Deloitte.

IT Resilience & & Modernizing the Three Lines Model

Knowledge Sharing

19 November 2021

MAKING AN IMPACT THAT MATTERS since 1845

Introduction - Speakers

Piroon Kittidatprecha
Director

Piroon Kittidatprecha
Risk Advisory
Bangkok, Thailand

pkittidatprecha@deloitte.com
P: +66(2) 676 5700

Languages:
English and Thai

Education:
Master of Science (Computer Information System), Assumption University, Thailand

Specific skills and experience:

- Internal Control Framework
- IT General Controls
- Application Controls
- SOX Controls
- Compliance and Governance
- Data Analytics

Relevant professional certifications:

- Certified Information System Auditor (CISA) – ISACA
- COBIT 5 Foundation
- ITIL V3 Foundation

Background

Piroon is a Director in IT Control Assurance practice within the Enterprise Risk Services at Deloitte Touche Tohmatsu Advisory. He has over 10 years of experience in various industries, such as banking, telecommunication, and manufacturing industries. For the information technology auditing area, he is responsible for reviewing information system controls on both application controls and general computer controls. His significant knowledge skills include evaluation and implementation of information system control and security using risk-based approach.

Selection of relevant project experience

- Managed IT risk assessment and IT audit for companies in Banking, Securities, Leasing, Entertainment, Hospital, Telecommunication, Retail, IT Service Center and Manufacturing industries.
- Managed SOX compliant IT control review for various industries .
- Managed IT Audit Co-sourcing e.g., provide technical training, perform IT risk assessment, assist/lead client to execute IT audit work, develop IT audit program and develop IT audit manual; for a large telecom company in Thailand.
- Managed IT Compliance Review to comply with BOT for large financial institutes.
- Managed IT Compliance Review to comply with SEC for Securities.
- Managed SOX 404 risk and control documentation development.

Roujkun Townamchai

Senior Manager

Roujkun Townamchai
Risk Advisory
Bangkok, Thailand

rtownamchai@ deloitte.com
P: +66(2) 034 0000 ext. 14971

Languages:
English and Thai

Education:
Master of Science, Computer Science, California State University Fullerton, USA
Bachelor of Engineer, Computer Engineer, Assumption University (ABAC), Thailand

Specific skills and experience:

- Project Management
- IT General Control Review
- Application Control Review
- Quality Assurance
- Agile Development
- IT Service Management Framework
- Internal Control Framework
- Compliance and Governance
- Data Analytics
- Expert in VBA Macro Programming

Relevant professional certifications:
Certified Information System Auditor (CISA), certification number 17138997
ISO/IEC 27001:2013 ISMS Auditor/Lead Auditor CQI/IRCA 47315

Background

Experiences in IT Audit, IT Consultant, and Software Testing as were Technology Audit Section Head in an international Bank, IT Audit Manager in an audit firm, Quality Assurance, Software Process Specialist and University Instructor for over 15 years.

Roujkun is highly experienced in IT Audit in financial service industry. His key client including listed, regulated, and multi-nation bank, insurance, and securities companies. He also used to be company instructor in an audit firm.

Selection of relevant project experience

- Managed and planed with audit team and client for IT general controls, application controls and IPE validation.
- Experienced in reviewing Service organization control report (ISAE3402) for international companies.
- Conducted risk assessments to identify IT dependencies and internal control deficiencies within business processes of banking, insurance, securities, retail sector.
- Conducted IT audits to ascertaining reliability of IT applications in accordance with best practices for banking, insurance, securities, retail sector.
- Led teams in maintaining and improving of IT Service Management processes such as Change Management, and Configuration Management banking, insurance, securities, retail sector.
- Conducted IT Service Management review for Change and Configuration Management modules banking, insurance, securities, retail sector.

IT Resilience

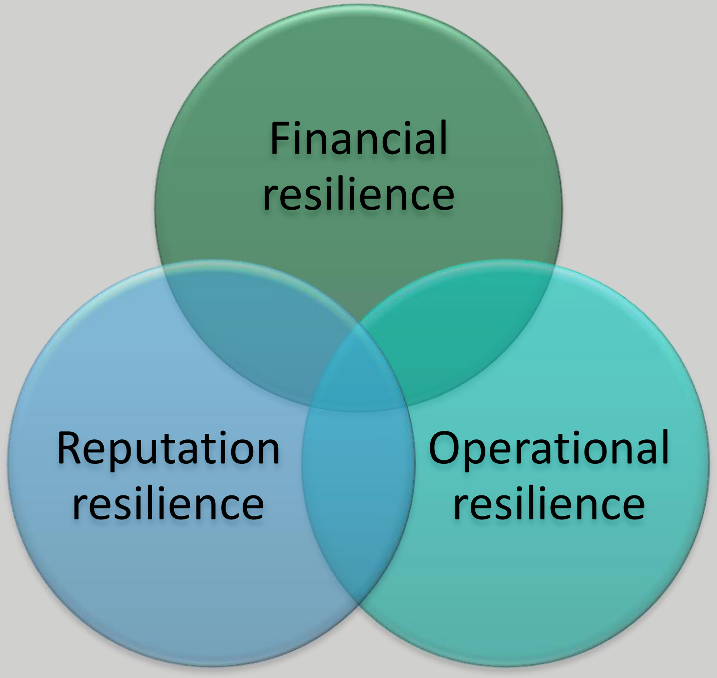
Resilience vs. Recovery

any different?

What is a resilient organization?

Resilient organizations plan and invest for disruption, and can adapt, endure, and rebound quickly in a way that enables them to not only to succeed in its aftermath, but also to lead the way to a “better normal”.

- Enables the organization to be better prepare to withstand events that impact liquidity income and assets



- Makes the organization more responsive to external perception and building a foundation of trust and dependability

- Ensure the organization can absorb impacts on people, data, technology, facilities, supply and demand.

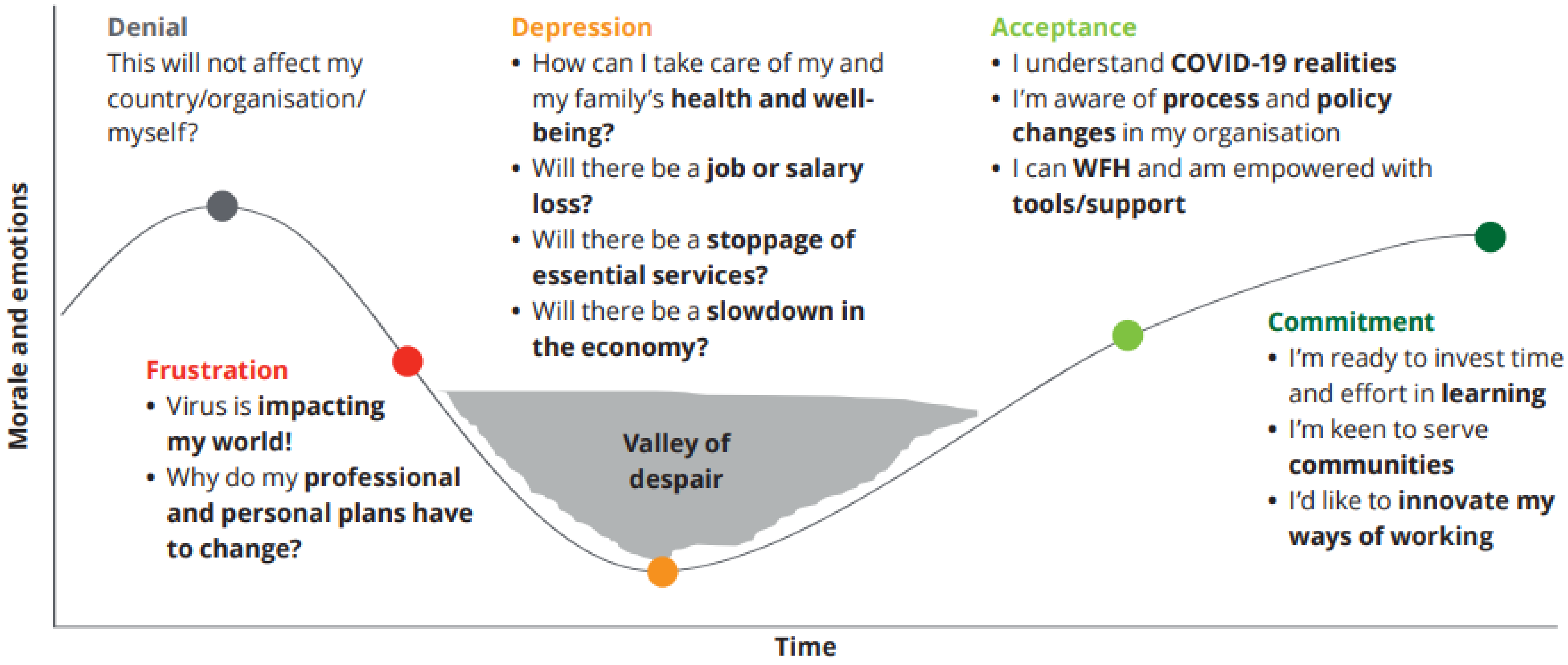
Is your organization resilient?

