

EISNERAMPER

Internal Audit Insights for the Insurance Industry

Wednesday, September 13th, 2023



Agenda

Intro and Overview

Internal Audit

Emerging
Technologies

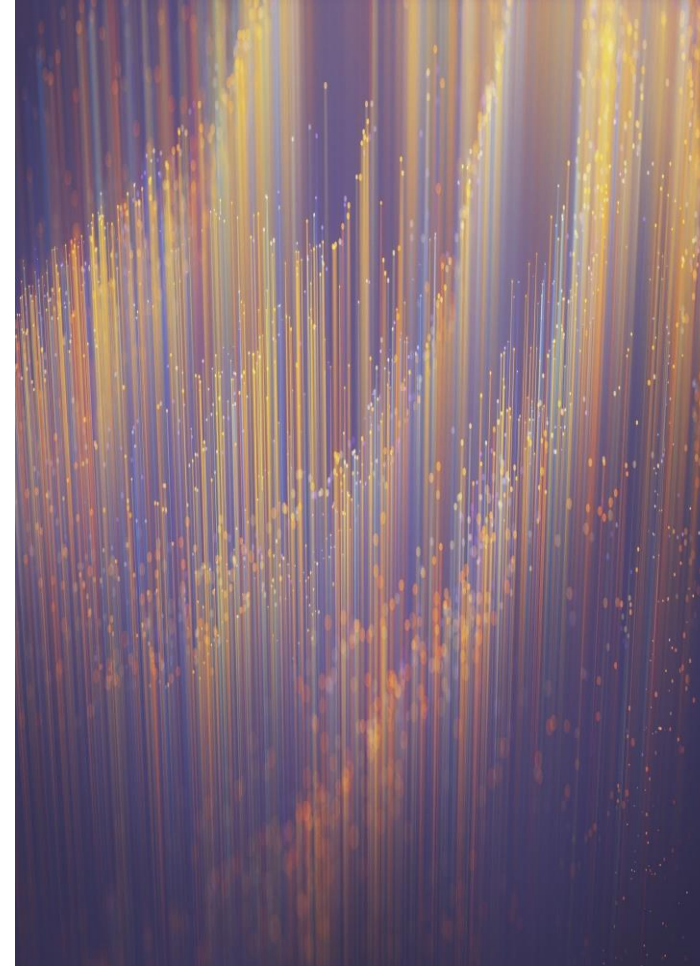
Wrap-Up

1. About Us
2. An Evolving Landscape

1. 3 Lines of Defense
2. Best Practices
3. Lessons Learned
4. Cyber Assessments

1. A Seismic Change
2. AI & The Blockchain
3. Use Cases
4. Implications

1. Concluding Remarks
2. Questions?
3. Contact Us



Intro and Overview



Our Presenters:



Raymond Soriano

Director, Eisner Advisory Group LLC

30 years of experience in internal audit, technology, and information security.

CSF, CRISC

University of Phoenix: BS; MS, Management



Gaini Umarov

Senior Manager, Eisner Advisory Group LLC

10 years of experience in IT and business advisory services.

