RISK AND RESILIENCY BOOTCAMP

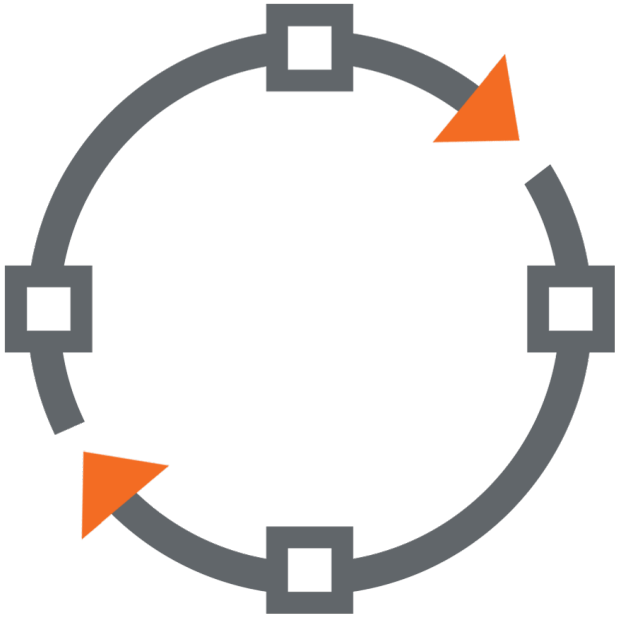
TEKsystems Global Services

WORKFORCE DEVELOPMENT

PROCESS MATURITY

In this module, we will

- Examine the concept of process maturity in IT
- How it helps or hinders risk and resiliency management
- How it applies to our own risk and resiliency processes



SOFTWARE ENGINEERING INSTITUTE

Commissioned by US Government (DoD) to find out how organizations built high quality software
Found it depended on three factors:

- The organization had a defined software production process
- The organization followed the process when they built software
- They were always improving the process in terms of efficiency and effectiveness

The measure of how well the organization follows these three factors is called *process maturity*

IMMATURE ORGANIZATIONS

- The process is often improvised by the developers and management during the course of the project
- Defined processes are often not followed or enforced
- Project activities are reactionary and often focus on solving immediate crises
- Schedules and budgets are based on unrealistic estimates and routinely exceeded
- Bringing a project in line with deadlines or costs causes functionally and product quality to suffer
- Product quality is difficult to predict and there are no objective standards to assess product quality

IMMATURE ORGANIZATIONS

- There are no standard ways for solving problems, everything is done on a “firefighting” basis where the same problems keep recurring with the same negative impacts
- The defined process is not realistic and the organization is characterized by the attitude “Following the rules won't get the job done”
- The defined process is often created in part by those who are not part of the development staff and tends to be more about reporting and management activities than work tasks

