

2011 / 2012

DCS PRIORITY FOCUS AREAS

Towards a Secured and Functional DCS Digital Nervous System

Presentation to Portfolio
Committee

DJ Moji

19 October 2011

- Reduced overcrowding and improved conditions of detention
- Improved state of DCS facilities
- Effective leadership and management
- Professionalised Correctional Services and Corrections Academy
- Partnerships for delivery of rehabilitation
- Standardisation and management of DCS performance indicators
- Efficient and effective spending of public money
- Effective people management and appropriate organisational structure
- Appropriate Correctional Services image and branding
- Common understanding of the core business of the department
- Effective Correctional Sentence Plans
- Effective Security
- Involvement of offenders in corrections programmes
- Focus on development and care programmes
- Protection of human rights of inmates, particularly of special categories of inmates

**A year of action to ensure all people in
South Africa are and feel safe**



correctional services

Department:
Correctional Services
REPUBLIC OF SOUTH AFRICA



Strategic

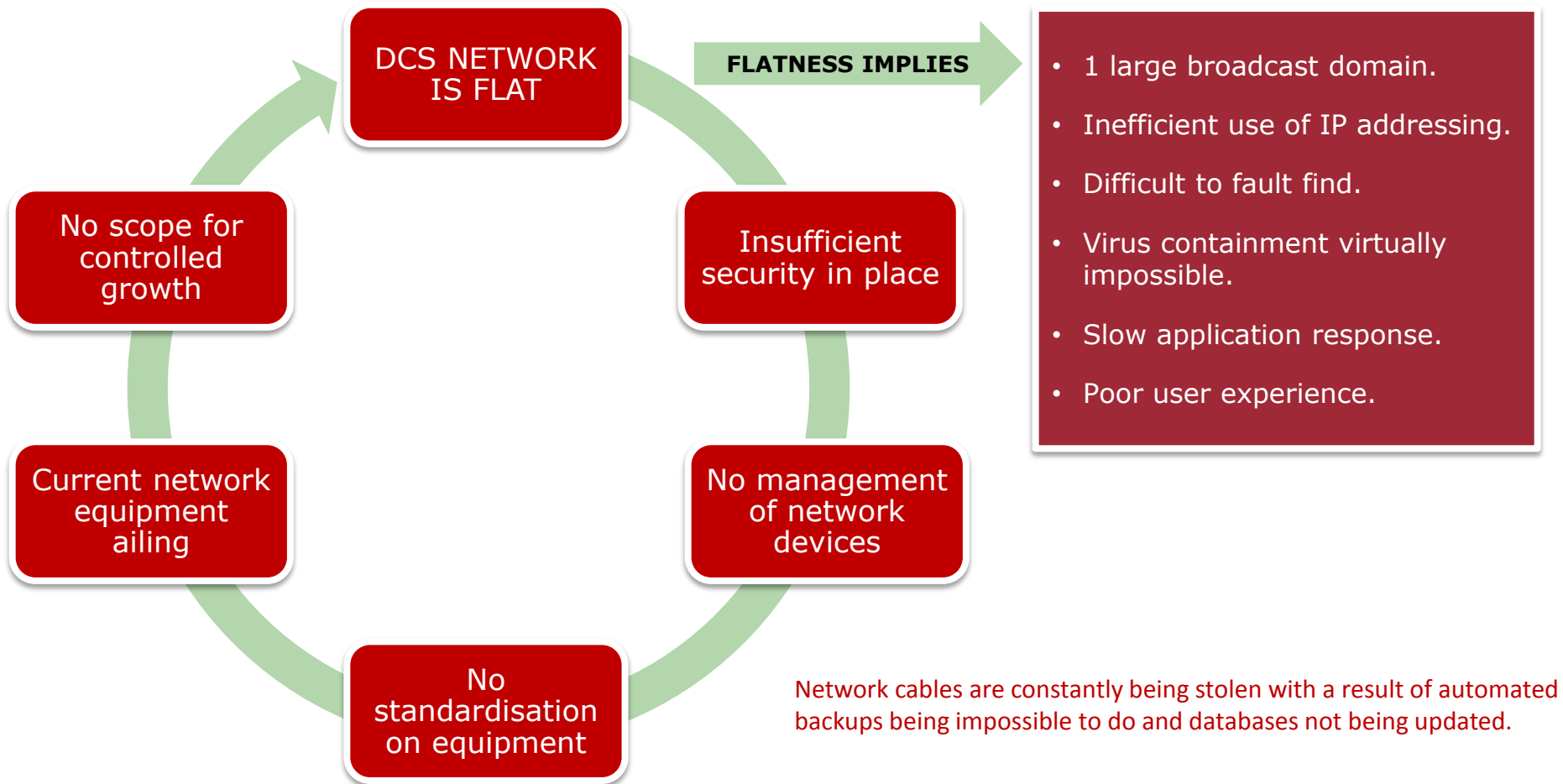
- No effective governance and accountability for IT applications.
- Multiple security technology stakeholders at centres.
- The infrastructure is not properly planned, deployed and managed.
- No effective management and strategic reporting.
- Lack of application integration and silo development.
- No centralised policy and therefore no adherence to standards.
- No user application tools for management reporting and data interrogation.
- Lack of IT service management across the entire organisation.

