

# Empowering NGOs through Effective IT Governance: From Initiation to Implementation

**Frank Chow**

**Vice-Chairperson**

**Professional Information Security Association**

**10 July 2024**



## Mr. Frank Chow

CGEIT CISSP-ISSAP-ISSMP CSSLP CCSP CISA CISM CRISC CDPSE CEH  
CHFI CBCP TOGAF PMP

Vice-Chairperson  
Professional Information Security Association

Director  
Cloud Security Alliance Hong Kong & Macau Chapter

Council Member  
Information Security and Forensics Society

Executive Committee  
ISC2 Hong Kong Chapter

Vice President  
Project Management Institute Hong Kong Chapter

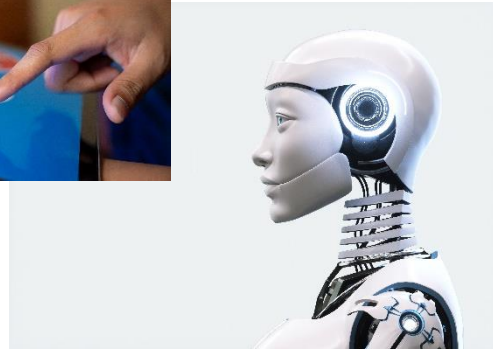
## Expertise

# IT governance      # cyber security      # fintech  
# technology risk      # business continuity      # training

## Previous Experience and Awards

- Served on various advisory panels of local and global organizations, including ISC2, DotAsia, EDB (教育局), ERB (僱員再培訓局), HKCAAVQ (香港學術及職業資歷評審局), and HKIRC
- Honoree of Asia Pacific Information Security Leadership Award from ISC2
- Received the Asia Business Continuity Award from BCI
- Received the Cyber Security Professional Award from HK Police Force
- Former Associate Director, Manulife Asia
- Former Head of Information Security and Risk Control, Fubon Bank
- Former Head of Cyber Security, Ping An OneConnect Bank
- Former Head of Information Security, Livi Bank

# IT in Every Corner of NGOs



# Current Challenges in NGOs regarding IT

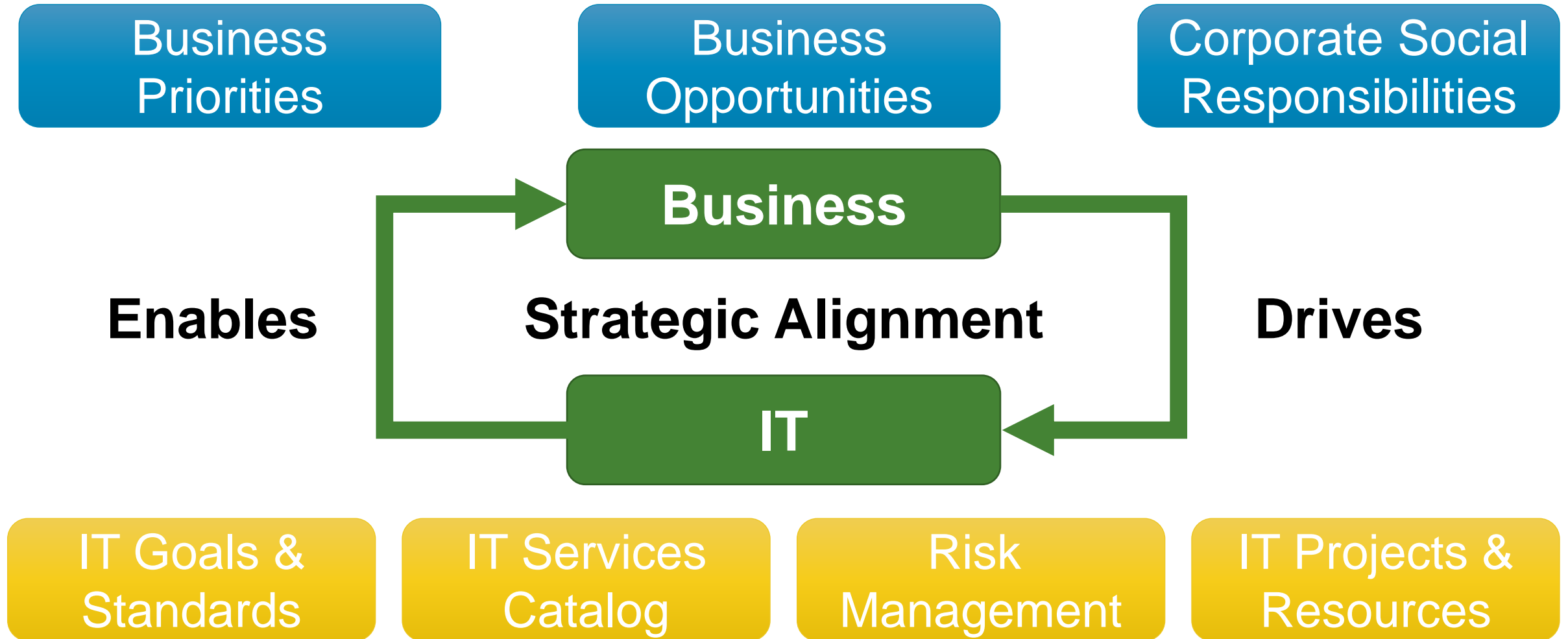
- **Limited Budgets:** Many NGOs operate with restricted budgets, making it difficult to invest in advanced IT infrastructure or professional IT staff.
- **Skill Gaps:** There's often a lack of IT expertise among NGO staff, which can lead to inefficient use of technology.
- **Data Security and Privacy:** NGOs handle sensitive information and often lack the robust systems needed to protect this data effectively.
- **Scalability Issues:** As NGOs grow, their initial IT systems may not scale efficiently, leading to operational inefficiencies.