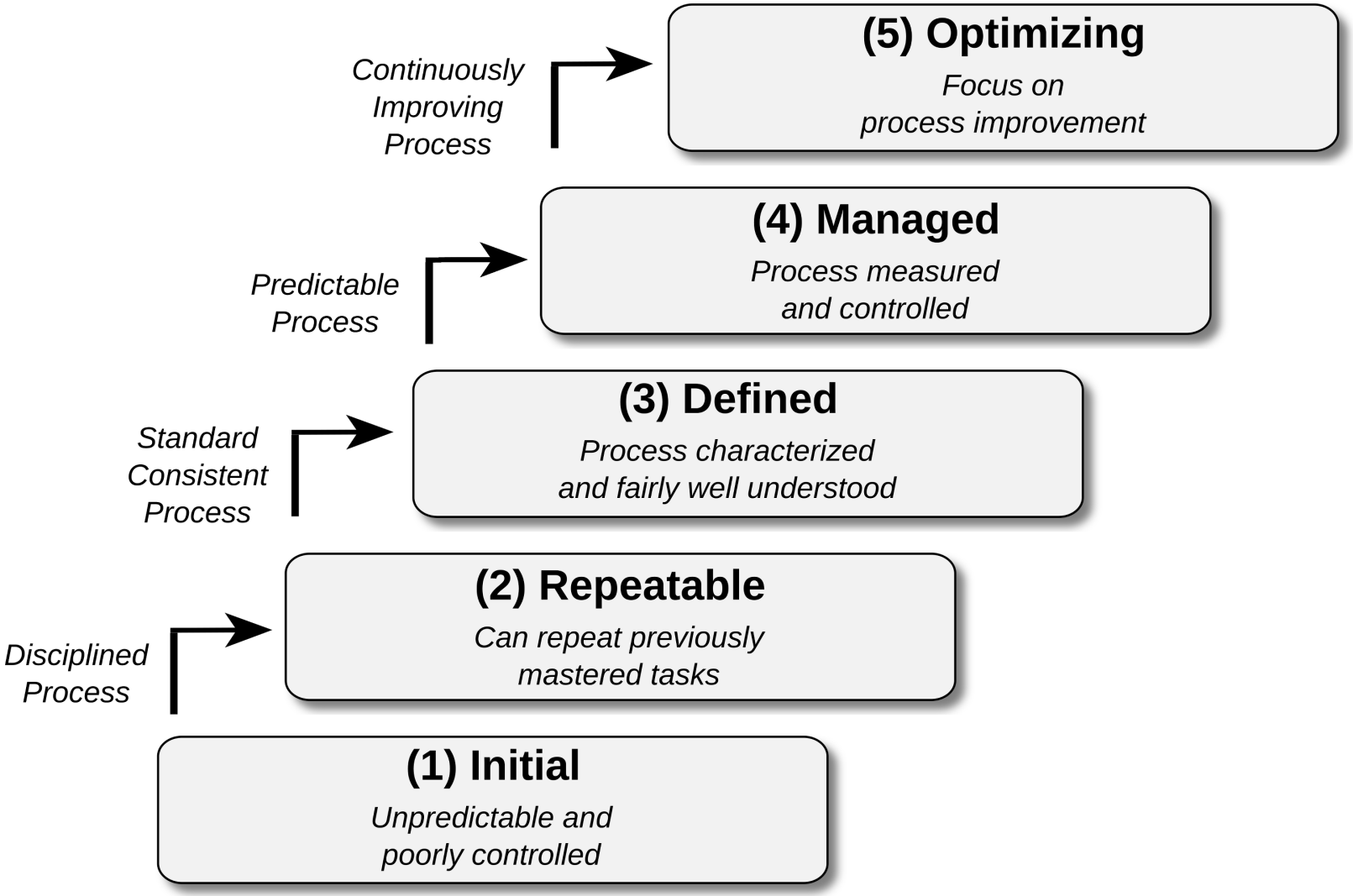
MATURE ORGANIZATIONS

- The software process is standardized across the organization and communicated to all existing staff and new employees
- All work activities are carried out according to the planned process
- The processes are usable and realistic because they describe how work actually gets done
- Defined processes are updated as necessary
- Improvements to the process are planned and evaluated through pilot tests or cost benefit analyses

MATURE ORGANIZATIONS

- Responsibilities are defined clearly in the organization and in each project
- Management continuously monitors the quality of the products and the processes using objective and quantifiable criteria
- There are defined processes for analyzing and solving problems with the product with diagnostic and remediation processes
- Budgets and schedules are realistic because they are based on historical performance data
- The infrastructure of the organization supports the process
- A disciplined process is consistently followed because all of the participants understand the value of doing so and enforce following the process at a peer level

THE LEVELS



THE LEVELS

- Initial
  - Describes a start-up company with no defined processes
  - Processes are counter productive and often inhibit innovation
  - Large process mature companies will often spin off incubator startups
  - These incubators provide a free-wheeling entrepreneurial environment
- Repeatable
  - Production process mastered: all projects are on spec, on time and to budget
  - Processes are well documented and standardized within specific projects or areas
    - For example, the QA department has a set of efficient and effective testing processes
    - The operations group has a set of standardized monitoring and deployment procedures

THE LEVELS

- Encultured
  - The organization has standardized processes that are used across the organization
  - They have customizable templates to tailor the process to specific requirements
  - For example:
    - Data migration project
    - Customer UI enhancement project
    - Regulatory compliance implementation project
  - However, it is more than just having a standardized set of processes
    - The processes have to actually be followed consistently and correctly
    - This happens when following the process is part of the organizational culture
    - It's *'the way we do it here'* and is enforced by everyone in the organization
    - People who don't follow the process are sanctioned by their peers, not management