Ask yourself these questions:

1. Do I have a clear view of what financial, operational, and reputational resilience means for my organization?
2. Is my organization prepared, both operationally and financially, for another public emergency or crisis?
3. Is my infrastructure and service-provider ecosystem agile and ready for a variety of different events?
4. Am I aware of how changing market dynamics and evolving public views may affect my organization and its reputation?
5. Does the culture of my organization support resilience, in terms of both dealing with disruptive shocks *(continuity)* and adapting to economic, political, or cultural changes *(adaptive capacity)?*
6. Does my company stand for a purpose that stakeholders can believe in and support?
7. Am I currently taking a proactive and holistic approach to building organizational resilience and managing risk?

QUARANTINE
AUTHORIZED PERSONAL ONLY
CAUTION
OUTBREAK ALERT

COVID-19 Change Curve



Denial

This will not affect my country/organisation/ myself?

Frustration

- Virus is **impacting my world!**
- Why do my **professional and personal plans have to change?**

Depression

- How can I take care of my and my family's **health and well-being?**
- Will there be a **job or salary loss?**
- Will there be a **stoppage of essential services?**
- Will there be a **slowdown in the economy?**

Acceptance

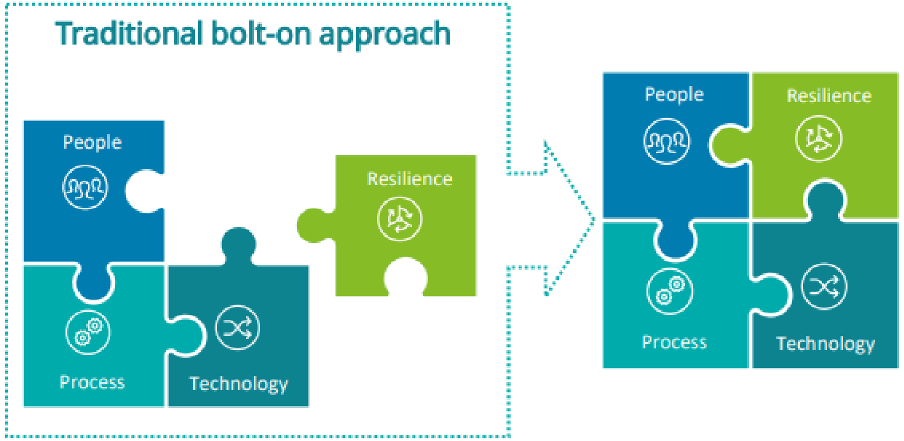
- I understand **COVID-19 realities**
- I'm aware of **process** and **policy changes** in my organisation
- I can **WFH** and am empowered with **tools/support**

Commitment

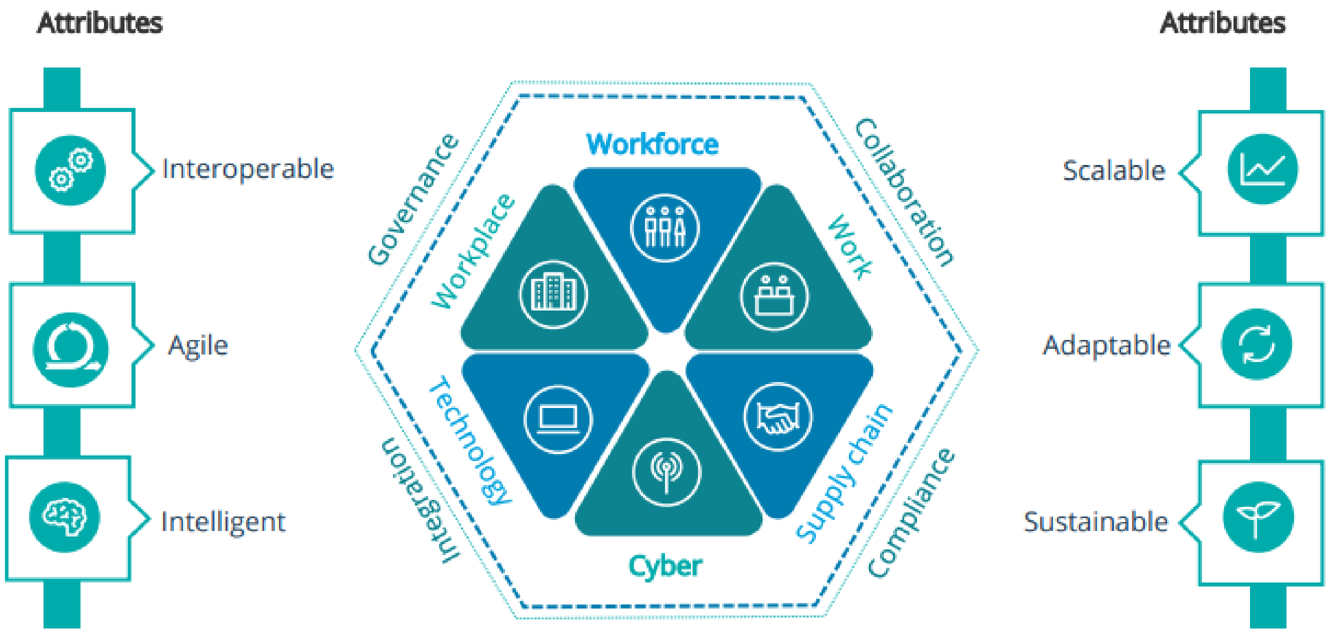
- I'm ready to invest time and effort in **learning**
- I'm keen to serve **communities**
- I'd like to **innovate my ways of working**

"Where are we?"

Resilience by Design Philosophy



Resilience Can no longer be looked at as a ‘Plan B’. Resilience must be an integral part of the organization DNA.