Operational

- Data islands with different types of data.
- Data integrity lacking.
- Reliance on rickety relationships with service providers.
- Inefficient business processes.
- Excessive manual intervention and handoffs.
- Lack of training on Microsoft Windows, Office and IT applications in general.
- IT human resources not properly coordinated for the good of the entire department.



The DCS network is old and has not been upgraded for the current load ...





Approximately 800 servers across the Department are very old and need to be replaced.

There are about 360 firewall servers across the country and 200 of them are not operational, meaning that the entire network of the Department is open to sabotage.

The Disaster Recovery Plan that was initially reported to the National Commissioner to be on track is actually not in place.

Most of the server rooms across the country do not meet safety and security standards. Some IP cameras in server rooms don't have maintenance contracts.

About R37 million was spent on automated backup equipment and most of it does not work due to the server rooms not being suitable for housing such delicate machines.

The email environment is highly unstable and shuts down regularly due to the Department's infrastructure and SITA's poor Wide Area Network (WAN) services.

Some consultants had a "Basic Infrastructure Business Case" for replacing the old servers at a cost of more than R3.2 billion over three years. A separate exercise was done and showed savings of about R2 billion or more on what was originally proposed



Head Office at Pretoria has about eighteen IT officials comprised of one director of systems development, four deputy directors and the rest are extremely junior officials and mostly administrators.

The four deputy directors have limited experience on IT technical matters and rely mostly on consultants.

The director: Systems Development and the Deputy Director: Information Security have been suspended. Deputy Director: Networks has been dismissed and a case of child pornography has been opened against him with the Police.

It was reported that there could be about 200 network controllers across the country who are mostly officials without IT experience.

At the beginning of the financial year, Head Office had about 83 (eighty three) IT consultants and another 50 (fifty) consultants doing systems development on a special project

Some consultants were found by the Auditor General to have been involved in contravention procurement processes.



We are
here

Back to Basics

- Infrastructure Renewal
- Develop IT Skills
- Structural improvements
- Secure IT system

IT is efficient

Business Support

- Business process automation (Core Systems)
- Business intelligence
- Integrated security management

