ISACA

JPA INTERNATIONAL | TRIPLE LEDGER LIMITED
Assurance. Consulting. Training.
New Zealand

DIGITAL TRUST

BOARD BRIEFING

#BuildingDigitalTrustTogether

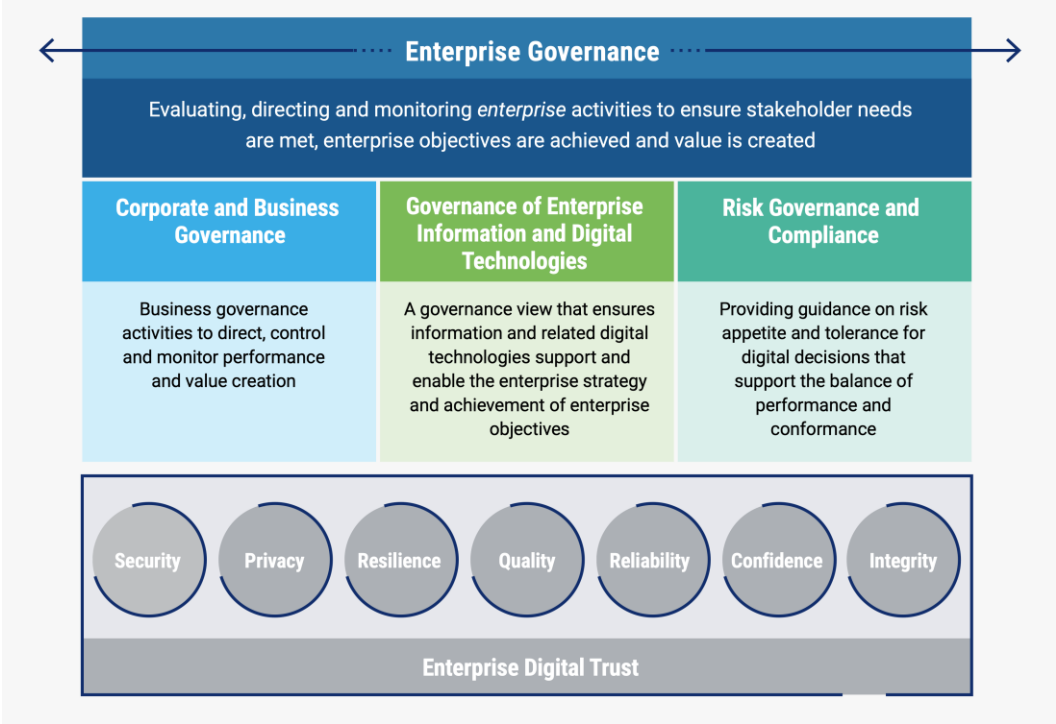
On Stage Today

Jason Wood

Managing Director
Triple Ledger Limited

- FMA licensed Auditor
- Chair and past president ISACA Auckland
- Certified Information Systems Auditor (CISA),
- Certified Internal Auditor (CIA)

Governance of Enterprise Digital Trust



- ISACA defines digital trust as the **confidence** in the **integrity** of the **relationships**, **interactions** and **transactions** among providers and consumers within an associated digital ecosystem.
- This includes the ability of **people, organisations, processes, information and technology** to create and maintain a trustworthy digital world.

WAYS TO FOSTER DIGITAL TRUST

The 8 Pillars

Define, communicate and support enterprise values and principles related to digital trust.

Establish or delegate the appropriate organizational structures to assist in the governance and management of digital trust.

Allocate resources and funding for digital trust investments aligned with organizational goals and objectives.

Establish communication mechanisms that provide those with digital trust responsibilities oversight and feedback on digital trust initiatives.

Create and monitor a reward system to promote desirable outcomes with regard to digital trust.

Actively support emergence that socializes management's support of digital trust activities (i.e., continual improvement).

Evaluate the effectiveness of the organization's digital trust practices and celebrate successes in relation to digital trust initiatives.

Create, enforce and update appropriate digital trust-related policies.

What the Board Should be Doing

What the Board Should Expect From Management

The Governing Body and Digital Trust—Five Principles

Below are the key digital trust principles for organizational boards and governing bodies.
All principles should be considered, not just one or two.

What the Board Should be Doing

What the Board Should Expect From Management

1

Principle 1
Systems Thinking

Boards must understand and approach digital trust as a strategic enterprise enabler and holistic system to achieve enterprise objectives and stakeholder needs—not just as an IT, security or privacy concern.

2

Principle 2
Risk Governance

Boards should understand the risk and benefits of digital trust with respect to the organization's circumstances and provide appetite and tolerance guidance.

3

Principle 3
Awareness

Boards should have adequate access to digital, cybersecurity and privacy expertise, and discussions about digital trust should be given adequate time regularly on board meeting agendas.

4

Principle 4
Appropriate Framework

Boards should set the expectation that management will establish an enterprisewide digital trust framework with adequate monitoring, reporting, training and budget.

5

Principle 5
Risk Management

Board-management discussions should include the identification and quantification of exposure to digital trust risk and which risk to avoid, accept, mitigate or transfer.

The 5 Trust Principles

PRINCIPLE 1

Systems Thinking

Boards must understand and approach digital trust as a strategic enterprise enabler and holistic system to achieve enterprise objectives and stakeholder needs—not just as an IT, security or privacy concern.

At the highest level of the organization, "systems thinking" is often synonymous with a holistic approach.

Key considerations for this principle include:

- Consider all enterprise activities as a whole, rather than as separate parts, and establish an understanding of how changes in one part of the organization can impact others.
- View digital trust as the umbrella over all privacy and cybersecurity matters.
- Integrate frameworks into the overall framework ecosystem, supporting systems thinking.
- Integrate enterprise architecture principles to model the current and future states of the enterprise "building blocks."

PRINCIPLE 2

Risk Governance

Boards should understand the risk and benefits of digital trust with respect to the organization's circumstances and provide guidance on risk appetite and tolerance.

There is a distinction between risk governance and risk management. Risk governance is responsible for guiding management in areas like risk appetite and tolerance and providing the delegation of authorities to management regarding actions taken.

Key considerations for this principle include:

- Identify, communicate and enforce risk appetite and tolerance levels across the organization to ensure that proper risk decisions align with the overall risk profile.
- Develop an enterprise risk register that receives inputs from other, more detailed registers throughout the organization.
- Develop appropriate authority levels for handling certain types of risk and determine escalation procedures for risk that exceeds those authority levels.
- Associate digital trust risk scenarios with business risk.

The 5 Trust Principles

PRINCIPLE 3

Awareness

Boards should have adequate access to digital, cybersecurity and privacy expertise, and discussions about digital trust should be given regular and adequate time on board meeting agendas.

Understanding the dynamic digital trust environment requires constant communication.

Key considerations for this principle include:

- Leverage external expertise for the board to ensure the most recent industry information is considered when making digital trust decisions.
- Ensure that digital trust outcomes are linked to successes in security, privacy and quality domains.
- Create a communication plan that endorses transparency throughout the organization regarding digital trust topics.
- Continually adjust the approach to digital trust as internal/external factors and organizational goals change.

PRINCIPLE 4

Appropriate Framework

Boards should set the expectation that management will establish an enterprise-wide digital trust framework with adequate monitoring, reporting, training and budget.

The board should expect management to establish an enterprise framework to address digital trust. A framework is the supportive structure for enabling the digital trust ecosystem that supports an organization's vision, mission, values, objectives and strategies. ISACA's Digital Trust Ecosystem Framework is one approach to managing digital trust initiatives.

Key considerations for this principle include:

- Select a framework that is open, flexible and aligned with major standards and industry models.
- Ensure the framework is holistic, tailorable and addresses all aspects of the digital trust ecosystem.
- Use the digital trust framework as a complement to and an extension, not a replacement, of current frameworks in the ecosystem.

The 5 Trust Principles

PRINCIPLE 5

Risk Management

Board-management discussions should include the identification and quantification of exposure to digital trust risk and which risk to avoid, accept, mitigate or transfer.

Not to be confused with risk governance, risk management is delegated from the board to management.

Key considerations for this principle include:

- Define a risk management process that identifies, assesses, responds to and monitors risk related to digital trust.
- Determine criteria for risk assessments such as likelihood and impact.
- Identify risk response options for digital trust, including accepting, avoiding, transferring or mitigating.
- Ensure that risk-based decisions are consistent with the risk governance guidance.

Bridging Business and Technology

Ready For Building Digital Trust?

Jason Wood

- FMA licensed Auditor & Managing Director Triple Ledger
- Chair and past president ISACA Auckland
- Certified Information Systems Auditor (CISA),
- Certified Internal Auditor (CIA)

Website
www.tripleledger.com

Email
jason.wood@tripleledger.com

Telephone
+64 27 403 9587

Address
139 Quay Street, Level 8, Auckland

Building Digital Trust Together

ISACA

JPA INTERNATIONAL

TRIPLE LEDGER LIMITED
Assurance. Consulting. Training.
New Zealand