A Little Bit of History Repeating Itself—Nolan’s Stages Theory and the Modern IS Auditor

One of the key aspects of an information systems (IS) audit is ascertaining the maturity of the technologies in use within an organisation or department. In reality, some areas of the business’s use of IT are more mature than others, and this is particularly true of companies that have undergone recent mergers or acquisitions.

The Stages of Growth Model for IT systems was developed by Richard L. Nolan in the 1970s. Though modified over time and subject to criticism in some quarters, it is still used to discuss the growth of IT within an organisation and is used by many companies and consultants to categorise the evolution of what was originally known as data processing departments.

In this article, the six (originally four) stages are discussed, along with their direct relevance to the IS auditor. Nolan’s theory can provide a useful framework for an audit engagement, especially for the less-experienced auditor who may not have had extensive exposure to a wide range of IT organisational systems.

The Creation and Evolution of Nolan’s Theory

When Richard L. Nolan first published his theory in 1973, there was no such thing as the microcomputer. The smallest configuration available was a minicomputer, such as the DEC PDP-7. Mainframe computers were the norm, dominating large air-conditioned data centres. Expensive to buy and expensive to run, these computers mostly operated in batch mode, with jobs submitted to be run overnight. While some real-time systems were available, the expensive communication links required made these viable only for particular niche areas, such as airlines and banking.

Within this context, however, Nolan provided a vision for what could happen within an organisation if the costs of data processing were reduced. Prophetic in his approach, many of his predictions came true—first for large corporations and then for much smaller businesses.

The Stages of Growth Model has not remained static. In 1979 Nolan added two further stages as the model tried to keep up with the dramatic developments in technology at the time.

Over time there have been criticisms of the theory, including the assumption that an organisation leaps from one state to another and the perception that an organisation must always strive to be benchmarked against the higher stages (i.e., data administration and maturity). Furthermore, other models have been developed that build on the work of Nolan, but attempt to alleviate what are seen by some as shortcomings. For example and perhaps in a nod to controlled risk self-assessment, the Data Management Practice Maturity Model is an approach that closely matches the original thinking of Nolan, but the theory is discussed in the context of 2012 rather than the 1970s.

Stage I—Initiation

This stage is concerned with the first introduction of technology into an organisation. While it may be hard to conceive for those who work in corporate IT, many small businesses thrive without a large IT infrastructure—consider the number of small businesses that need only a mobile phone and diary to complete their work.

The initiation stage in an organisation was identified by Nolan as being the point at which an organisation first purchases technology. In the 1970s, this was inevitably a minicomputer; now, with laptop costs tumbling and the use of smartphones for many day-to-day business functions, this starting point is much harder to determine. Personal devices are frequently being repurposed for the needs of the business. In this way, the starting point can very easily become blurred, and the increasing reliance upon IT goes unnoticed. For many small businesses, information assurance may not be a major concern, but as everyone who has lost a phone is aware, an effective backup (even of phone contacts/diary entries) is critical.
Within larger organisations, a base level of IT infrastructure is now certain to be found. However, stage I can also be applied to any emerging technologies. It is highly unusual for an innovative technology to be introduced by policy. Rather, the introduction is usually by small initial successes in pockets of the organisation’s employees acting individually. For example, consider the initial deployment of smartphones within organisations. Originally, these were purchased by the individuals who saw the potential of these devices for their personal productivity, but then expected to be able to connect these to the corporate network—frequently with little concern for the security issues surrounding mobile devices.

The internal IS auditor has a role in identifying these early accesses. They can identify best practice and suggest adoption by other areas. While this may be a good way of disseminating information, it may also inadvertently lead to many of the problems discussed in stage II.

Conversely, internal audit could identify new technologies and work with the organisation to promote the development of regulation and control. If this happens in parallel with the adoption of the technology rather than after implementation, the difficulties of stage II could be greatly reduced.

STAGE II—CONTAGION
This is a critical stage of IT growth and is identified by the proliferation of systems within the organisation. Different technologies may compete to be dominant within the organisation, e.g., the decades-old Mac vs. PC dispute. Today debates ensue, for example, about whether information itself must be held within the organisation or whether cloud computing and storage are appropriate.

In the early days of data processing, vendors were keen to ensure that their customers were ‘locked in’ to their systems and data file formats. Even agreements on the sequence for alphanumeric sorting and storage of data were proprietary, with ASCII (DEC) and EBCDIC formats used by ICL and IBM. Many of us have experienced the frustrations of different data formats, but nowadays data can often be converted between systems. Extensible Markup Language (XML) schemas and improved data quality standards have helped significantly within this area.

The danger of this stage stems from lack of control, spiralling costs, and errors that arise through the need for manual data input to transfer information among systems or incorrect controls when transferring data between systems. This growth frequently occurs at the same time as the company expands. IT can be a facilitator of growth and, at the same time, can become a victim of its own success.

Again, using the smartphone as an example, after seeing early adopters benefit from their use, more individuals and departments adopted them, but still not within a corporate framework. Hence, there has been a proliferation of models and operating systems, leading to incompatibilities and additional support demands.

The role of internal audit at this stage can be that of a sheepdog or cattle herder, providing assurance that numerous disparate systems have appropriate controls. Frequently, the internal IS auditor is uniquely placed to recognise where synergies may be possible due to their wider organisational scope. This may be particularly relevant for integrated audits that ‘combine both financial and operational audit steps’. By identifying these synergies, the internal IS auditor can assist the organisation’s progress through this chaotic stage and into stage III. If an organisation fails to do this, there are significant risks for the long-term success of both the IT within an organisation and the organisation itself.