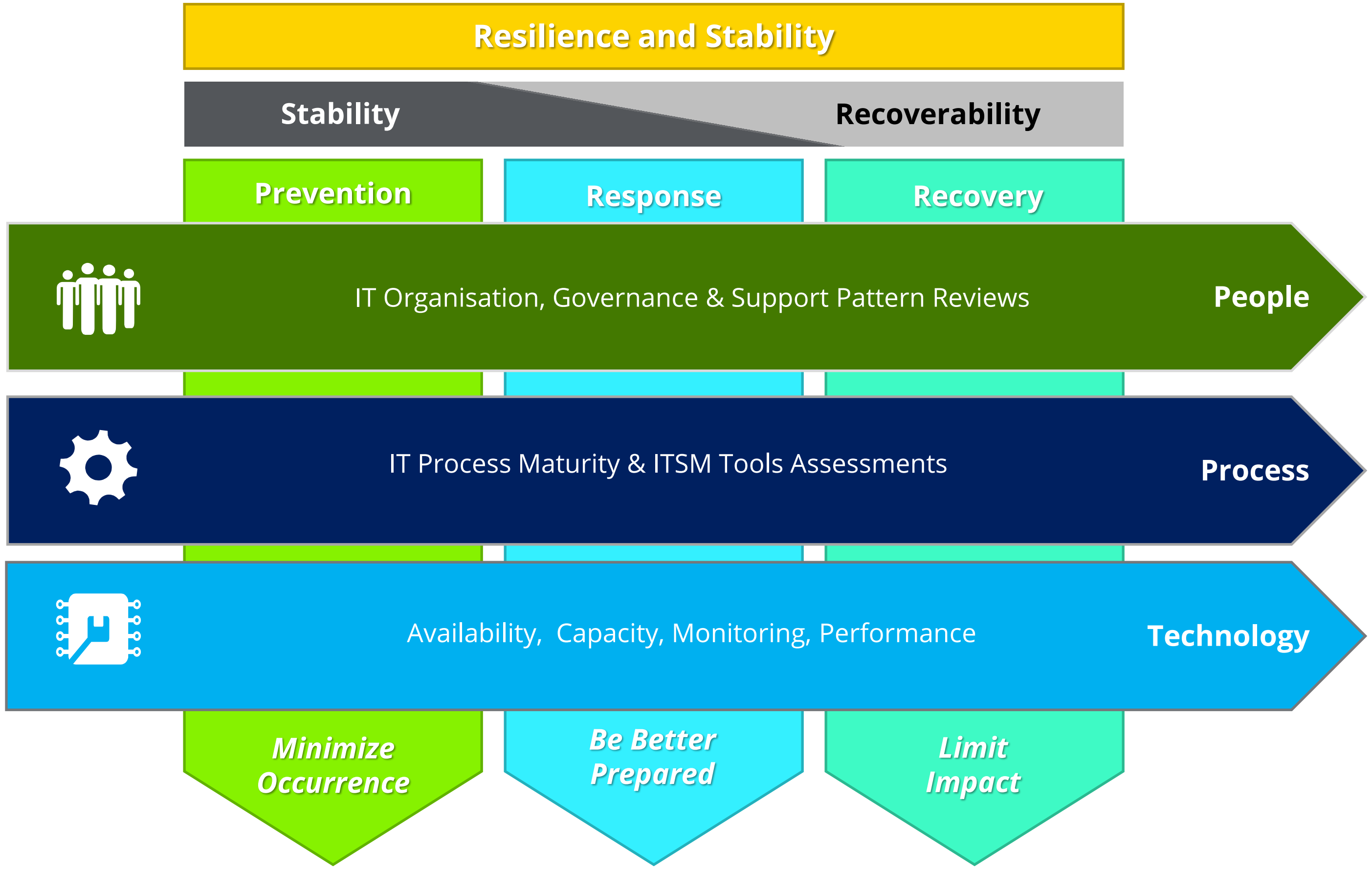


Focus areas

- Failure Scenario Analysis built into the process definition and design
- Elimination of Single-Point-of Failure across the process cycle through redundancy
- Recovery strategies intrinsically built as part of the process workflow
- Stress testing at every stage of the process cycle to provide ongoing confidence
- Building resilient organisational culture through ongoing awareness

Improving resilience is multifaceted…

Enterprise resiliency is the interplay between People, Process and Technology domains along 3 dimensions of Prevention, Response and Recovery


Resilience and Stability
Stability
Recoverability
Prevention
Response
Recovery
IT Organisation, Governance & Support Pattern Reviews
People
IT Process Maturity & ITSM Tools Assessments
Process
Availability, Capacity, Monitoring, Performance
Technology
Minimize Occurrence
Be Better Prepared
Limit Impact

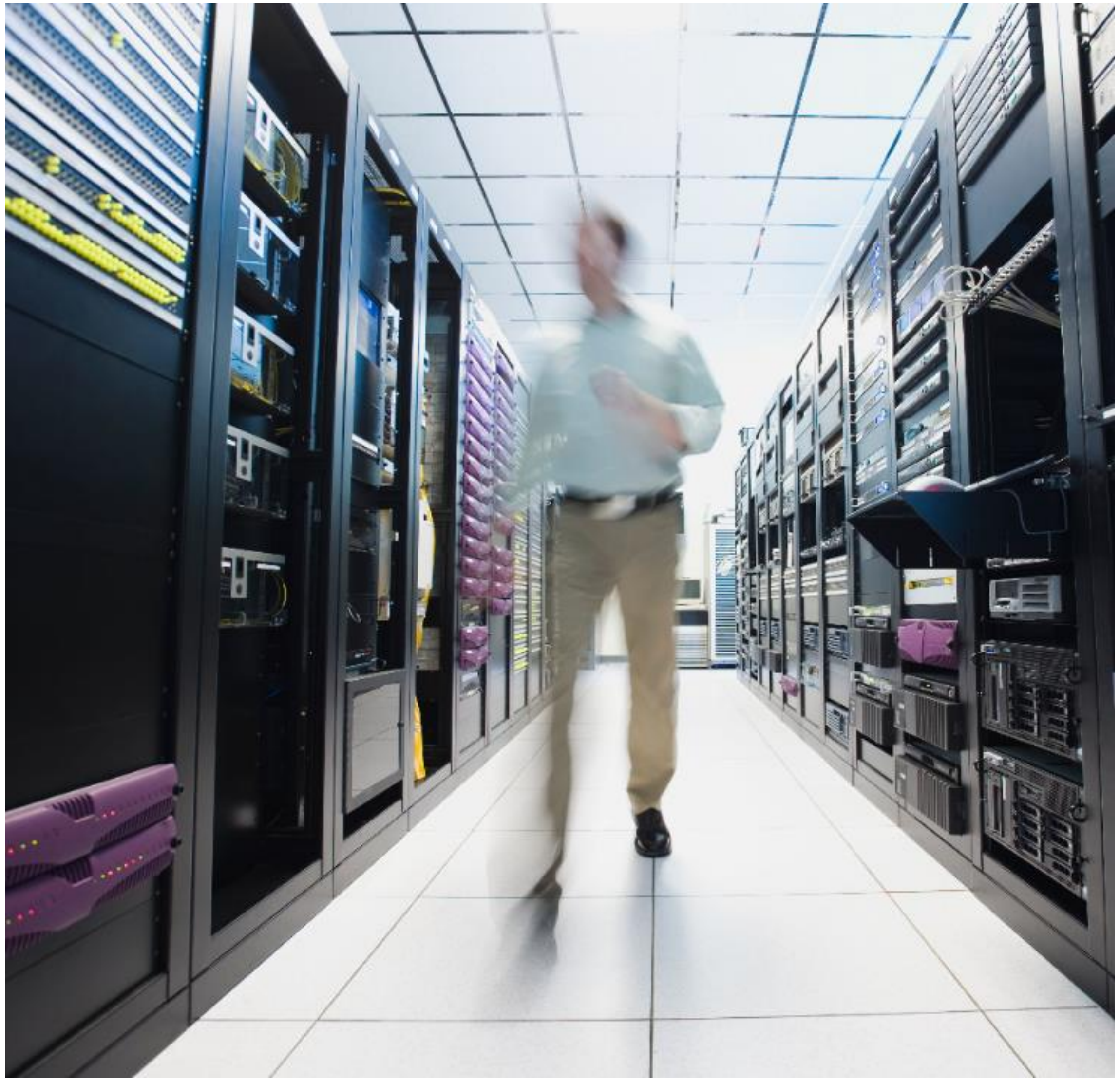
SOLUTIONS

1. **Service Delivery (ITSM), Operational Processes and Governance**
2. **Automation and Tooling**
3. **Application Resilience**
4. **Infrastructure Provisioning and Management**
5. **Data Center / Cloud Platform Resilience**

1. Service Delivery, Operational Processes and Governance

Key Issues	Causes
• Multi-vendor support model with no single ownership • Delays in identifying incidents and the magnitude of this issue • Informal hand-offs from engineering to Ops • Multiple Ticket hops leading to high MTTR (Mean time to recovery) • Unable to replicate production issues in Non-Prod environments • Poorly tested apps deployed to production cause impacts to other apps and infra	• Lack of Service Integration & Management (SIAM) • Siloed teams with no Single Point-of-contact • Incorrect skill-set mapping and under-skilled resources • Lack of change management processes and version control • Inadequate or outdated app to inframapping • Inadequate testing and production readiness checklists

