Intellectual capital

What it is

Organisational, knowledge-based intangibles, including:

– intellectual property, such as patents, copyrights, software, rights and licences
– 'organisational capital' such as tacit knowledge, systems, procedures and protocols.

2. Intellectual capital

For over **70 years**, Sentinel has built up a vast store of **knowledge**, insights and systems that enable the **Fund** to **create value** for members, pensioners, beneficiaries and society. Our long proven **expertise** and **capability** underpin Sentinel's reputation for a consistently superior offering and **cost-effective** services.

How Sentinel manages intellectual capital

Innovation

Sentinel has long pursued a policy of continually reviewing and improving its products where feasible. We have evolved into a multi-industry retirement fund by redesigning Sentinel's structure and products for a broader range of employers and members, while engaging with potential clients outside of the mining sector.

Administrative strengths and competencies

— Daily unitisation
— Member account maintenance
— Daily compliance
— Regulatory reporting.

Technology

The Fund deploys sophisticated information technology (IT) to serve the needs of stakeholders accurately and cost-effectively. We view IT as a critical enabler for business, therefore partner with world leading software development houses. Sentinel ensures that all systems are operated within set parameters and that policies are in place to protect, archive and secure data while privacy is maintained. Our comprehensive disaster recovery procedure incorporates full back-up of all electronic files daily to an off-site location. In the event of a disruption in business, the Fund has secured two disaster recovery sites that will ensure the swift restoration of operations.

Performance

KPI: Introduction of new products and services and ensuring these adhere to legislation and participant demands.
Objective: To ensure that, to the extent allowed by our rules and legislation, our products and services are responsive to participant requirements.

Outcomes – 2017
Risk benefit product offering

The search for a holistic risk benefit product solution has advanced during this year. As an interim measure until a comprehensive solution is in place, employers who exercise the option to opt out of the Fund's risk benefit product can request Sentinel to accept their preferred death cover insurance policy as a tax-approved, Sentinel-owned policy.

Retirement reform:

National Treasury published three regulations during 2017 as part of retirement reform plans, ie:
— Regulation 37: Default Investment Portfolios
— Regulation 38: Default Preservation and Portability Strategy
— Regulation 39: Default Annuity Strategy

The Fund's rules already comply with most of the regulations and will be ready for implementation when these become effective.

KPI: Technology as critical enabler for business
Objective: Ensuring that appropriate technology and software solutions are added where a need has been identified.

Outcomes – 2017

New software or applications were not required in this period.

Objective: Ensuring that all application software releases are updated to support new functionality, while maintaining IT equipment to ensure reliable 24/7 performance.

Outcomes – 2017

All software has been updated to latest releases.

Objective: Ensuring system productivity levels support the ongoing provision of a superior client service experience.

Outcomes – 2017

Software is used to monitor productivity levels of both hardware and operating systems on a 24/7 basis. Included in the monitoring process is transaction level monitoring as well as business process management level monitoring. Business intelligence software is used as a management tool to continuously improve productivity levels.

KPI: Data security, quality and protection
Objective: Ensuring data remains secure and protected.

Outcomes – 2017

As the technology adoption rate increases worldwide and makes its way into every facet of routine life, cybercrime has become one of the leading risks facing organisations and individuals alike. As a custodian of member data, Sentinel understands the potential harm to individuals in the event of data breaches through system hacking or other forms of cybercrime.

Although insurance policies are available to compensate organisations and individuals for damages sustained as a consequence of cybercrimes, Sentinel has taken the approach that 'prevention is better than cure'. Sentinel is extremely serious about keeping member data secure. To achieve this, the Fund has invested time and money into upgrading all the data protection layers in accordance with global best practices. These will be re-evaluated regularly.

Sentinel understands that even best practices cannot guarantee 100% safety and has taken out cybercrime insurance to minimise financial damages should all defences get breached.

Much attention was devoted to ensuring that Sentinel's systems can deal effectively with cyber attacks. Computer security awareness dashboards were installed to raise staff awareness regarding password security, phishing and other cyber security warnings. Sentinel can report that all instances of attempted cyber attack in this financial year were effectively warded off.

Objective: Ensuring that business decision-making is based on accurate data.

Outcomes – 2017

Through the use of business intelligence software, management can now perform data quality and integrity checks. Data cleansing and sanitisation projects are implemented to remedy areas of weakness in the data.

Objective: Ensuring the high availability of network and systems while simultaneously protecting data through best practice backup procedures.

Continuous maintenance, improving and testing of Sentinel's fully fledged disaster recovery plan to ensure that the Fund can resume business within hours after a major disruption or disastrous event.

Outcomes – 2017

The recovery and restoration of the Fund's total technology architecture was tested and passed successfully.