THE LEVELS

- Proactive
  - Having a standard process from level 3 allows the collection of standard data
  - Measures the effectiveness and efficiency of the process across projects
  - Allows for the development of standards and best practices
    - These are empirical, based on historical data
  - This results in a review based culture
    - Everything is reviewed to ensure it is in alignment with best practices and quality metrics
    - Proactively identifying problems and issues before they can occur
    - Includes application code, deployment processes, operations procedures
  - Best practices are constantly updated to incorporate new data

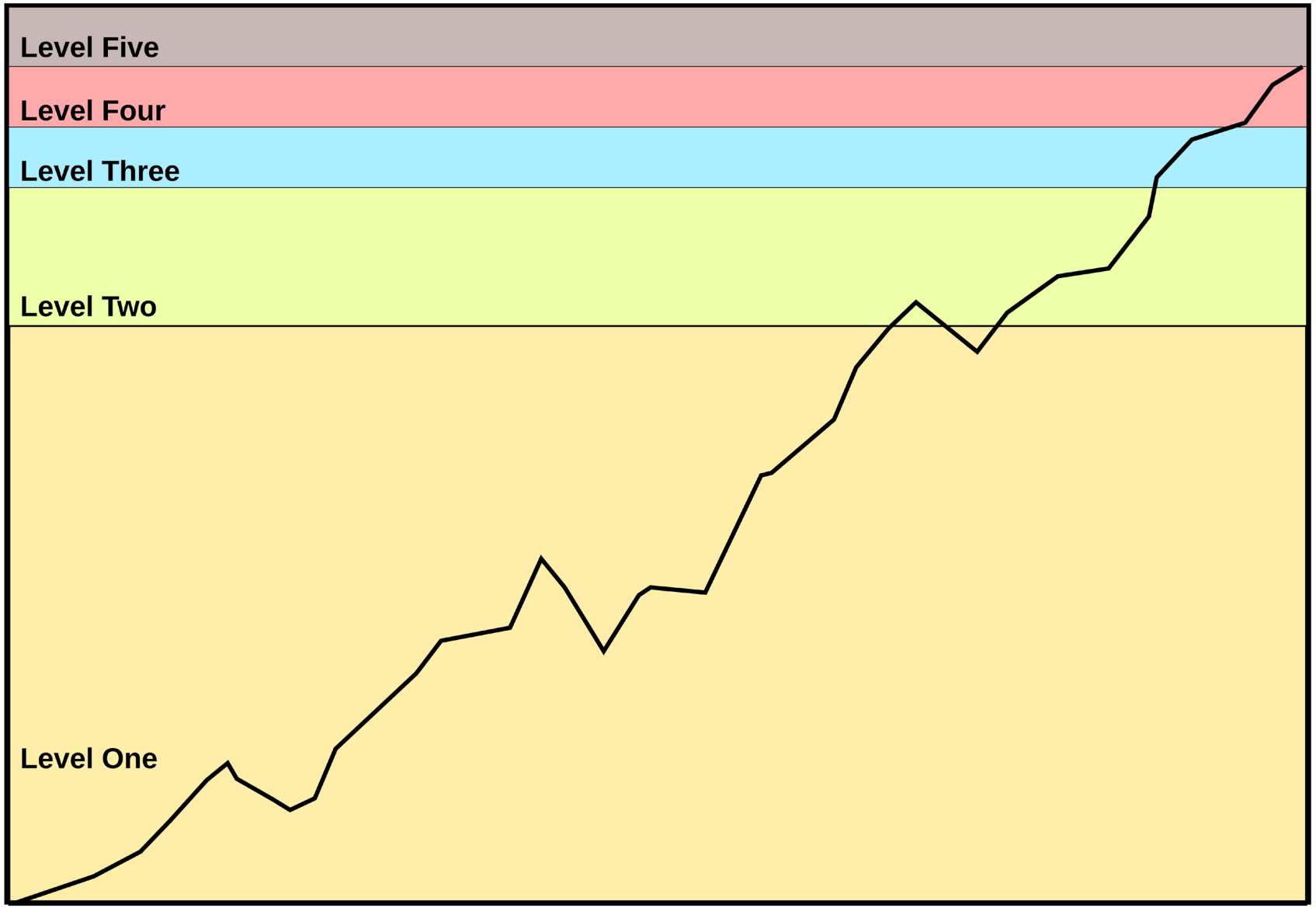
THE LEVELS

- Integrated
  - Processes are not only standardized and reviewed but are fully embedded into the organization's ecosystem
  - They are interconnected across functional areas and self-correcting
    - Deviations or inefficiencies are automatically detected and resolved without waiting for external intervention
  - Some characteristics of this level
    - *Continuous Feedback Loops:* Monitoring, analytics, and automation feed data back into processes in real-time, enabling proactive adjustments
    - *Predictive Risk Management:* Instead of reacting to issues, predictive analytics and trend analysis identify potential risks before they occur
    - *Cross-Functional Integration:* Risk, operations, governance, and development streams (like in ALM) are tightly linked so changes in one area immediately reflect in others
    - *Culture of Resilience:* Resilience isn't just a goal: it's baked into every decision. Staff at all levels act with risk-awareness as second nature

TIME TO MATURITY

- A long and difficult journey
  - Getting to level two represents a major accomplishment for many organizations
- Organizations don't just decide to be at a specific level
  - The levels are benchmarks of growth and progress
  - Not a set of rules that are followed or checklists
  - Based on measurable qualities of the organization's culture and working processes
  - Each level builds on mastering the preceding levels
- Getting to level two is often the hardest
  - Because of the number of foundational processes that need to be mastered
    - For example: data management, QA and testing, code development, etc.
  - It's not unusual for an organization to take ten years to get to level five, but seven years of the ten to get to level two

TIME TO MATURITY



IMMATURITY LEVELS

- In response to the maturity level model
  - Tom Schorsch proposed a set of immaturity levels
  - These levels were intended to satirize the fact that many organizations are not interested in becoming process mature or getting better at what they do
- The immaturity levels