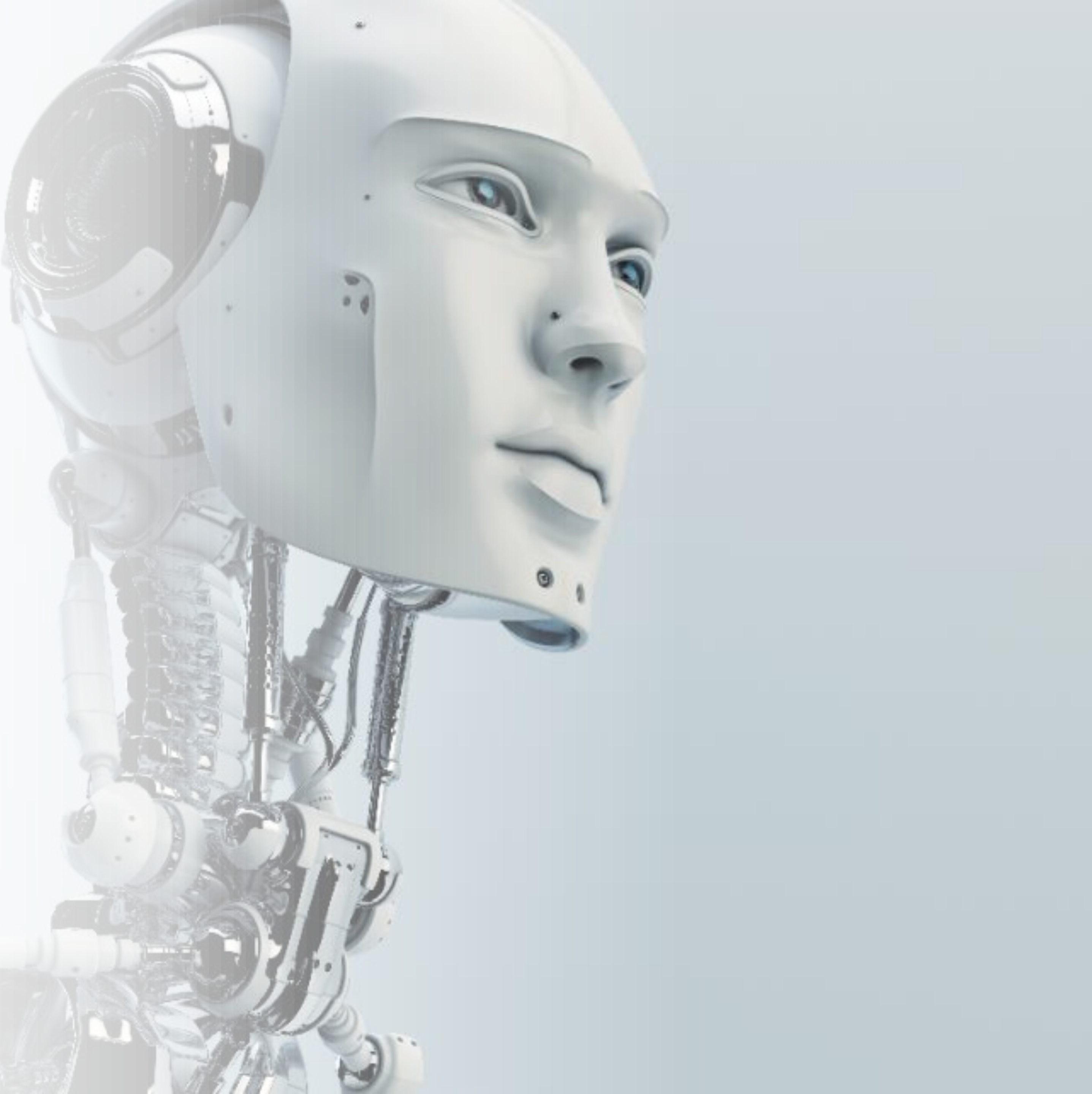
Resolution
• Implement SIAM with ownership resting with the Client or a single vendor • Implement and continuously update CMDB (configuration Management Database) with Application to Infrastructure dependency mapping • Identify Critical Business Flows and map it to Application & Infrastructure Components • Create an integrated App + Infra support team • Establish DevOps and / or formal operational handoff from Engineering to Operations • Correct skillset and level mapping • Enforce version control for the Apps & Platform



2. Automation and Tooling

Key Issues	Causes
• Inadequate / incomplete logs for high priority apps delay resolution of high priority incidents • Overlooking actionable alerts • Undocumented knowledge assets • Outdated Knowledge Management Repository • Inadequate change management processes	• Capability gaps in logging and monitoring, transaction traceability and app/infra inter-dependency mapping • High volume of false alerts • Delay in updating knowledge base

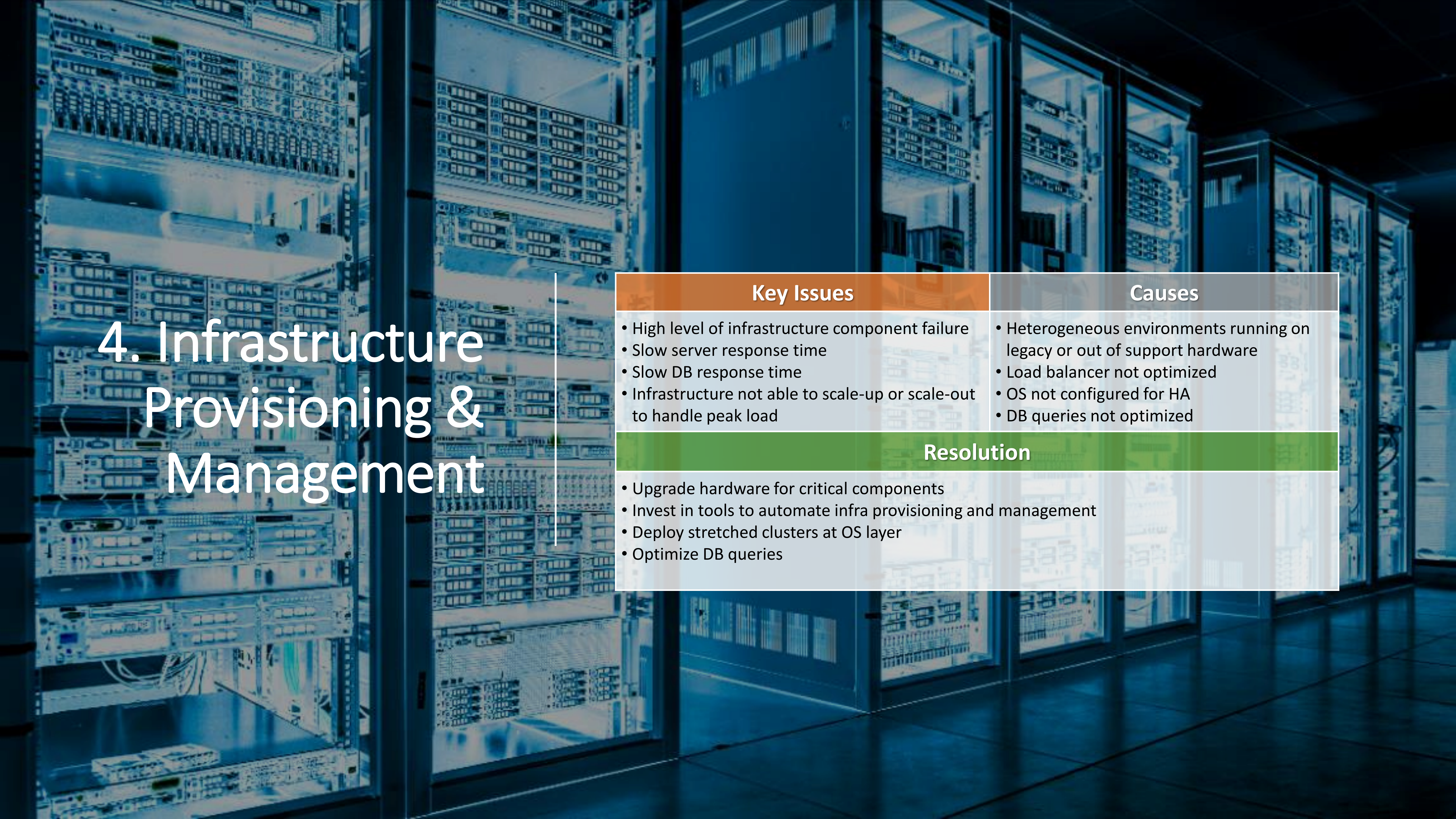
Resolution
• Deploy Performance monitoring and logging tools • Deploy Event Correlation and suppression engine • Implement DevOps and Process Automation Tools • Robust Knowledge Management documentation • Enforce regular update of knowledgebase