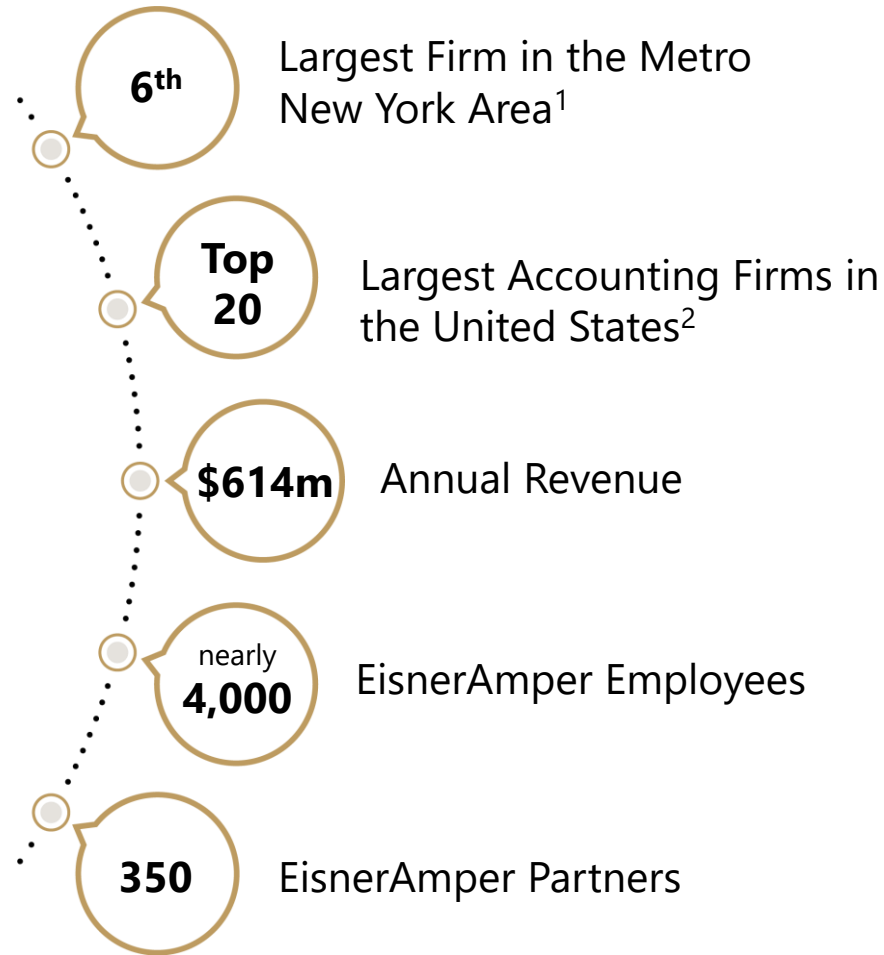
CISA, PMP, ITILvF

University of Essex, United Kingdom: BS, Business Management

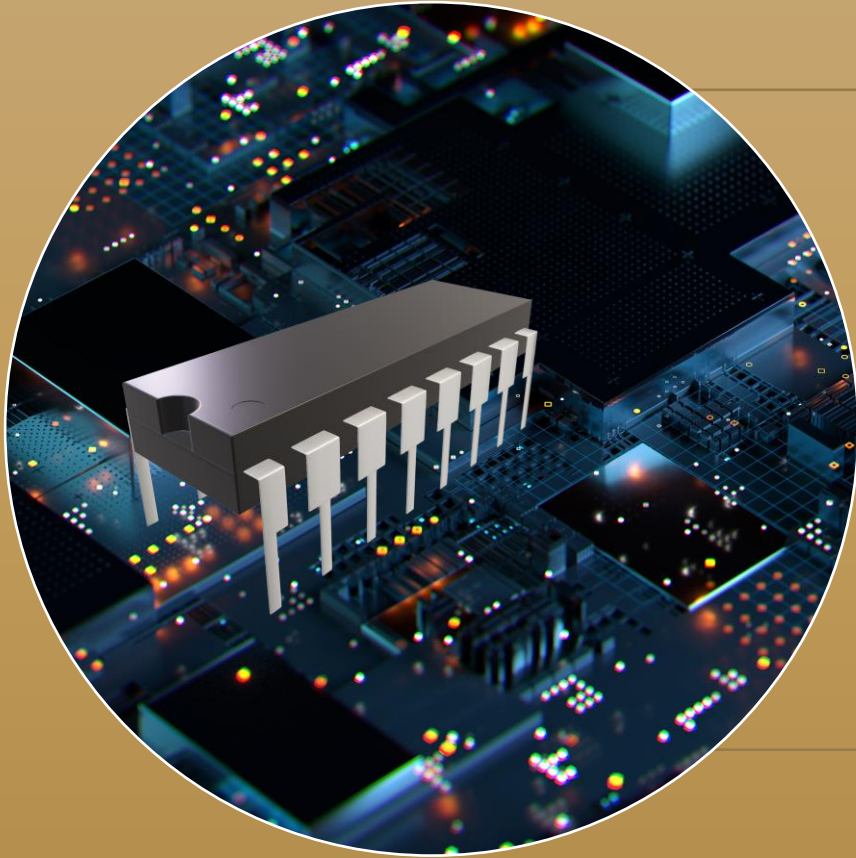


About Us: EisnerAmper Digital

Audit, accounting, tax, and business advisory professionals serving public and private companies across a broad range of industries.



An Evolving Landscape



Technology Risk IS Financial Risk

- Risk management plays a pivotal role in the sustainability and success of insurance companies



According to IBM, the average cost of a data breach is **\$4.45 million**

- With the emergence of new technologies and risks in the ever-changing landscape of the industry, organizations are faced with numerous challenges that necessitate effective risk management practices



For U.S. data breaches, the average cost rises to **\$9.48 million**

- Increasing SEC guidance introduced on how to handle breaches to strengthen cyber risk management response¹


¹ [SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies](https://www.sec.gov/cybersecurity)





Importance of Industry Best Practices


Notable Recent Data Breaches

 Bitmarck
•April 2023
•Systems taken offline; Patient data “was and is never endangered”

 Point32Health
•April 2023
•Ransomware Attack

 LATITUDE
•March 2023
•14 million customer records stolen (largest data breach in NZ history)

 Capita
•March 2023
•Data taken from 0.1% of servers; estimated costs of up to £20 million

 NationsBenefits
•January 2023
•Information for potentially 3 million subscribers stolen; class action pending

- Insurance Groups are often targeted for the **personal and financial data** (PII, PHI, etc.) that they possess
- Adherence to anything less than Best Practices exposes any company to **greater risk** for data breaches and cyber crime
- According to a 7/25/2023 IBM Report, 82% of breaches involved data stored in the cloud