  - Level 0: Negligent: Indifference
    - Failure to allow successful development process to succeed
    - All problems are perceived to be technical problems (“It’s because we use Linux”)
    - Managerial and quality assurance activities are deemed to be overhead and superfluous to the task of software development process
    - Reliance on silver bullets and miracle solutions (“Let’s just make everything a microservice”)

IMMATURITY LEVELS

- Level -1: Obstructive: Counter Productive
  - Counterproductive processes are imposed
  - Processes are rigidly defined and adherence to the format is stressed
  - Ritualistic ceremonies abound replacing productive work planning
  - Collective management precludes assigning responsibility
  - Status quo über alles
- Level -2: Contemptuous: Arrogance
  - Disregard for good software engineering institutionalized
  - Complete schism between software development activities and software process improvement activities
  - Complete lack of a training program
  - *"Industry-wide processes and standards won't work for us because we are unique and unlike anyone else"*

IMMATURITY LEVELS

- Level -3: Undermining: Sabotage
  - Total neglect of own charter
  - Conscious discrediting of peer organizations' software process improvement efforts
  - Rewarding failure and poor performance

RISK AND RESILIENCE ANALYSIS

- Level 1: Initial (Ad Hoc / Startup Mode)
  - Strengths:
    - High flexibility, rapid innovation, ability to pivot quickly
    - Low bureaucracy
  - Weaknesses:
    - No consistent processes: unpredictable outcomes
    - High dependency on individuals, not systems
    - No institutional resilience; survival depends on firefighting

RISK AND RESILIENCE ANALYSIS

- Level 1: Initial (Ad Hoc / Startup Mode)
  - Risk and resilience implications:
    - *Preventive controls*: Absent or inconsistent
    - *Detective controls:* Minimal, often manual
    - *Corrective controls:* Reactive only; recovery depends on heroic effort
    - Very fragile to disruptions; downtime or incidents can be catastrophic
  - Examples:
    - A startup releasing features without QA or security testing
    - Small businesses relying on one sysadmin to handle outages
    - Early dot-com companies where “move fast and break things” was the norm

RISK AND RESILIENCE ANALYSIS

- Level 2: Repeatable (Basic Project Discipline)
  - Strengths:
    - Processes exist and can be repeated with predictable outcomes
    - Projects delivered on time, within budget, meeting basic specs
    - Beginning of operational stability
  - Weaknesses:
    - Still project-centric, not an organization-wide culture discipline
    - Risk management is procedural, not proactive
    - Resilience depends on discipline of teams rather than systemic enforcement