3. Application Resilience

Key Issues	Causes
• Single Application instance failure leading to business downtime • Application unable to scale-up to handle peak load • Messages stuck in transmission queue • High batch job failure rate	• Legacy Applications not architected for High Availability • Point-to-point interfaces • Messaging middleware systems not optimized • Idle batch jobs not decommissioned

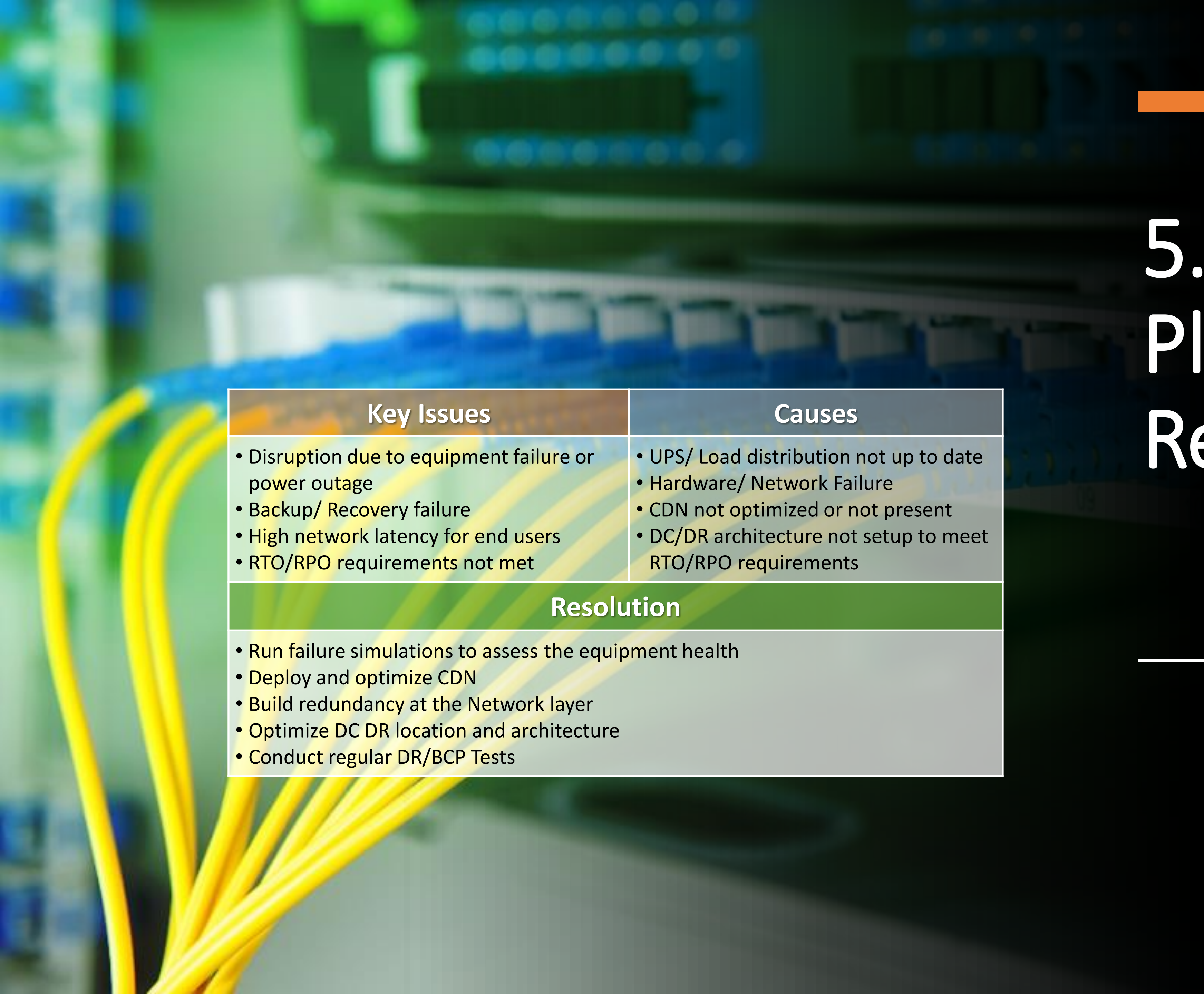
Resolution
• Identify critical application candidates for refactoring to enable HA • Enforce Cloud Native & Micro services architecture for new developments • Enable application synthetic monitoring, infrastructure monitoring and notification processing • Develop a resiliency index to measure app resilience



4. Infrastructure Provisioning & Management

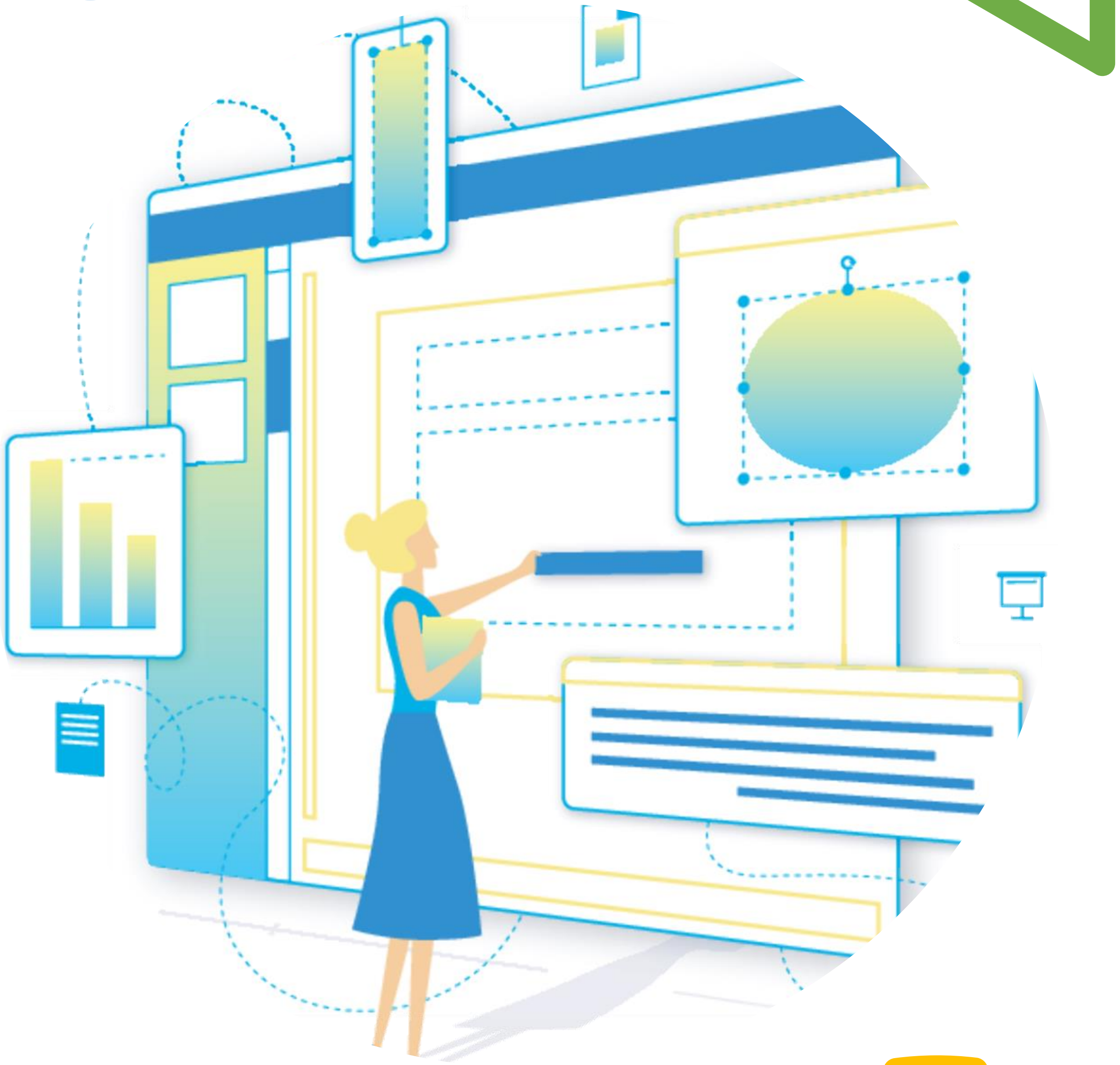
<table>
<tr><th>Key Issues</th><th>Causes</th></tr>
<tr><td>• High level of infrastructure component failure
• Slow server response time
• Slow DB response time
• Infrastructure not able to scale-up or scale-out to handle peak load</td><td>• Heterogeneous environments running on legacy or out of support hardware
• Load balancer not optimized
• OS not configured for HA
• DB queries not optimized</td></tr>
<tr><th colspan="2">Resolution</th></tr>
<tr><td colspan="2">• Upgrade hardware for critical components
• Invest in tools to automate infra provisioning and management
• Deploy stretched clusters at OS layer
• Optimize DB queries</td></tr>
</table>