Internal Auditing



Lines of Defense

The “Three Lines of Defense” of User Access Recertification refer to the three stages of the best-practice process to **ensure the security and integrity of sensitive information and systems**

1



Line 1: Application Owners & Admins

Roles/Responsibilities:

- Continuous monitoring of respective application user base
- Quarterly review and documentation of User Access Listings
- Notify 2nd and 3rd lines of defense in the event of control changes

2



Line 2: Corporate IT & Security

Roles/Responsibilities:

- Corporate IT monitoring to ensure provisioning & deprovisioning is conducted in a timely manner
- Monitoring & review of logical access control execution

3



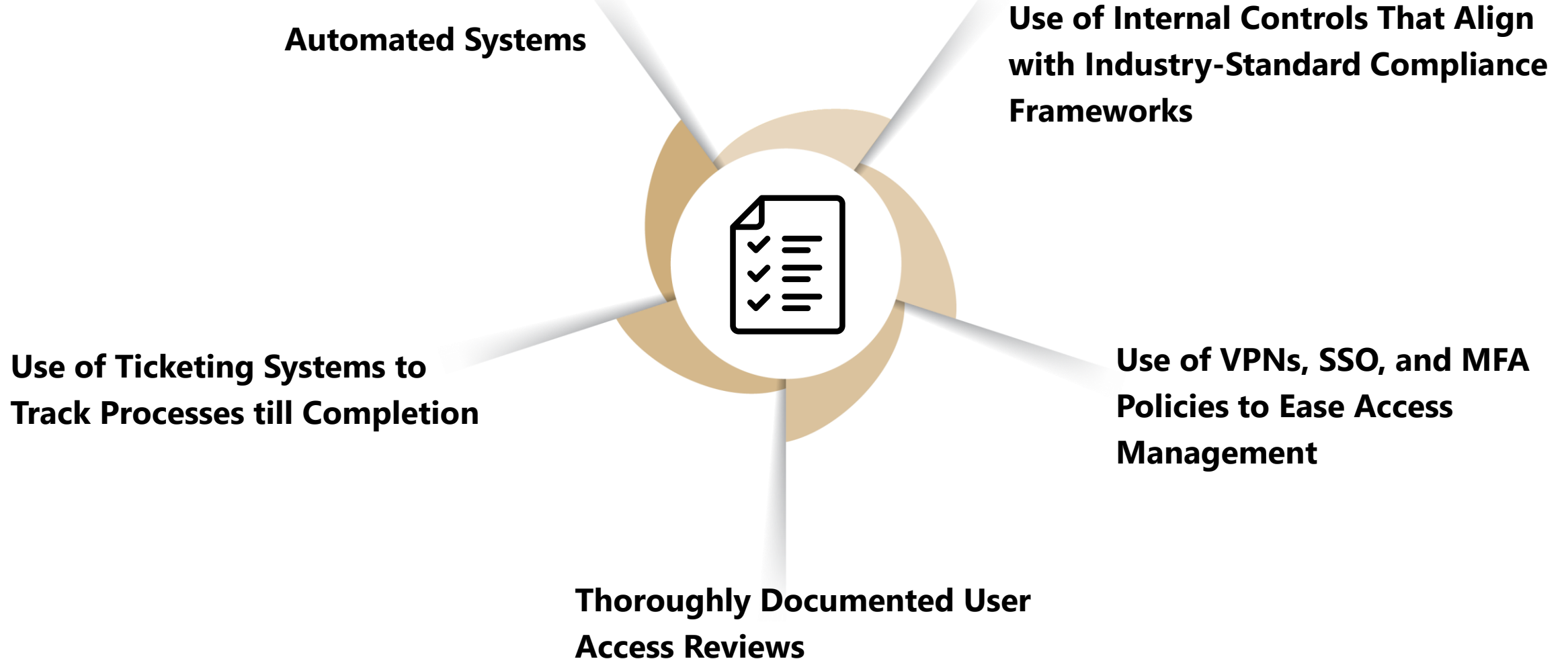
Line 3: Independent Auditors

Roles/Responsibilities:

- Objective assessment of logical access controls in place
- Compliance with regulatory requirements ensured
- Provides assurance of control effectiveness to stakeholders

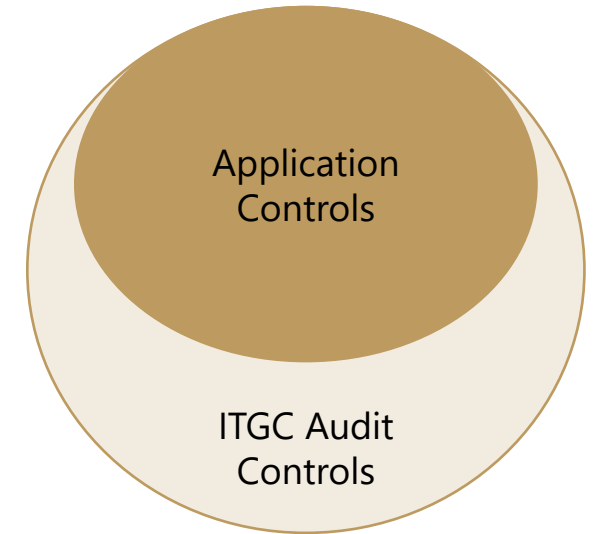


Best Practices: Universal Procedures



Best Practices: Specialized Policies

- Application Controls
 - Many compliance frameworks require specialized controls for applications that can impact financially relevant data.
 - Implementation of effective Application controls helps tighten an organization's risk management policies, mitigate risks not covered by ITGC's, and improves the organization's cybersecurity environment.
 - When designing an application control, keep in mind the following questions:



How could this application have a financially material impact on our organization?