RISK AND RESILIENCE ANALYSIS

- Level 2: Repeatable (Basic Project Discipline)
  - Risk and resilience implications:
    - Preventive controls: Introduced (checklists, basic SOPs)
    - Detective controls: Project reviews and monitoring start to appear
    - Corrective controls: Still heavily reliant on manual intervention
    - Moderate resilience: disruptions can be recovered from, but only with effort
  - Examples:
    - An IT team that has a standard patching process but no enterprise-wide monitoring
    - A bank's IT division delivering projects reliably, but each project operates in silos
    - Organizations following ITIL checklists mechanically but without cultural adoption

RISK AND RESILIENCE ANALYSIS

- Level 3: Encultured (Institutionalized Process)
  - Strengths:
    - Processes embedded into culture: "the way we do things here"
    - Broad organizational buy-in; staff enforce consistency
    - Risk awareness starts becoming cultural
  - Weaknesses:
    - Culture can become rigid; resistant to innovation
    - Risk handling still relies on compliance rather than continuous improvement
    - May create "checkbox resiliency" (following rules without adaptive thinking)

RISK AND RESILIENCE ANALYSIS

- Level 3: Encultured (Institutionalized Process)
  - Risk and resilience implications:
    - *Preventive controls:* Widely adopted; culture enforces SOPs
    - *Detective controls:* Routine monitoring and audits exist
    - *Corrective controls:* Documented recovery processes followed consistently
    - *Stronger resilience:* outages handled predictably, though recovery may still be slow
  - Examples:
    - Hospitals enforcing hygiene checklists at every stage of care
    - IT organizations where patching, access control, and backup processes are religiously followed

RISK AND RESILIENCE ANALYSIS

- Level 4: Proactive (Continuous Review & Alignment)
  - Strengths:
    - Processes are actively reviewed and aligned with best practices
    - Metrics and quality benchmarks drive improvement
    - Risk management shifts from compliance to anticipation
  - Weaknesses:
    - Heavy reliance on review cycles; still retrospective (fix after reviewing)
    - Can be slow if review processes are bureaucratic
    - If reviews lag, risks slip through

RISK AND RESILIENCE ANALYSIS

- Level 4: Proactive (Continuous Review & Alignment)
  - Risk and resilience implications:
    - Preventive controls: Regularly refined against industry standards
    - Detective controls: Formalized reviews, audits, benchmarking
    - Corrective controls: Feedback loops exist, but still human-driven
    - High resilience: the organization is unlikely to repeat mistakes, but not yet self-healing
  - Examples:
    - Tech companies adopting DevSecOps reviews and automated quality metrics
    - Financial institutions with constant regulatory alignment reviews
    - Aviation industry processes with rigorous after-action reviews

RISK AND RESILIENCE ANALYSIS

- Level 5: Integrated (Self-Correcting Enterprise)
  - Strengths:
    - Processes interconnected, adaptive, and self-correcting
    - Continuous monitoring and automation reduce human error
    - Risk awareness is systemic; resilience is built-in
  - Weaknesses:
    - High cost and complexity to implement
    - Requires strong governance and advanced analytics
    - Risk of over-reliance on automation without human oversight

RISK AND RESILIENCE ANALYSIS

- Level 5: Integrated (Self-Correcting Enterprise)
  - Risk and resilience implications:
    - *Preventive controls:* Automated, predictive (e.g., AI detecting risks early)
    - *Detective controls:* Advanced analytics, real-time anomaly detection
    - *Corrective controls:* Automated failover, rollback, and self-healing systems
    - *Resilience is dynamic:* systems adapt in real-time, minimizing impact of disruptions
  - Examples:
    - Cloud-native companies with automated self-healing infrastructure
    - High-frequency trading platforms with real-time risk engines
    - Large-scale e-commerce (Amazon, Netflix) using chaos engineering to continuously test resilience

RISK & RESILIENCE CAPABILITIES

- Level 1: Initial (Ad Hoc / Startup)
  - What you can do:
    - React to incidents as they occur
    - Rely on individual heroics to restore systems
    - Learn from major failures (if knowledge is captured)
  - Limits:
    - Cannot systematically prevent risks
    - Cannot guarantee recovery or resilience (no processes in place)
    - Limited visibility into risks: only the obvious ones are seen
    - Highly fragile; any disruption can derail operations