5. Infrastructure Platform Resilience



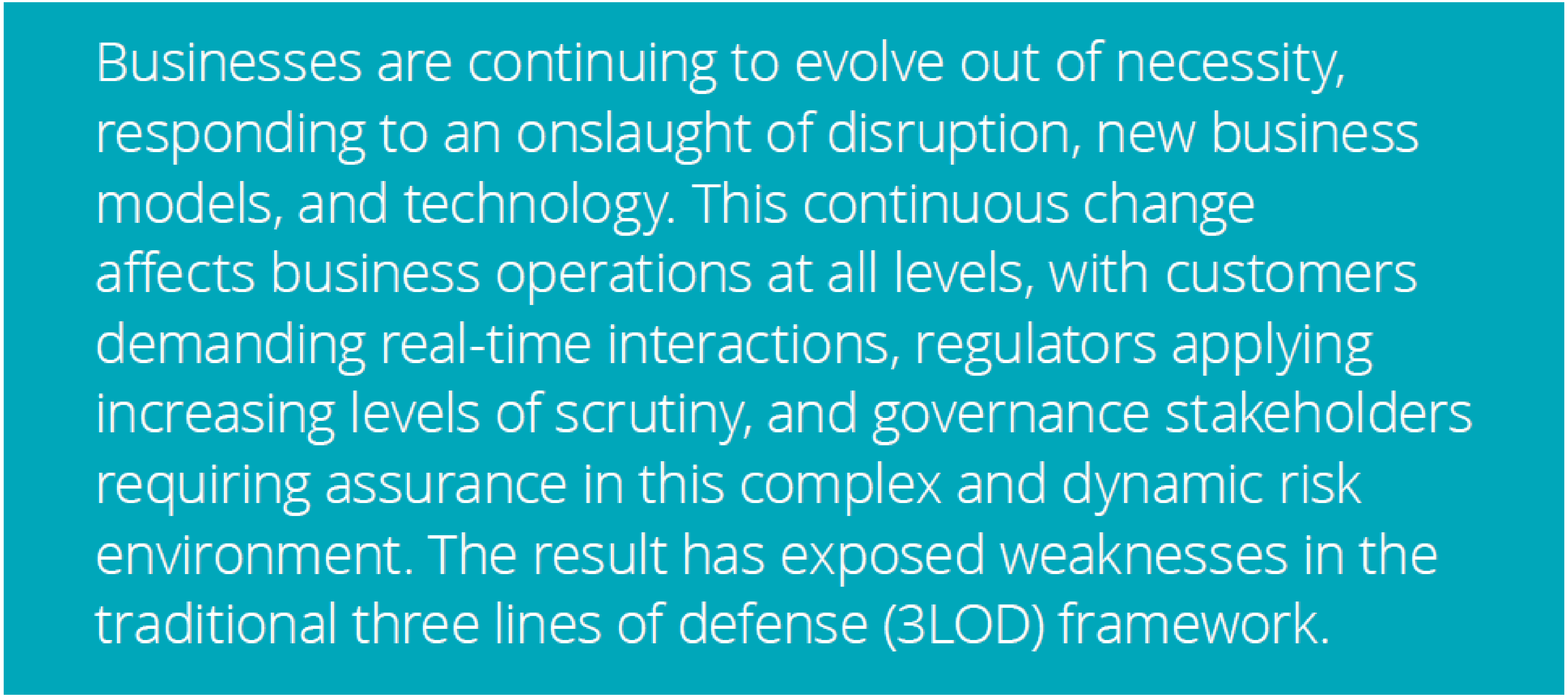
Key Issues	Causes
• Disruption due to equipment failure or power outage • Backup/ Recovery failure • High network latency for end users • RTO/RPO requirements not met	• UPS/ Load distribution not up to date • Hardware/ Network Failure • CDN not optimized or not present • DC/DR architecture not setup to meet RTO/RPO requirements

Resolution
• Run failure simulations to assess the equipment health • Deploy and optimize CDN • Build redundancy at the Network layer • Optimize DC DR location and architecture • Conduct regular DR/BCP Tests