STAGE III—CONTROL
From a management perspective, having seen the proliferation of systems present in stage II (and their usefulness), a need to introduce controls can be identified, not only on the number of systems, but also on the budgets associated with these systems. The need for this control may possibly be recognised through an internal audit, identifying that despite the early successes of stage I and the mass (but uncontrolled) proliferation of stage II, the technology is now becoming a behemoth. For example, a disaster recovery or business continuity incident may occur, which demonstrates an intolerable risk to the organisation of simply having too many systems to attempt to recover in a limited time. Recovery time objectives (RTOs) and recovery point objectives (RPOs) become impossible to achieve, as a lack of standardisation of procedures means that recovery becomes overly complex and the interruption window becomes too large for the business to tolerate.
On initial inspection, it may be considered that this stage is where internal audit should enter the process. This is not the case; internal audit may have already proposed controls that now have to be formalised and, more important, applied and monitored. If an organisation does not enforce control (with the assurance of internal audit), not only will it not progress, but it can easily slip back to stage II, as individual areas once again implement disparate IT solutions without corporate authority.

Continuing the smartphone example, at this stage internal IS auditors should have identified the issues associated with the multitude of different devices in use. They may well recommend control over the devices’ use or suggest an organisational purchase policy. These recommendations should not only be directed at the actual device, but also at its use, thereby moving the technology onwards to stage IV.

STAGE IV—INTEGRATION

After getting the systems under control in the previous stage, the organisation may wish to further develop the maturity of the IT systems and begin to consolidate the systems and the data that underlie the core functionality of the organisation. It is at this point that the organisation-wide experience of the internal IS auditor begins to come to the forefront in an advisory role rather than in monitoring and control, further developing this role in stage V. It may be that the internal IS auditor is the only individual who has the holistic view of all levels of the organisation, particularly if a decentralised management structure (such as a matrix structure) exists.

Nowadays, integration inevitably leads to the consideration of enterprise resource planning (ERP) systems. The market for these has grown rapidly in the last 20 years, and many vendors offer services for small and medium-sized enterprises (SMEs). It is feasible, therefore, that an organisation that experiences brisk growth may be able to leapfrog from stage I to stage IV without the plethora of systems associated with stages II and III, and with a tighter control of costs, which is particularly necessary in SMEs.

Internal audit may be tempted to rely solely upon standard reports generated by the ERP systems themselves. It is essential that the auditor’s independence, including independence from the systems themselves, is maintained. Internal IS auditors now have the potential to access vast repositories of data, this makes it essential that they consider the use of automated tools (e.g., computer-assisted audit techniques (CAATs)) to analyse the data available. The difficulty may now reside in identifying and obtaining the data sets necessary and deriving the tests to be applied upon them, rather than in assuring the relevance and accuracy of the data.

STAGE V—DATA ADMINISTRATION

The data administration stage is less of a technological shift, and more of a philosophical culture change within the organisation. The issue of data ownership (DO) is at the forefront at this stage. Rather than the data being owned by the IT department (or outsourced provider), the users take ownership of the data. Internal audit can help define the concept of DO within the specific context of the organisation and the allocation of a responsible person for the ownership, access and protection of the information asset.

The data within the ERP system can be opened up to a wider user base, and the organisation needs confidence (through role-based access) that the individuals know how to use the information to which they are granted access.

By this stage, the role of the internal IS auditor has shifted from that of an IT policeman to that of ensuring data and information resources are being used effectively and correctly by an organisation, complying with both external regulatory frameworks and best practice.

Continuing the mobile device example, there is a need for the internal IS auditor to ensure that individual users appreciate the issues of data being removed from the organisation and the importance of synchronisation of data, thereby ensuring integrity across the organisation. The emergence of cloud storage may help at this level, allowing clear demarcation of the data custodian, the data owner and the data user—regardless of their location and access device.

STAGE VI—MATURITY

The final stage identified by Nolan is achieved when all systems within an organisation are developed to their optimum state and can be said to have reached both a technological maturity and system stability commensurate with the business’s reliance upon those systems. While external benchmarking can provide some level of reassurance, it is also possible for the organisation to become complacent, in which case strategic drift could ensue. Therefore, the role of the internal IS auditor is to ensure that complacency is avoided or eliminated.

In reality, the pace of technological and business change means that systems need to be constantly developed. This could be to maintain competitive advantage, enter a new market or take advantage of (for instance) falling IT architecture costs.
Hence, although seemingly impossible to achieve, the IT maturity stage is something to which the organisation should continually strive, and the charter for the IT steering committee could identify the realisation of this stage as an ongoing and organic strategic objective.

**CONCLUSION**

As demonstrated, IT technologies undergo a series of incremental stages. At each stage internal and external factors will drive change forward, and overall the role of the internal IS auditor is to ensure that this occurs in a controlled manner. By associating an organisation or department with a particular stage of the model, an auditor can identify the necessary actions to drive the technology onto the higher levels, tending toward maturity. Therefore, Nolan’s model offers a useful tool to the auditor when discussing long-term strategic planning as part of an institution’s IT audit function, ensuring that senior management recognise the risk of uncontrolled IT adoption and seize the opportunities of moving forward with a coherent and structured IT strategy.

**ENDNOTES**