# Governance

Aspect	NGO Governance	IT Governance
<b>Goals</b>	Aims for organizational effectiveness, efficiency, and sustainability in fulfilling the mission.	Aims to ensure IT delivers value, manages risks, and supports organizational goals.
<b>Focus Areas</b>	Includes strategic planning, program development, financial management, risk management, and compliance.	Includes IT strategy alignment, IT risk management, IT resource management, and IT performance measurement.
<b>Risk Management</b>	Manages risks impacting the NGO's mission delivery.	Manages IT-specific risks like cybersecurity threats.
<b>Accountability</b>	Establishes accountability and performance metrics for programs and operations.	Establishes accountability and performance metrics for IT services and initiatives.
<b>Compliance</b>	Ensures compliance with laws, donor requirements, and non-profit regulations.	Ensures compliance with IT-related regulations and standards (e.g., GDPR, HIPAA).
<b>Stakeholder Engagement</b>	Engages with donors, beneficiaries, and partners to align goals.	Engages with stakeholders to ensure IT services meet their needs.
<b>Frameworks and Standards</b>	Utilizes NGO-specific frameworks (e.g., NGO Code of Conduct, INGO Accountability Charter).	Utilizes IT-specific frameworks (e.g., COBIT, ITIL, ISO/IEC 38500).
<b>Decision-Making</b>	Involves Board of Directors, and governance committees.	Involves IT governance committee, CIO, and senior IT managers.



# Strategic Importance of IT Governance for NGOs



# Strategic Importance of IT Governance for NGOs

## Why IT Governance?

- **Strategic Alignment:** Ensures IT initiatives support and align with the NGO's mission and strategic objectives.
- **Enhanced Transparency and Accountability:** Provides a clear framework for decision-making and accountability in IT investments.
- **Risk Mitigation and Compliance:** Identifies and manages IT-related risks, ensuring compliance with legal and regulatory requirements.
- **Resource Optimization:** Ensures efficient use of IT resources, reducing waste and maximizing impact.

