What do the results of an Information Governance Maturity Assessment mean?

Information governance principle	What does it mean if you scored below 3?
Accountability Information governance is a priority for the organisation, and senior managers are responsible for it (and they know it!). Clear roles and responsibilities concerning information governance have been assigned throughout the organisation. Policies, standards and procedures have been put in place to ensure that the level of information governance can be audited.	How an organisation ranks on the accountability principle, indicates whether information governance is a priority. We briefly touched on this in lesson #1, when we spoke about getting buy-in for POPIA compliance. Becoming POPIA compliant without looking at how all information is governed is not only difficult, it's also dangerous. It is entirely possible that the organisation is faced with more significant risks to other categories of information (e.g. your intellectual property). The organisation should consider starting an information governance project instead of a POPIA project. Compliance with the POPIA can be one phase of the information governance project.
Standardisation There is an agreed way of working at the organisation. Business processes and activities are well-defined and documented in an open and verifiable way. The documentation must be available to employees and third parties who play a role in the processes and activities.	When you evaluate POPIA compliance, you are evaluating policies and procedures. If there are none, or they are poorly implemented, you have nothing to evaluate. So, if your organisation does not have a documented way of working, POPIA compliance will not be possible. The organisation should consider starting a corporate governance project instead of a POPIA project.
Confidentiality Confidential and personal information must be protected from unauthorised destruction, modification or access.	Confidentiality is one leg of the CIA triad, which is used in information security management. It is also a requirement of the POPIA. If an organisation does not proactively protect the confidentiality of its information, it should consider starting an information security management project, before it embarks on a POPIA project.
Integrity The right processes are in place to guarantee that information is comprehensible, clear, consistent and reliable.	Integrity is one leg of the CIA triad, which is used in information security management. It is also a requirement of the POPIA (in respect of personal information). If an organisation does not have processes to ensure the integrity of its information, it should consider starting an information security management project, before it starts a POPIA project.
Availability Policies and business continuity plans are in place to ensure that information,	Availability is one leg of the CIA triad, which is used in information security management. It is also a POPIA requirement (in respect of personal information). On

Information governance principle	What does it mean if you scored below 3?
and the infrastructure the organisation needs to manage and use that information, is available to the appropriate people at the appropriate time.	organisation's business continuity plans must include plans to ensure the availability of information and information infrastructure. If the business does not do business continuity planning, or if information assets are not included in its business continuity planning, the organisation should consider a business continuity management project, before it starts a POPIA project.
Compliance The organisation has structures, policies and processes in place to ensure that the organisation complies with all legislation, supervisory requirements created by Regulators, codes of conduct and other rules, codes of conduct or standards that apply to the organisation. There is a continuous process through which compliance risks are identified, analysed (rated according to their impact and likelihood), addressed and monitored. This forms part of the organisation's enterprise risk management process.	Almost all types of information are regulated in some way or another. The introduction of the POPIA creates significant regulatory compliance risk. If an organisation does not have a reasonably mature compliance management function, POPIA compliance is impossible. Also, if the organisation is not currently managing regulatory risk, there are likely areas of non-compliance with other legislation that exposes the organisation to bigger riks than the POPIA. The organisation should consider doing a compliance management project before it starts a POPIA project. If the organisation does not manage any form of risk, it should consider undertaking an enterprise risk management project.
Records management The organisation manages records (information maintained as evidence of actions or decisions). The organisation only retains information for as long as it is required by legal, regulatory, fiscal, operational and historical requirements.	The organisation should consider doing a records management project before it starts a POPIA project.
Change management and empowerment The organisation pro-actively manages change by assessing the impact of events and strategies on its policies, processes, infrastructure and people. The organisation's employees are empowered through training and skills development to work responsibly with information and to protect it.	The POPIA is not an IT problem; it is a people problem. See lessons #7 and #9. The majority of information risks are either caused or exacerbated by human error. If the organisation does not have a strong culture of change management and empowering people through training and skills development, POPIA compliance will be tough to achieve and maintain. The organisation should consider strengthening its change management function before starting a POPIA project.