RISK & RESILIENCE CAPABILITIES

- Level 2: Repeatable (Project Discipline)
  - What you can do:
    - Deliver projects consistently on time and within budget
    - Apply basic preventive measures (e.g., patching SOPs, change control)
    - Recover from common incidents with repeatable playbooks
  - Limits:
    - Cannot ensure organization-wide risk management (processes are siloed)
    - Cannot adapt rapidly to new risks: improvements lag
    - Resilience depends on discipline of teams, not systemic enforcement
    - Still reactive when facing novel or complex risks

RISK & RESILIENCE CAPABILITIES

- Level 3: Encultured (Institutionalized Process)
  - What you can do:
    - Enforce processes through culture: everyone follows the process
    - Achieve consistent resiliency in routine operations (e.g., backups, patching)
    - Create organizational memory of risk responses
  - Limits:
    - Cannot easily innovate: culture resists change
    - Cannot adapt processes quickly to new risk scenarios
    - Risks outside the “cultural model” may go unseen (blind spots)
    - Resilience is strong but not agile; recovery can be slow

RISK & RESILIENCE CAPABILITIES

- Level 4: Proactive (Review & Continuous Improvement)
  - What you can do:
    - Continuously refine controls based on reviews, audits, and metrics
    - Anticipate risks using trends and lessons learned
    - Prevent recurrence of known failures
    - Maintain high compliance and alignment with best practices
  - Limits:
    - Cannot yet self-correct in real time; responses still depend on human review
    - Cannot fully predict or prevent novel/black swan risks
    - Resilience is high but still retrospective: based on after-the-fact improvement
    - Review cycles may delay action if governance is slow

RISK & RESILIENCE CAPABILITIES

- Level 5: Integrated (Self-Correcting Enterprise)
  - What you can do:
    - Automate preventive, detective, and corrective controls
    - Predict and mitigate risks before they occur
    - Self-heal during disruptions (e.g., auto-failover, rollback)
    - Achieve dynamic resilience across the enterprise
  - Limits:
    - Cannot eliminate all risks: black swan events still possible
    - Automation may miss context or create false confidence
    - High implementation costs and complexity limit feasibility for smaller organizations
    - Over-reliance on AI/automation can create hidden risks if not overseen

CAPABILITY MODELS

- Maturity modeling is a universal approach
  - Applied to testing, data, continuity, cybersecurity, governance, people, operations and development
  - The core pattern is always
    - From ad hoc → repeatable → institutionalized → optimized → adaptive/self-correcting
  - These flesh out the maturity framework with specific milestones and practices that are relevant for that domain
    - Some of these, like the testing and data maturity models depend on the overall process maturity level of the organization
    - As a rule of thumb, a specialized maturity model is often (but not always) limited to the overall maturity level of the organization

CERT RESILIENCE MANAGEMENT MODEL

- CERT Resilience Management Model (CERT-RMM)
  - Developed by Carnegie Mellon's CERT (Computer Emergency Response Team)
  - Focused on operational resilience, security risk management, and continuity of critical services
  - Integrates principles of security, business continuity, and IT operations into a single maturity model
  - Widely used in critical infrastructure sectors (finance, energy, government)
  - Unlike generic models, CERT-RMM is explicitly designed for operational resilience
  - Directly ties risk management, security, and continuity together
    - Level 1–2 = survival by firefighting (fragile resilience)
    - Level 3 = consistency (resilience by design)
    - Level 4 = predictability (resilience by measurement)
    - Level 5 = adaptability (resilience as a living capability)

CERT RESILIENCE MANAGEMENT MODEL

- Level 0: Incomplete
  - No formal resilience processes in place, just ad hoc responses to incidents
  - Strengths:
    - Flexibility, quick improvisation
  - Weaknesses:
    - No predictability, high dependence on individuals, reactive only
  - Risk and resilience implications:
    - *Preventive*: None
    - *Detective*: Incidents discovered accidentally or by external parties
    - *Corrective*: Recovery is improvised, often incomplete
    - Organizational resilience is fragile: disruptions often catastrophic
  - Example:
    - A small startup with no backups, no disaster recovery plan, and ad hoc security