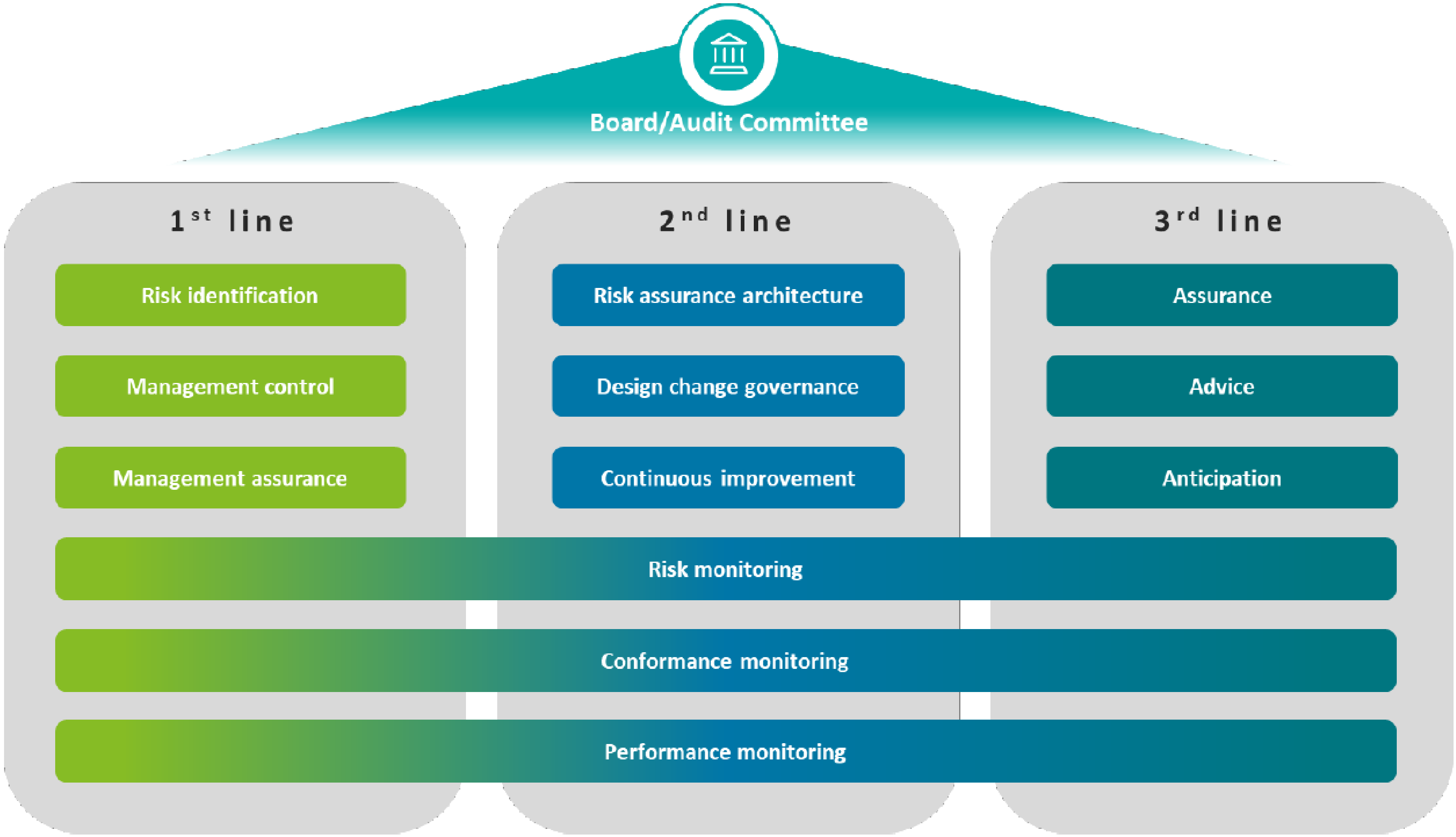
Modernizing the Three Lines Model

Modernizing the Three Lines Model



Businesses are continuing to evolve out of necessity, responding to an onslaught of disruption, new business models, and technology. This continuous change affects business operations at all levels, with customers demanding real-time interactions, regulators applying increasing levels of scrutiny, and governance stakeholders requiring assurance in this complex and dynamic risk environment. The result has exposed weaknesses in the traditional three lines of defense (3LOD) framework.

Three Lines Model



Board/Audit Committee

1st line

- Risk identification
- Management control
- Management assurance

2nd line

- Risk assurance architecture
- Design change governance
- Continuous improvement

3rd line

- Assurance
- Advice
- Anticipation

Risk monitoring

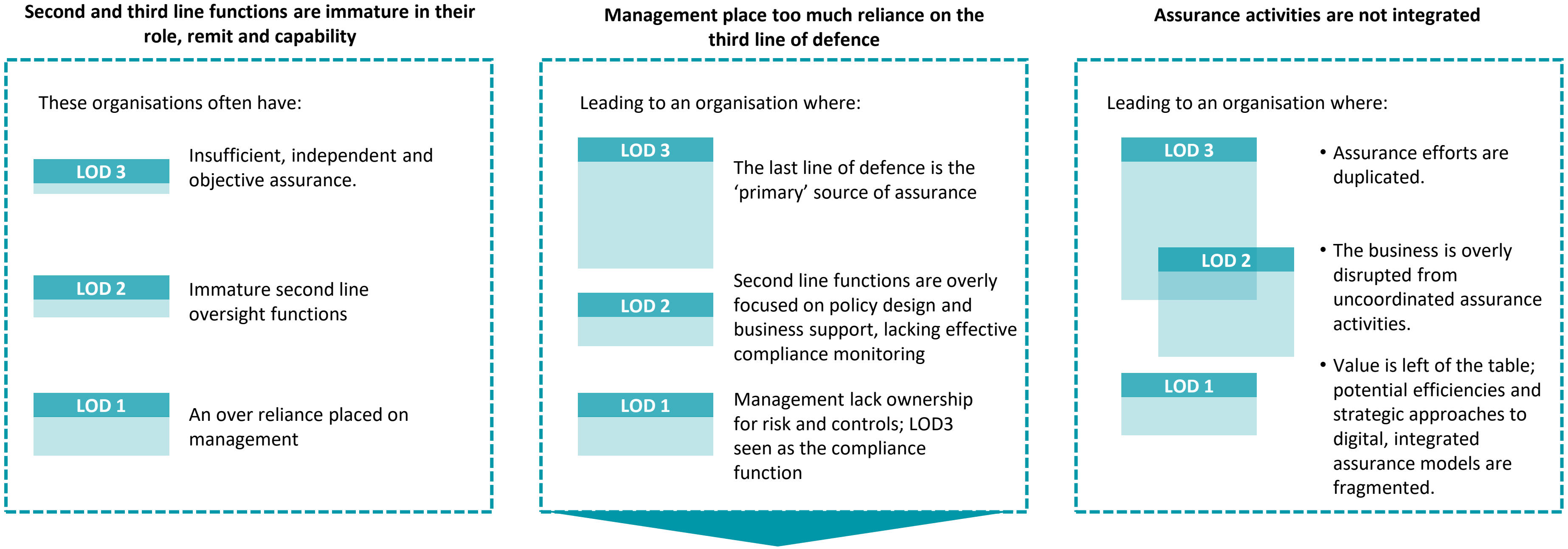
Conformance monitoring

Performance monitoring

Today’s three lines of defence

TODAY

The three lines of defence model is well understood but implemented in a range of forms and levels of maturity.
For example in many organisations:



Second and third line functions are immature in their role, remit and capability

These organisations often have:

LOD 3 — Insufficient, independent and objective assurance.

LOD 2 — Immature second line oversight functions

LOD 1 — An over reliance placed on management

Management place too much reliance on the third line of defence

Leading to an organisation where:

LOD 3 — The last line of defence is the ‘primary’ source of assurance

LOD 2 — Second line functions are overly focused on policy design and business support, lacking effective compliance monitoring

LOD 1 — Management lack ownership for risk and controls; LOD3 seen as the compliance function

Assurance activities are not integrated

Leading to an organisation where:

- Assurance efforts are duplicated.
- The business is overly disrupted from uncoordinated assurance activities.
- Value is left of the table; potential efficiencies and strategic approaches to digital, integrated assurance models are fragmented.

Where too much reliance is placed on the third line, Internal Audit functions can:

- Spend a disproportionate amount of time on compliance, detracting from the truly greatest risks;
- Erode trust with management; Internal Audit are perceived as a ‘policing function’;
- End up reporting low-level compliance exceptions, failing to create impact or drive change; and
- Create an industry of management actions and follow-up, often distracting the business from managing greater risks.

The opportunity to drive change

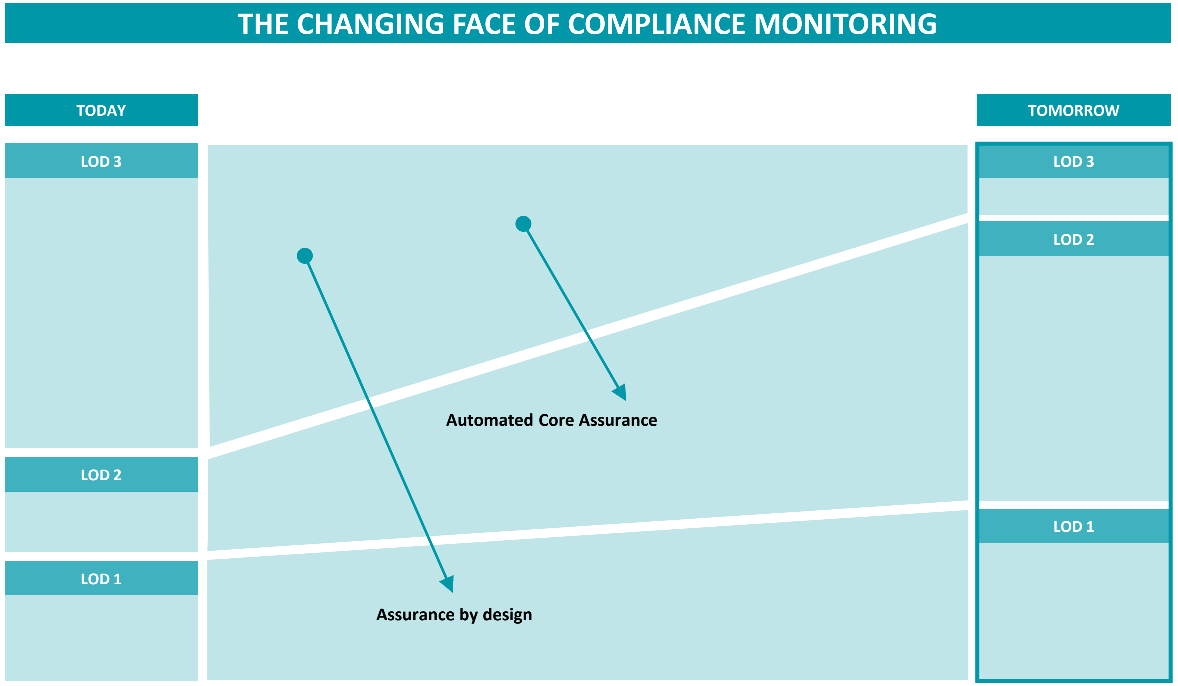
- New technologies are creating an environment in which assurance mechanisms can be designed into the first line of defence.