What is the likelihood that this application negatively impacts our organization?

What steps can we take to further reduce this risk?

Which personnel will be responsible for implementing this control?



Best Practices: Vendor Applications



**Ensure Relevancy
of Contracts**



**Use of
Trustworthy
Organizations**

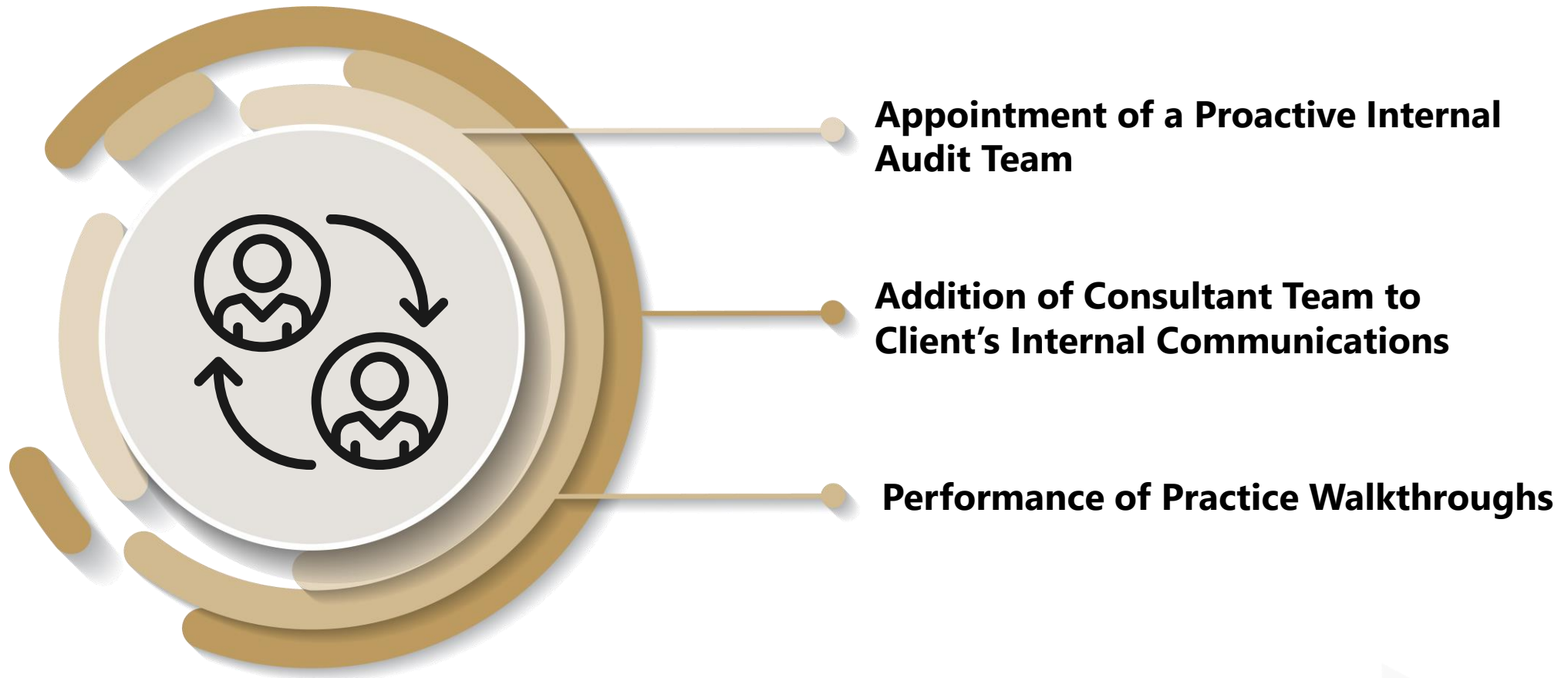


**External Admin
Reviews**



**Maintain a Positive
Relationship with
Vendors**

Best Practices: Communication with Internal Auditors



Best Practices: Communication with External Auditors



**Accurate, Up-to-Date
Dashboards**



Use of Audit Tools



Agile Approach



Example Agile Approach to Internal Audit

Day	Weekly Preparation	Monday	Tuesday	Wednesday	Thursday	Friday
Action	<ul style="list-style-type: none"> Common agile sprints first provide an agenda and potential document requests to the client for preparation of the sprint. 	<ul style="list-style-type: none"> Walkthrough conducted to demonstrate the controls currently in place Obtain evidence of a first sample – Test of Design phase If applicable, the population will be sampled for testing 	<ul style="list-style-type: none"> Supporting documentation is provided by client Review of the evidence received and, if needed, follow up with client 	Checkpoint meeting: <ul style="list-style-type: none"> Status Any missing evidence Potential Deficiencies 	Quick Touchpoint (if needed): <ul style="list-style-type: none"> Any pending items Any additional questions Potential Deficiencies 	Wrap-up call: <ul style="list-style-type: none"> Summary of deficiencies noted (if any) Discussion of Next steps, Mitigations and Remediations Any Potential pending items, follow-ups
Estimated Time	NA	1 hour to 1.5 hours	30 min (if needed)	30 min	30 min (if needed)	30 min-1 hour

Key Recommendations:

- Suggest to design the sprints based on system owner’s availability.
- If the system owner is responsible for multiple applications, one sprint can cover all of them.
- Sprints help in reduction of multiple follow-ups and Email exchanges.
- Sprints also help to keep the workload limited in time and to prevent audit fatigue.



Cyber Risk Assessments

Primary Goals:

Provide a **birds-eye-view** of your organization's cybersecurity environment



Review current policies & procedures to identify areas of improvement

Identify unknown issues present within your organization

Best Practices & Benefits:

- Encourage effective coordination between IT consultants & security teams to increase efficiency
 - Align the goals of security teams with IT consultants
- Proper leverage of the findings of the cyber risk assessments facilitates positive change within your organization
- Align your organization with compliance requirements



Cyber Liability Insurance

- Engineered to manage the risks of cyberattacks and data breaches in the modern business landscape
- Often customizable, including **First-party Coverage** (i.e., expenses related to business interruption and crisis management) and **Third-party Coverage** (i.e., legal costs if a third-party sues, possible litigation, etc.)