CERT RESILIENCE MANAGEMENT MODEL

- Level 1: Performed
  - Some resilience-related practices exist but are inconsistent and undocumented
  - Strengths:
    - At least basic awareness of the need for resilience
  - Weaknesses:
    - Reliance on individuals; outcomes unpredictable
  - Risk and resilience implications:
    - *Preventive:* Basic measures (passwords, occasional backups)
    - *Detective*: Manual monitoring, informal reporting
    - *Corrective*: Incident response handled ad hoc
    - *Resilience* still low and unpredictable
  - Example:
    - IT team that occasionally patches systems and keeps informal backup copies

CERT RESILIENCE MANAGEMENT MODEL

- Level 2: Managed
  - Resilience practices are planned and tracked at the project or team level
    - Processes repeatable, but not standardized enterprise-wide
  - Strengths:
    - Teams can deliver resilience outcomes consistently
  - Weaknesses:
    - Silos; resilience varies across the organization
  - Risk and resilience implications
    - *Preventive*: Basic SOPs for security, backup, patching
    - *Detective*: Logs reviewed manually or semi-regularly
    - *Corrective*: Recovery documented but not standardized across units
    - Resilience moderate but fragmented: depends on team maturity
  - Example:
    - One business unit has a tested recovery plan; others rely on ad hoc fixes

CERT RESILIENCE MANAGEMENT MODEL

- Level 3: Defined
  - Organization-wide resilience processes are defined, documented, and standardized. Clear policies exist for continuity, risk, and security
  - Strengths:
    - Consistency across the enterprise; resilience part of culture
  - Weaknesses:
    - May become compliance-focused; adaptation to new risks still slow
  - Risk and resilience implications:
    - *Preventive*: Enterprise-wide policies (security standards, resilience training)
    - *Detective*: Consistent monitoring and incident tracking
    - *Corrective*: Recovery procedures formally documented and tested
    - Strong resilience, but not yet adaptive
  - Example:
    - A bank adopting standardized incident response and continuity planning across all departments

CERT RESILIENCE MANAGEMENT MODEL

- Level 4: Managed and Measured
  - Resilience processes are quantitatively managed and measured with performance metrics (MTTR, incident trends, compliance KPIs)
  - Strengths:
    - Decisions driven by data and continuous measurement; risk appetite and tolerance explicitly managed
  - Weaknesses:
    - Measurement frameworks can be rigid or overly complex
  - Risk and resilience implications:
    - *Preventive*: Continuous improvement of controls based on risk metrics
    - *Detective*: Advanced monitoring, dashboards, regular testing of resilience
    - *Corrective*: Lessons learned fed back into resilience planning
    - Resilience is strong, predictable, and improving over time
  - Example:
    - A power grid operator measuring resilience metrics like recovery time and incident containment rate, adjusting controls proactively

CERT RESILIENCE MANAGEMENT MODEL

- Level 5: Optimizing
  - Resilience is institutionalized, adaptive, and continuously optimized
    - Organization learns and evolves in real time
  - Strengths
    - Predictive resilience through analytics and automation; resilience is self-correcting
  - Weaknesses:
    - High cost and complexity; potential over-reliance on automation
  - Risk and resilience implications:
    - *Preventive*: Automated threat intelligence integration, predictive risk models
    - *Detective*: AI-driven anomaly detection, continuous monitoring
    - *Corrective*: Self-healing systems, automated failover, continuous learning
    - Dynamic resilience: Organization adapts to risks as they emerge
  - Example:
    - Large e-commerce platform (e.g., Amazon) continuously running chaos engineering to validate resilience; financial markets with predictive risk engines

BUSINESS CONTINUITY MATURITY MODEL

- Developed by the Business Continuity Institute (BCI) and industry practitioners
  - Provides a structured way to assess an organization's business continuity (BC) and recovery planning maturity
  - Levels run from ad hoc self-governed efforts to fully optimized, enterprise-wide resilience capability
    - Level 1–2 = survival through local heroes
    - Level 3 = consistency across the enterprise
    - Level 4 = data-driven improvement
    - Level 5 = resilience as a competitive advantage

BUSINESS CONTINUITY MATURITY MODEL

BUSINESS CONTINUITY MATURITY MODEL

- Level 1: Self-Governing
  - Continuity efforts are isolated, often initiated by individuals or specific teams
    - No enterprise recognition
  - Strengths:
    - Some awareness exists; motivated individuals may keep local processes alive
  - Weaknesses:
    - No formal governance; fragmented, inconsistent, and unreliable
  - Risk and resilience implications:
    - *Preventive*: Minimal; depends on local champions
    - *Detective*: No systematic monitoring of continuity risks
    - *Corrective*: Recovery is improvised, often incomplete
    - Resilience: Fragile: survival depends on local initiative
  - Example:
    - An IT admin who personally runs backups without management support or policy

BUSINESS CONTINUITY MATURITY MODEL

- Level 2: Repeatable
  - Continuity processes are repeatable within certain areas but not standardized
    - BC plans exist for critical functions
  - Strengths:
    - Predictability within pockets of the organization
  - Weaknesses:
    - Plans vary in quality; no organizational oversight
    - Risks outside critical areas remain unmanaged
  - Risk & Resilience Implications:
    - *Preventive*: SOPs exist in certain departments
    - *Detective*: Limited monitoring, manual checks
    - *Corrective*: Local recovery possible, but gaps in coverage
    - Resilience: Better than ad hoc, but fragmented: a disruption may expose unprotected areas
  - Example:
    - A business unit maintains a tested continuity plan, but other units have none

BUSINESS CONTINUITY MATURITY MODEL

- Level 3: Defined
  - Enterprise-wide BC policies and processes defined
    - Roles and responsibilities assigned; continuity embedded into organizational culture
  - Strengths:
    - Standardization across the organization; consistent coverage
  - Weaknesses:
    - Focus may be compliance-driven; adaptation to new risks still limited
  - Risk and resilience implications:
    - *Preventive*: Enterprise-level BC policies enforce preventive controls
    - *Detective*: Regular monitoring and reviews of continuity plans
    - *Corrective*: Documented and tested recovery procedures
    - *Resilience*: Consistent and reliable, but may lag in agility
  - Example:
    - A global bank standardizes its continuity framework across all regions and tests critical recovery processes annually

BUSINESS CONTINUITY MATURITY MODEL

- Level 4: Managed
  - Continuity processes are monitored, measured, and proactively managed with performance metrics (RTO, RPO, recovery success rates)
  - Strengths:
    - Continuous improvement based on data; proactive adjustments
  - Weaknesses:
    - Risk of excessive focus on metrics; bureaucratic slowdowns
  - Risk and resilience implications:
    - *Preventive*: Controls regularly updated based on risk metrics
    - *Detective*: Advanced monitoring systems track compliance and risks
    - *Corrective*: Lessons learned systematically integrated
    - *Resilience*: High resilience — tested, measured, and predictable
  - Example:
    - A telecom provider measures time-to-recovery after outages and improves continuity planning based on trend analysis

BUSINESS CONTINUITY MATURITY MODEL

- Level 5: Optimized
  - Continuity is institutionalized as a dynamic, adaptive capability
    - Resilience processes are integrated across business, IT, supply chain, and partners
  - Strengths:
    - Self-optimizing and adaptive; BC is a strategic capability that drives competitive advantage
  - Weaknesses:
    - High complexity, costly to maintain, requires executive commitment
  - Risk and resilience implications:
    - *Preventive*: Predictive continuity planning; proactive risk scenario modeling
    - *Detective*: Real-time monitoring, automated continuity drills (e.g., chaos engineering in IT)
    - *Corrective*: Automated recovery and adaptive response mechanisms
    - *Resilience*: Enterprise-wide, adaptive resilience: disruptions absorbed with minimal impact
  - Example:
    - Amazon or Netflix continuously stress-test their operations (via chaos engineering) to validate continuity and resilience at scale

RISK AND RESILIENCE MATURITY

- Risk and resilience work is a process
  - Identifying risks, writing SOPs, testing recovery plans, or proposing controls, are not one-off tasks
  - These are repeatable activities that can be structured, measured, and improved over time
  - Like software testing or continuity planning, risk management itself has a maturity curve

Q&A AND OPEN DISCUSSION