- Similarly, tech-enablement is also helping second line functions take greater ownership of compliance monitoring.

- Internal Audit can help organisations revisit the design of assurance across the three lines of defence. For example, by advising the first line on how to build assurance mechanisms into the design of systems and processes.

- In an ideal world, second line functions would lead the transformation of their compliance monitoring capabilities. In practice, they will need support.

- As the historic assurance providers for compliance monitoring, Internal Audit functions can pioneer the adoption of robotics and AI to 'automate assurance' over core processes, and export this capability to the second line.



Tomorrow’s three lines of defense

ASSURANCE STRATEGY - A single assurance strategy on the providers and users of assurance to bring clarity to the assurance landscape, the demand drivers (setting the dial), and supply options (optimising the assurance layers).

COMMON METHODOLOGY & TOOLS - A common, or aligned, methodology and supporting tools, to drive minimum standards and enable cross functional reliance on different sources of assurance.

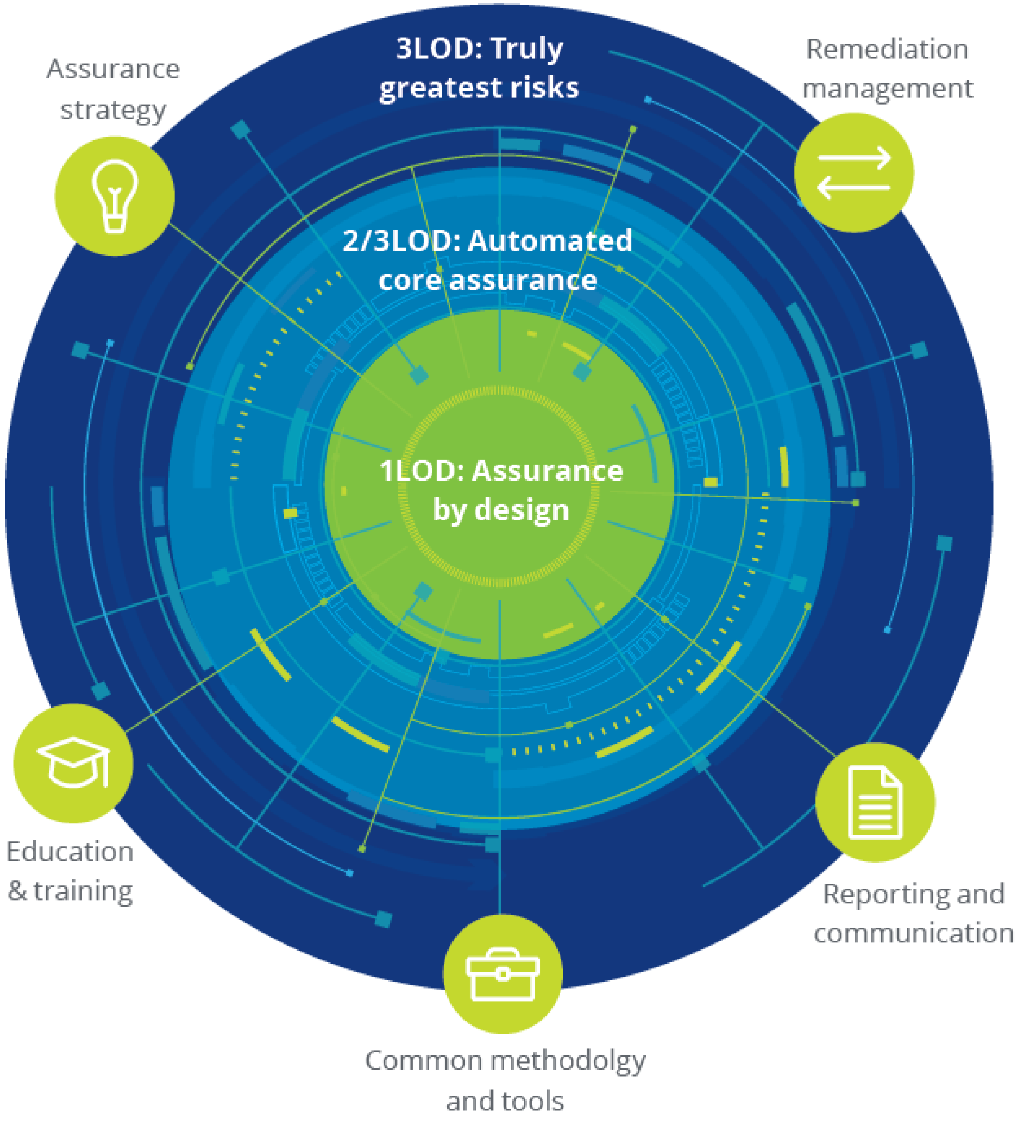
REPORTING & COMMUNICATION / REMEDIATION MANAGEMENT - Integrated reporting, communication, and remediation management of assurance outcomes, leveraging a common digital risk management and assurance platform.

EDUCATION & TRAINING - Co-ordinated education and knowledge sharing efforts to maximise learning and continuous improvement from assurance outcomes.

ASSURANCE BY DESIGN - Greater ownership of assurance within LOD 1 through enhanced controls and embedding self-assurance mechanisms into the design of systems and processes.

AUTOMATED CORE ASSURANCE - Tech-enabled LOD2 (Robotics Process Automation, Artificial Intelligence, and Analytics) to automate assurance over the control environment and enable real time monitoring and remediation of control weaknesses.

TRULY GREATEST RISKS - A strategic and holistic LOD3 assurance provider, focusing on the design and performance of assurance activities, providing advice on the truly greatest risks, and helping to anticipate new challenges.


Assurance strategy
3LOD: Truly greatest risks
Remediation management
2/3LOD: Automated core assurance
1LOD: Assurance by design
Education & training
Reporting and communication
Common methodolgy and tools

Internal Audit of the Future

Feedback-oriented
Willing to give and receive difficult feedback, and adapt based on feedback received

Collaborative
Works closely with others, particularly with non-technical backgrounds

Communicative
Comfortable packaging and presenting information in different ways

Business-oriented
Driven to execute against business objectives, finding the right path to achieve them

Analytical
Sees and interprets connections between information

Innovative
Creatively approaches problems, embracing new techniques

Inquisitive
Asks productive questions and focuses on delivering clear and compelling answers

Entrepreneurial
Comfortable working through ambiguity and outside of formal structure

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

About Deloitte Thailand
In Thailand, services are provided by Deloitte Touche Tohmatsu Jaiyos Co., Ltd. and its subsidiaries and affiliates.

Disclaimer for proposals
This document has been prepared by Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd. for the sole purpose of providing a proposal to the parties to whom it is addressed in order that they may evaluate the capabilities of Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd. to supply the proposed services.

The information contained in this document has been compiled by Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd. and includes material which may have been obtained from information provided by various sources and discussions with management but has not been verified or audited. This document also contains confidential material proprietary to Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd.. Except in the general context of evaluating our capabilities, no reliance may be placed for any purposes whatsoever on the contents of this document or on its completeness. No representation or warranty, express or implied, is given and no responsibility or liability is or will be accepted by or on behalf of Deloitte Touche Tohmatsu Jaiyos Advisory Co., Ltd. or by any of its partners, members, employees, agents or any other person as to the accuracy, completeness or correctness of the information contained in this document or any other oral information made available and any such liability is expressly disclaimed.

This document and its contents are confidential and may not be reproduced, redistributed or passed on, directly or indirectly, to any other person in whole or in part without our prior written consent.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment.