43

IT GOVERNANCE

Tony Fish

“Finance for the non-finance leader” is the framing for this chapter and I am therefore presenting this as “IT governance questions for non-IT leaders.” It will guide those who are willing, keen, and supportive of their peers in the complex decisions that IT demands, through questions and not judgement. IT governance is one of the latest additions to the corporate governance agenda and is not as mature as finance or legal. In short, IT governance enables an organisation to:

- sustain and extend the organisation’s strategies and objectives;
- demonstrate that IT is aligned with delivering broader business goals;
- meet all relevant legal and regulatory obligations, including compliance with public listing rules or requirements; and
- assure stakeholders they can have confidence, faith, and trust in an organisation’s IT services.

I have left off a link to improving return on investment, financial returns, and efficiency as these measures tend to limit the scope of IT governance to a finance dimension, ignoring the human cost.

The media continually promotes the outcomes from errors in IT oversight as data leakage, outage, and cyberattacks. Each story becomes a new case study, with highly sophisticated attacks being defensible only after the event. IT governance remains itself fixed in a cycle of identifying the problem after the event, learning fast how to adapt, and finding whom to blame for the unimagined event. IT governance lacks the prestige of financial governance and audit, and the budget of legal and regulatory compliance, yet without our IT systems, companies are simply unable to function. As IT has become increasingly sophisticated and specialised, it has often left one person both recommending and making the decisions that a board should agree together. Since the level of detail, technical language, and implications affecting and effecting every aspect of the business is so complex, many leaders find they are unable to operate at the level of detail needed to add value and in such a way that it does not result in frustrating the decision-making processes or a loss of respect. Sometimes it is easier to talk about anything else other than IT. This chapter focuses on how to support those who are accountable for IT governance in their role. IT governance concerns layers of increasing complexity and interdependency. IT governance embraces at one end the integration of discrete hardware, software, and embedded systems and solutions. At the other end, IT governance encompasses how the internal systems depend on third-party solutions and eco-system integration, which has a dependency on the company's own internal resources; those in the eco-system and the interface to and with the customer. Within the simple scope, IT governance demands that:

- a leadership team can verify, test, and trust all third-party suppliers, their systems, their third-party supplier, and all processes, to at least the same level you demand of yourselves continuously;
- other leaders in your eco-system believe you are able to deliver the same verification, test, and trust level to them;
- you can understand the limitations and biases of your internal development and integration and accept, manage, and communicate the risks;
- you understand your peers and staff, their motivations; contexts; and behaviours; and
- the data that you have, and use does not create bias, prejudice, or misleading recommendations.

IT governance possibly demands the widest variety of skills outside of the core disciplines (finance, legal, marketing, operations) and includes: anthropology, sociology, behavioural sciences, economics, moral philosophy, coding, computer science, data science, power planning, physics, building design, and IT. To explore the diverse skills requirements by example, we should ask, “what is your password policy?” It is perfectly possible to make a system 100% secure; however, it will be unusable. There are necessary compromises between usability and security that every board member needs to agree on, understand, and appreciate sincerely. Setting a password management policy too high means that users will write them down; a policy of updating a password too often will lead to bypass, where a user will forward to a personal useable off-system account, or too weak a system, and passwords are easily broken. Taking away your employees’ agency with draconian policies means you undermine your core values. Giving employees too much control leads to security breaches. Monitoring staff use of IT creates distrust. IT governance needs a leadership team who can debate these complicated issues without becoming righteous and argumentative. IT always becomes personal and is based on our own preferences. As a second example, “Which design philosophy and policy does the company follow?” Design for security, design for use, design for privacy, or design for the customer first? In reality, probably all four are valid in different areas, but what gaps are created, and where and what are the compromises and risks from different ideals?

IT governance is about

- creating policies that align to, and with, core values;
- balancing risks, understanding the compromises, and being able to explain them;
- aligning design philosophies across the company operating functions;
- delegating what to whom and why;
- continually learning, refining, and updating; and
- responding to a crisis.

IT governance is not about

- agility, which technology, which platform, or whose software;

- security breaches, hacking, permissions, cyberattacks, or root passwords;
- cost allocation, budget controls, and that scale is very hard;
- humans being in the loop, even though this will always remain an IT governance nemesis;
- compliance, procedures, processes, and methodologies;
- development tools, controls, or outsourcing; or
- your personal problems with login, software choices, or phone providers, however important you feel they are.

Questions to support full board engagement for better IT governance

Skills

- What IT skills do we have at this table?
- How do we assess sufficiency in skills?
- Are there any gaps?
- Are we focused on IT governance or IT compliance, and do we know the difference?
- Do we have the skills/resources to cope with every possible IT crisis?
- Will our response to a crisis be good enough?
- Are we able to explain automated decisions made by our IT system?

Alignment

- How are we sure that our IT can deliver our vision and strategy?
- How sure are we that our IT will deliver our vision and strategy?

Policy

- What IT governance/compliance policies do we have?
- Do our IT policies align to and with core values?
- What is our risk profile for IT?
- Is our risk profile for IT aligned to other risk profiles?
- How are we checking that we are genuinely measuring and balancing the risks?

- Who has delegation authority for what IT-related decisions and why?
- How are we understanding and communicating the compromises?
- Is our communication good enough on compromises to stakeholders?
- Do we use our controlled IT environment/platform for everything, or do we depend on something outside of the system (for example, spreadsheets) for control, management, and oversight?
- Is our policy and approach to IT sustainable?

Design

- What design and control philosophies do we have/use?
- What design/control frameworks are we using and why?
- How do we know our philosophies and framework are aligned?
- Do we know what bias is in our philosophies and framework and what the implications or unintended consequences are?
- How do we know we are continually learning, refining, and updating to improve?
- How do we decide on what IT support, tools, and services we use, service, or provide?
- What level of automation do we have, and are we aiming for?
- Who tests the testers, who controls to controls, who questions the alignments?

Data

- What is our data policy and how many do we have?
- What is our data philosophy?
- Do our data philosophy, privacy, and controls align with our values?
- Do we know what bias is in our data, and what the implications are?
- What assurance do we have that information and analysis presented for decisions is true and linked to a source for future reference and checking?