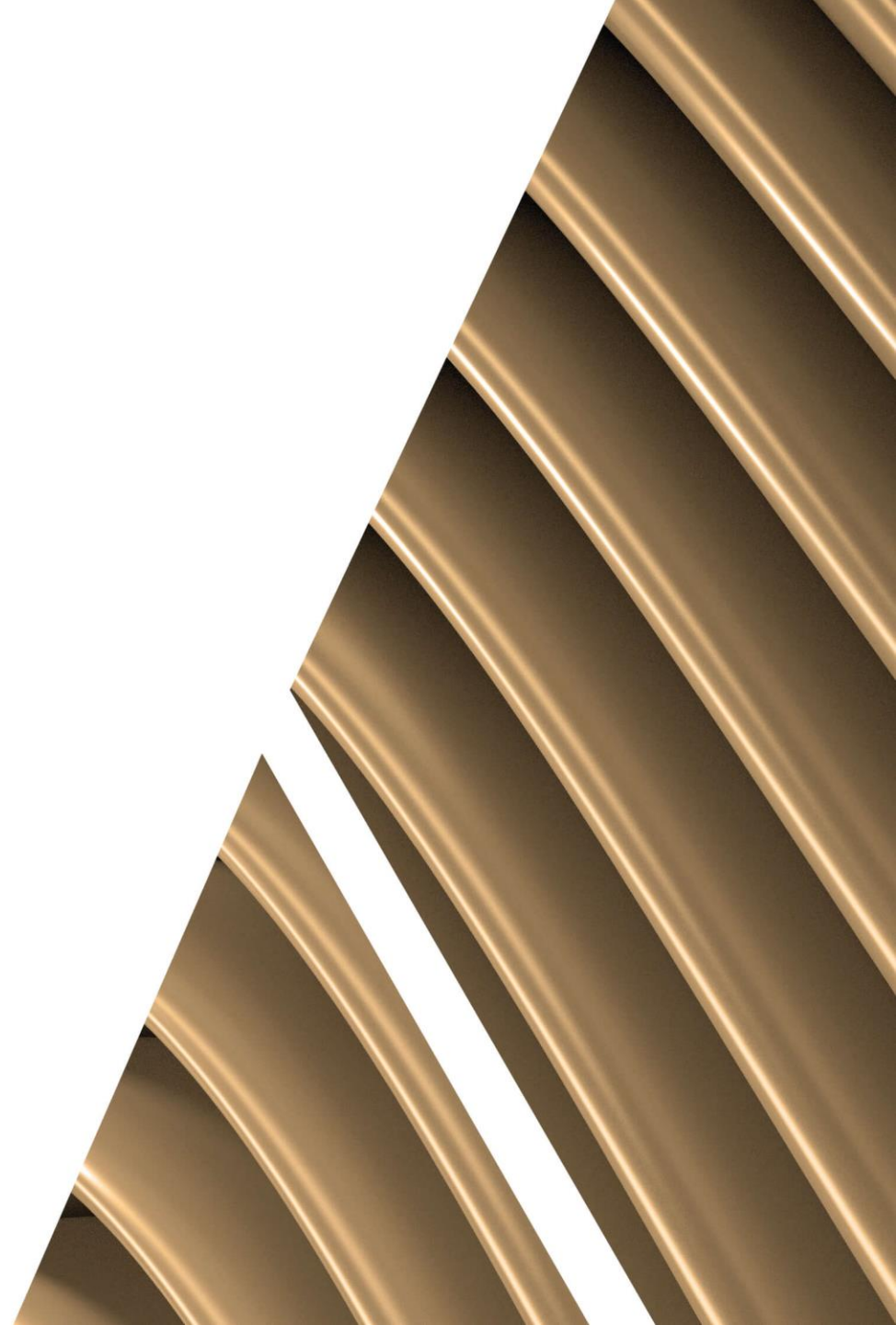
MANAGES RISKS STEMMING FROM

Malware	Ransomware	Phishing	Denial-of-Service	And More...
<ul style="list-style-type: none"> • Usually designed for damage • Various forms and goals 	<ul style="list-style-type: none"> • Designed for locking down • Payment for release • Surged in 2022 	<ul style="list-style-type: none"> • Email Phishing • Spear Phishing • Many Others... 	<ul style="list-style-type: none"> • DDoS if large-scale • GitHub 2018 	<ul style="list-style-type: none"> • Terrorist Acts • International Cyber Attacks

Sampling of U.S. Cyber Insurance Firms:



Artificial Intelligence



A Seismic Change



Harnessing the Power of AI In the Insurance Sector
April 17, 2023 - [Harnessing The Power Of AI In The Insurance Sector \(forbes.com\)](https://www.forbes.com)

Training Machines To Learn More Like Humans Do
May 9, 2023 - [Training machines to learn more like humans do | MIT News | Massachusetts Institute of Technology](https://news.mit.edu)

ChatGPT Was a Black Swan Event
May 24, 2023 - [ChatGPT Changed Everything and Was a Black Swan Event \(businessinsider.com\)](https://www.businessinsider.com)



Artificial Intelligence Use Cases:

Faster Underwriting



- AI facilitating risk analysis
- Rapid and precise response to new data

Easier Claims Processing



- Faster submission analysis
- Near-instant cost estimates

Fraud Prevention



- Predictive analytics
- Analyzing datasets for abnormalities

Customer Service



- Streamlined Service
- Personalized service without human intervention (i.e., chatbots)

AI IN INSURANCE



Nauto - Driver Safety System based on AI and Telematics

Nauto

Cytora

Cytora - Platform for underwriting transformation

Cytora



Metromile - Pay-as-you-drive Auto Insurance

Metromile

zest finance

Zest AI - Financial company driven by AI

Zest AI



Lemonade - Leverages AI to improve customer experiences

Lemonade



Implications

Faster Purchasing Timeline

- AI-driven customer service will accelerate the insurance shopping process

Improved “Instant Quotes”

- Maturing of pricing algorithms will expand the ability to offer reliable “instant quotes”

Use-Based-Insurance

- Normalization of Dynamic UBI products will transition most insurance from the traditional renewal model to a more continuous and adaptive model

Automated Underwriting

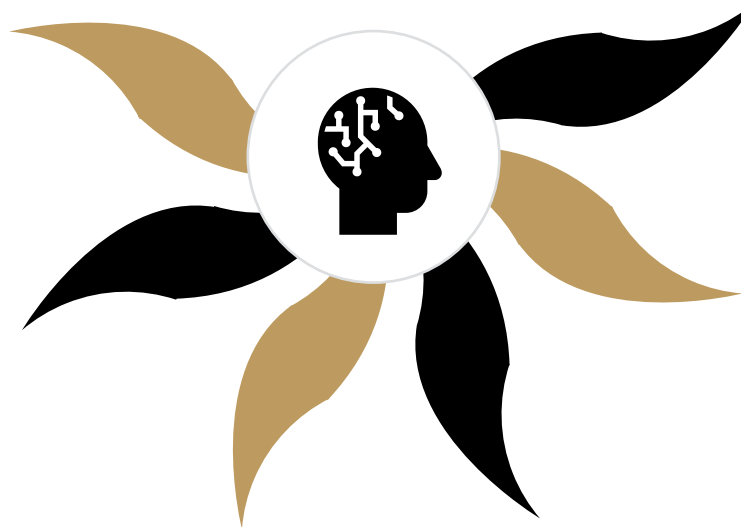
- AI and ML are expected to automate the underwriting process thanks to their vast pools of data and maturing analytical capabilities

Engaged Employees

- Not just IT teams, but also the C-suite and customer service teams will invest the resources required to understand the new omnipresent AI technology

Quick Claims

- Improved automation and algorithms will lead to increased claims processing power