# Strategic Importance of IT Governance for NGOs

## Strategic Benefits

- **Improved decision-making capabilities.**
- **Enhanced stakeholder trust and credibility.**
- **Better resource management leading to cost savings.**



# Key Components of IT Governance for NGO

## Frameworks and Standards

- **COBIT (Control Objectives for Information and Related Technologies):** Provides a comprehensive framework for IT governance and management.
- **ITIL (Information Technology Infrastructure Library):** Focuses on aligning IT services with the needs of the business.
- **ISO/IEC 38500:** Provides guiding principles for directors on the effective, efficient, and acceptable use of IT.
- **iBDG Big Data Governance:** Provides a practical framework when handling enterprise business data.

# Key Components of IT Governance

## Core Principles

- **Strategic Alignment:** Ensures IT supports and is aligned with the NGO's strategic objectives.
- **Value Delivery:** Ensures IT delivers value by optimizing costs and proving the business value of IT.
- **Risk Management:** Identifies, assesses, and manages IT-related risks to the organization.
- **Resource Management:** Ensures optimal investment in and management of IT resources.
- **Performance Measurement:** Tracks and measures IT performance to ensure objectives are met.

# Role of Board Members in IT Governance

## Board Leadership in IT Governance

- **Vision and Strategy:** Establish a clear vision for IT's role in achieving the NGO's mission.
- **Policy Setting:** Approve IT governance policies and frameworks.
- **Resource Allocation:** Ensure adequate resources are allocated for IT initiatives.
- **Oversight and Accountability:** Monitor IT governance implementation and hold management accountable.

# Role of Board Members in IT Governance

## Board Member Actions

- **Champion IT Governance:** Advocate for the importance of IT governance within the organization.
- **Stakeholder Engagement:** Engage with key stakeholders to ensure alignment and support.
- **Performance Monitoring:** Regularly review IT performance reports and KPIs.

# Role of Senior Management in IT Governance

## Senior Management Responsibilities

- **Strategic Alignment:** Ensure IT initiatives align with organizational goals.
- **Policy Implementation:** Develop and enforce IT governance policies.
- **Resource Management:** Allocate and manage resources effectively.
- **Performance Monitoring:** Track and report on IT performance.
- **Risk Management:** Identify and mitigate IT-related risks.

# Role of Senior Management in IT Governance

## Senior Management Actions

- **Leadership and Advocacy:** Lead by example and promote IT governance principles.
- **Collaboration:** Work closely with IT staff and other departments to implement governance frameworks.
- **Communication:** Maintain open channels of communication with the board and other stakeholders.
- **Training and Development:** Ensure ongoing training and capacity building for IT staff.

# Relationship Between Board Members and Senior Management

## Strategic Collaboration

- **Communication:** Regular and transparent communication between the board and senior management.
- **Alignment:** Senior management aligns IT strategy with the strategic vision set by the board.
- **Feedback Loop:** Continuous feedback loop for policy adjustments and strategic decisions.



This Photo by Unknown Author is licensed under CC BY



# Relationship Between Board Members and Senior Management

## Roles and Responsibilities

- **Board Members:** Set strategic direction, approve policies, allocate resources, and oversee implementation.
- **Senior Management:** Implement policies, manage resources, monitor performance, and report to the board.



# Relationship Between Board Members and Senior Management

## Effective Governance Practices

- **Joint Committees:** Establish joint IT governance committees involving board members and senior management.
- **Regular Reporting:** Implement regular reporting mechanisms to keep the board informed on IT governance progress.
- **Strategic Reviews:** Conduct periodic strategic reviews to ensure IT governance remains aligned with organizational goals.

