignore the uncertainty
    - Assume the status quo will continue, often the worst possible choice

Q&A AND OPEN DISCUSSION