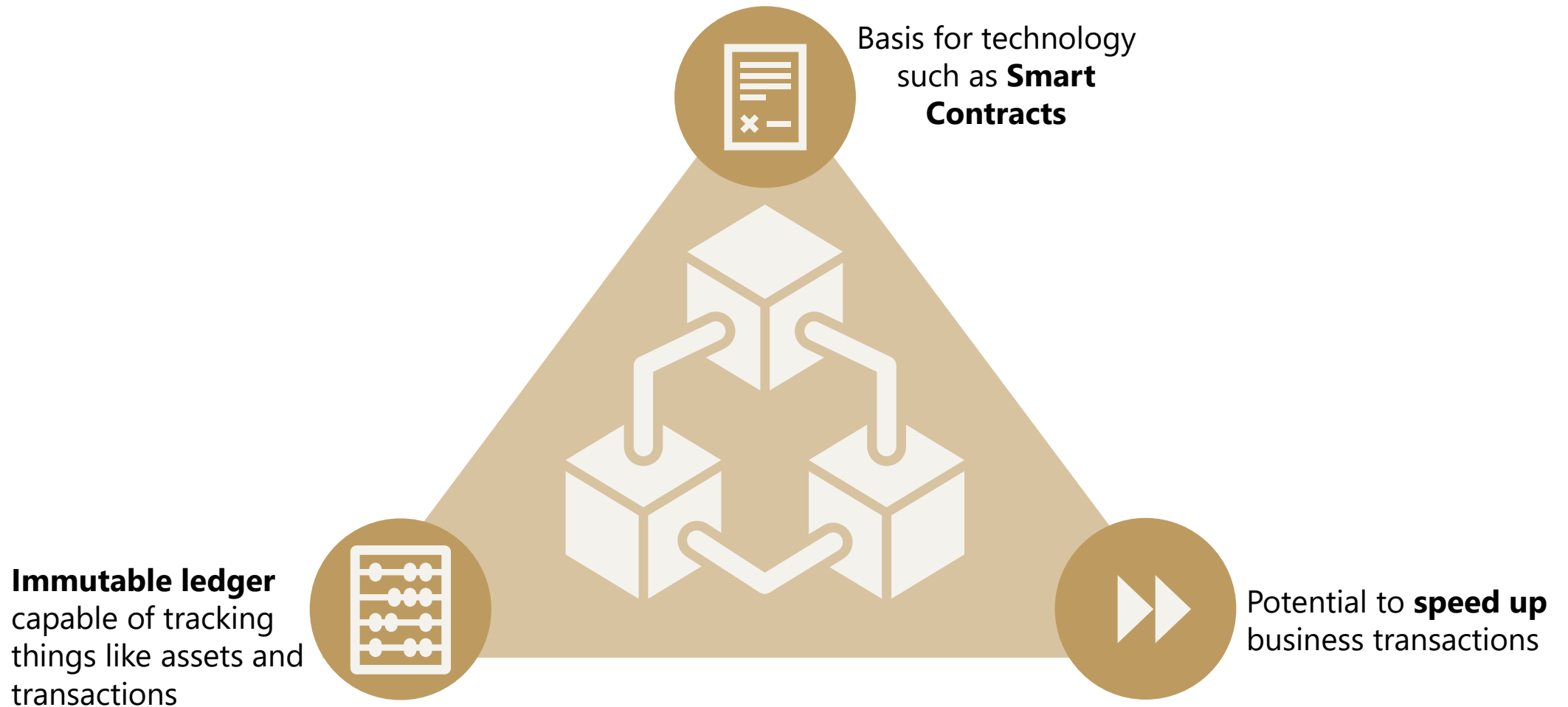
¹ <https://www.mckinsey.com/industries/financial-services/our-insights/insurance-2030-the-impact-of-ai-on-the-future-of-insurance>



Blockchain



Blockchain Overview



Use Cases

Smart Contracts



- Digital contracts stored on a blockchain
- Self-execute once certain predetermined conditions are met
- Immutable and Permanent
- Potential to lower administrative costs
- Viable when contract terms can easily be transcribed into immutable code, but struggle to translate concepts like “good faith” and “reasonableness”

Cryptocurrency-Related Insurance



- Insurance for risks related to holding and managing crypto, including technology liability and cyber liability insurance
- Nascent product offering

BLOCKCHAIN IN INSURANCE

RYSKEX

Ryskex - Uses Quorum blockchain technology developed by JP Morgan

superscript

Superscript - Lloyd's broker; Offers Daylight, insurance targeted at crypto business risk