# Example Structure of Implementing IT Governance

## Strategic

Board of Directors

## Executive

IT Governance  
Committee

Project Management

## Operations

IT Advisory Group

External Advisors

Business Unit  
Representatives

Developers / Analysts

Administrators /  
Engineers

# Board Members' Roadmap from Initiation to Governance

Lifecycle Phase	Small NGOs	Medium NGOs	Large NGOs
<b>Initiation</b>	Basic IT audits, setting minimal governance policies.	Detailed IT audits, comprehensive maturity assessments, stakeholder engagement.	Extensive strategic planning, in-depth IT audits, in-depth maturity assessments, high-level stakeholder engagement.
<b>Planning</b>	Simple frameworks, basic policies.	Structured frameworks, formal policy development.	Comprehensive frameworks, detailed policy development, resource allocation.
<b>Implementation</b>	Focus on essential tech solutions, simple training.	Implement structured policies, mid-range tech solutions, formal training programs.	Deploy advanced tech solutions, comprehensive training, dedicated governance teams.
<b>Governance</b>	Informal governance structures, regular team check-ins.	Formal committees, regular performance reviews, comprehensive KPIs.	Complex governance frameworks, detailed performance tracking, continuous improvement.

# Board Members' Roadmap from Initiation to Governance

Phase	Timeframe	Steps
<b>Initiation</b>	1-3 months	Conduct a thorough <b>IT audit</b> and <b>maturity assessment</b> . Develop a strategic IT vision aligned with the NGO's mission.
<b>Planning</b>	3-6 months	Choose an appropriate <b>IT governance framework</b> (COBIT, ITIL, ISO/IEC 38500). Draft and approve IT governance policies. Allocate necessary resources, including budget and personnel.
<b>Implementation</b>	6-12 months	Implement <b>policies</b> and <b>procedures</b> ; deploy necessary <b>technology</b> . Ensure effective <b>communication</b> and <b>training</b> for staff. Set up <b>KPIs</b> and <b>KRIs</b> for ongoing performance tracking.
<b>Sustaining</b>	Ongoing	Regularly <b>review</b> and <b>update</b> IT governance practices. Foster a <b>culture</b> of continuous improvement and learning. Maintain transparency through regular performance and risk reports to the board.

# Tools and Resources for IT Governance

Category	Example Tools
<b>Governance Frameworks</b>	COBIT, ITIL, ISO/IEC 38500, iBDG
<b>Software Tools</b>	<b>GRC Platforms</b> (e.g., RSA Archer, MetricStream), <b>Project Management Tools</b> (e.g., Microsoft Project, Asana, Trello), <b>IT Service Management (ITSM) Tools</b> (e.g., ServiceNow, BMC Remedy)
<b>Additional Resources</b>	<b>Training and Certification</b> (Courses and certifications in COBIT, ITIL, ISO standards), <b>Consulting Services</b> (External expertise to guide IT governance implementation)

# Initiation Phase

Task	Details
<b>Assessing Current State</b>	Conduct an IT audit to evaluate current IT infrastructure and processes. Perform a <b>maturity assessment</b> to identify gaps and opportunities.
<b>Setting Strategic Objectives and Scope</b>	Define clear <b>IT governance goals</b> that align with the NGO's mission and strategic objectives. Prioritize initiatives based on their potential impact and feasibility.
<b>Stakeholder Engagement</b>	Identify key stakeholders, including <b>board members, senior management, IT staff</b> , and beneficiaries. Ensure buy-in and support through regular communication and involvement in decision-making processes.



# Planning Phase

Task	Details
<b>Developing an IT Governance Framework</b>	Select and customize an IT governance framework that fits your <b>NGO's size</b> and <b>needs</b> . Establish governance <b>structures</b> , such as IT steering committees and roles.
<b>Formulating Policies and Procedures</b>	Develop policies for <b>IT management</b> , <b>data protection</b> , <b>cybersecurity</b> , and <b>compliance</b> . Establish procedures for monitoring, reporting, and ensuring adherence to policies.
<b>Resource Allocation</b>	Develop a <b>budget</b> for IT governance initiatives, considering both initial and ongoing costs. Assign <b>roles</b> and <b>responsibilities</b> , ensuring that staff have the necessary skills and resources.

# Implementation Phase

Task	Details
<b>Executing the Plan</b>	Implement the developed <b>policies</b> and <b>procedures</b> . Deploy necessary technology solutions to support IT governance.
<b>Change Management</b>	Communicate changes effectively to all stakeholders. Provide training and support to ensure <b>staff understand</b> and adhere to new processes.
<b>Monitoring and Reporting</b>	Establish <b>Key Performance Indicators</b> (KPIs) to track IT governance effectiveness. Regularly <b>report progress</b> to stakeholders, using data-driven insights.

# Sustaining Phase

Task	Details
<b>Review and Update</b>	Regularly review and update <b>IT governance practices</b> to ensure they remain relevant and effective.
<b>Continuous Improvement</b>	Foster a <b>culture</b> of continuous improvement and learning within the organization.
<b>Performance Monitoring</b>	Continuously monitor IT performance and <b>risk indicators</b> to ensure ongoing alignment with organizational goals.
<b>Stakeholder Engagement</b>	Maintain <b>regular communication</b> with all stakeholders to ensure ongoing support and alignment.
<b>Compliance and Audit</b>	Conduct regular compliance checks and audits to ensure adherence to policies and <b>regulatory requirements</b> .

# IT Governance Documentation

Document Type	Description
<b>IT Governance Framework</b>	A comprehensive document outlining the overall IT governance structure and principles.
<b>IT Policies</b>	Specific guidelines and rules governing IT operations and use within the organization.
<b>IT Procedures</b>	Detailed instructions on how to carry out specific IT tasks and processes.
<b>IT Strategy Document</b>	A strategic plan aligning IT initiatives with organizational goals and objectives.
<b>Risk Management Plan</b>	A document identifying potential IT risks and outlining mitigation strategies.
<b>Compliance Reports</b>	Regular reports ensuring adherence to regulatory and policy requirements.
<b>Performance Reports</b>	Reports tracking the performance of IT services and governance.

# Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs)

KPIs for IT Governance	KRIs for IT Governance
<b>System Uptime:</b> Measure the availability and reliability of IT systems.	<b>Incident Response Time:</b> Time taken to respond to and resolve IT incidents.
<b>Compliance Rates:</b> Track adherence to policies and regulatory requirements.	<b>Security Breaches:</b> Number and severity of security breaches.
<b>User Satisfaction:</b> Assess user satisfaction with IT services and support.	<b>Data Accuracy:</b> Accuracy and integrity of data managed by IT systems.
<b>Project Delivery:</b> Monitor the timely and within-budget delivery of IT projects.	<b>Resource Utilization:</b> Efficiency in the use of IT resources.

# Measuring Success

<b>Key Performance Indicators (KPIs)</b>	<ul style="list-style-type: none"><li>• <b>Metrics for assessing IT governance effectiveness</b>, such as system uptime, compliance rates, user satisfaction, and project delivery.</li></ul>
<b>Continuous Improvement</b>	<ul style="list-style-type: none"><li>• <b>Regular reviews and updates</b> to the governance framework based on performance data.</li><li>• <b>Incorporating feedback</b> from stakeholders and lessons learned into future iterations.</li></ul>



# Challenges and Solutions

Common Challenges	Strategies to Overcome Challenges
<b>Resistance to change among staff and stakeholders.</b>	<b>Building a Culture of Continuous Improvement:</b> Encourage a mindset of ongoing learning and adaptation.
<b>Limited resources, including budget and expertise.</b>	<b>Leveraging External Expertise and Partnerships:</b> Utilize consultants, partnerships with tech firms, and industry best practices.
<b>Ensuring continuous improvement and adaptation.</b>	<b>Regular Training and Capacity Building:</b> Invest in ongoing training programs to enhance staff skills and knowledge.



# Conclusion

# Recap

NGO Size	Recommendations
Small	May start with <b>basic</b> frameworks and gradually build complexity.
Medium	Can implement more <b>structured</b> processes and dedicated IT roles.
Large	Should consider <b>comprehensive</b> frameworks and dedicated IT governance teams.



# Q & A

Contact: [frank.chow@pisa.org.hk](mailto:frank.chow@pisa.org.hk)