Black.Insure - Blockchain-enabled Platform-as-a-Service



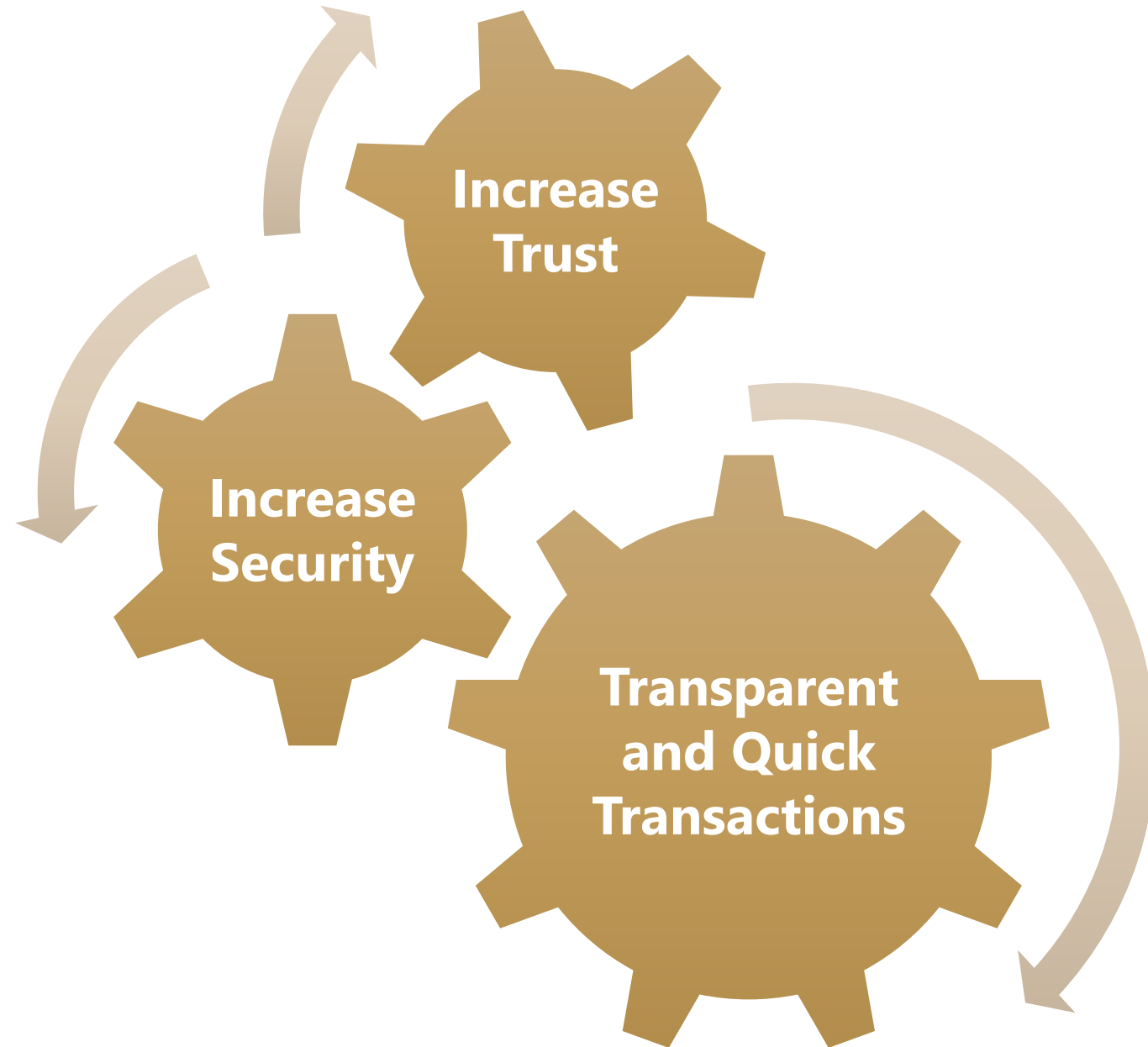
Lemonade - Crypto Climate Coalition, blockchain-based crop protection aimed at subsistence farmers, built on Avalanche



Avalanche - Infinitely-scaling smart contracts platform



Implications



Wrap-Up



Our Mission



Helping Finance and Technology Leaders Transform Risk Into Opportunity

Technology risk IS financial risk - the average cost of a data breach is \$4.45 million.

Partnering with our Technology Risk professionals not only lets you see the big picture and uncover risks that were previously invisible, it also helps you make confident investment decisions, build trust and achieve “peace of mind” in your technology and transformation strategy with stakeholders.

Questions?





This publication is intended to provide general information to our clients and friends. It does not constitute accounting, tax, or legal advice; nor is it intended to convey a thorough treatment of the subject matter.

"EisnerAmper" is the brand name under which EisnerAmper LLP and Eisner Advisory Group LLC and its subsidiary entities provide professional services. EisnerAmper LLP and Eisner Advisory Group LLC practice as an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations and professional standards. EisnerAmper LLP is a licensed independent CPA firm that provides attest services to its clients, and Eisner Advisory Group LLC and its subsidiary entities provide tax and business consulting services to their clients. Eisner Advisory Group LLC and its subsidiary entities are not licensed CPA firms. The entities falling under the EisnerAmper brand are independently owned and are not liable for the services provided by any other entity providing services under the EisnerAmper brand. Our use of the terms "our firm" and "we" and "us" and terms of similar import, denote the alternative practice structure conducted by EisnerAmper LLP and Eisner Advisory Group LLC.