IT is an enabler

Strategic Partner

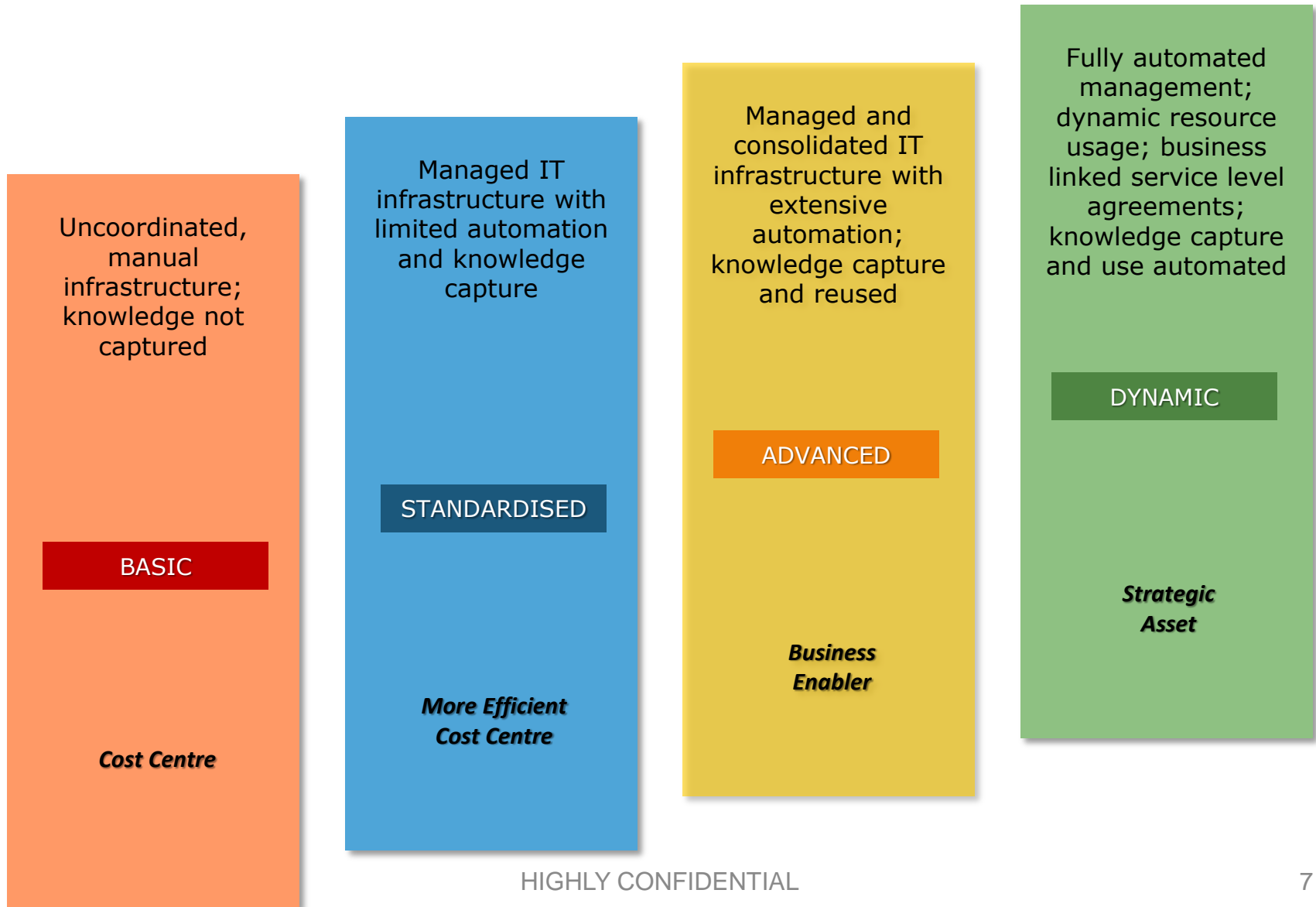
- Forecasting
- Offender Management
- Cybercrime Intervention
- IT programs for Offender rehabilitation

IT is a strategic asset

Key implication: Stop all application development on RDOMS and ad hoc requests.

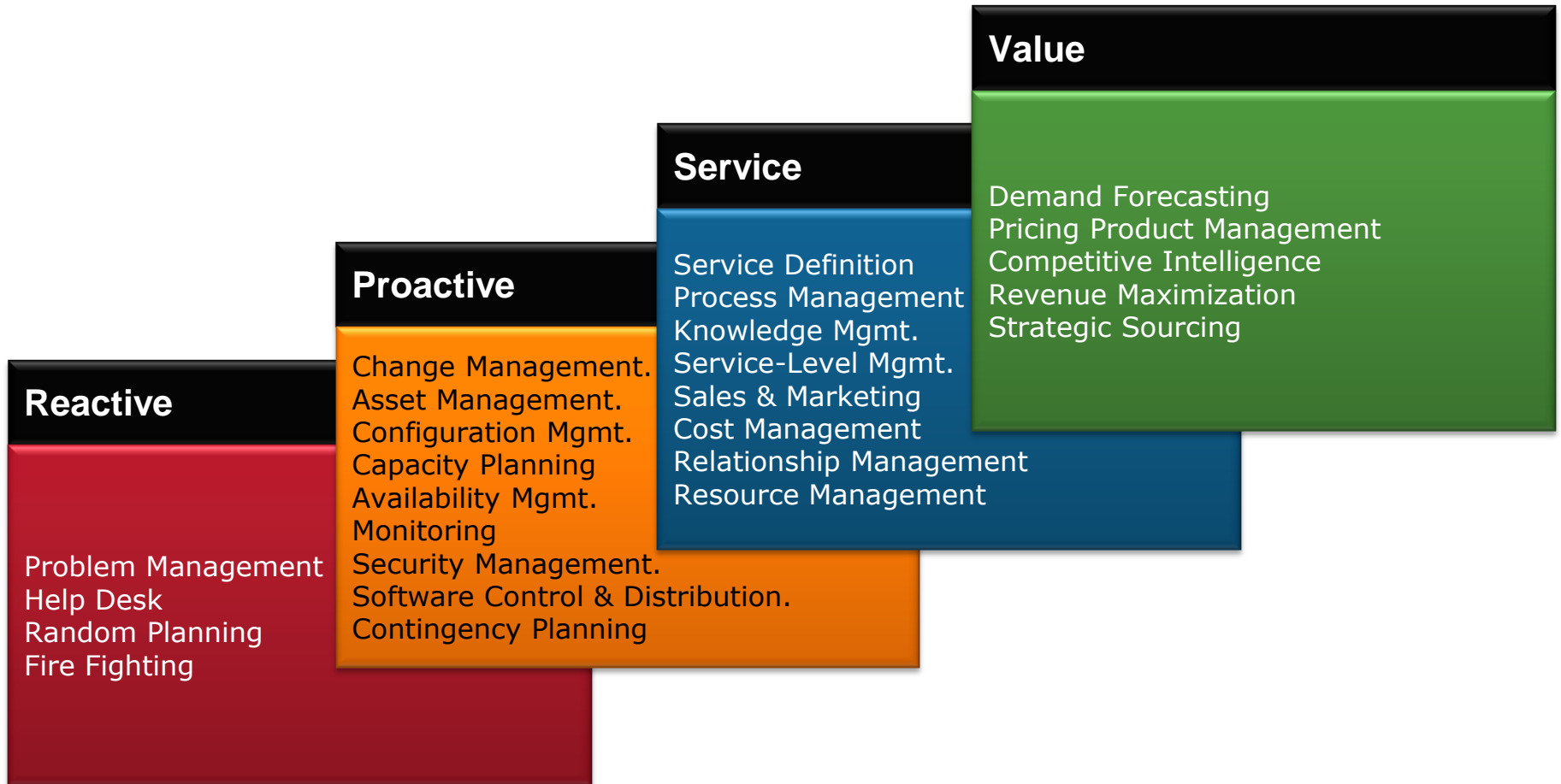


DCS IT needs to start to ramp it up in order to improve services ...



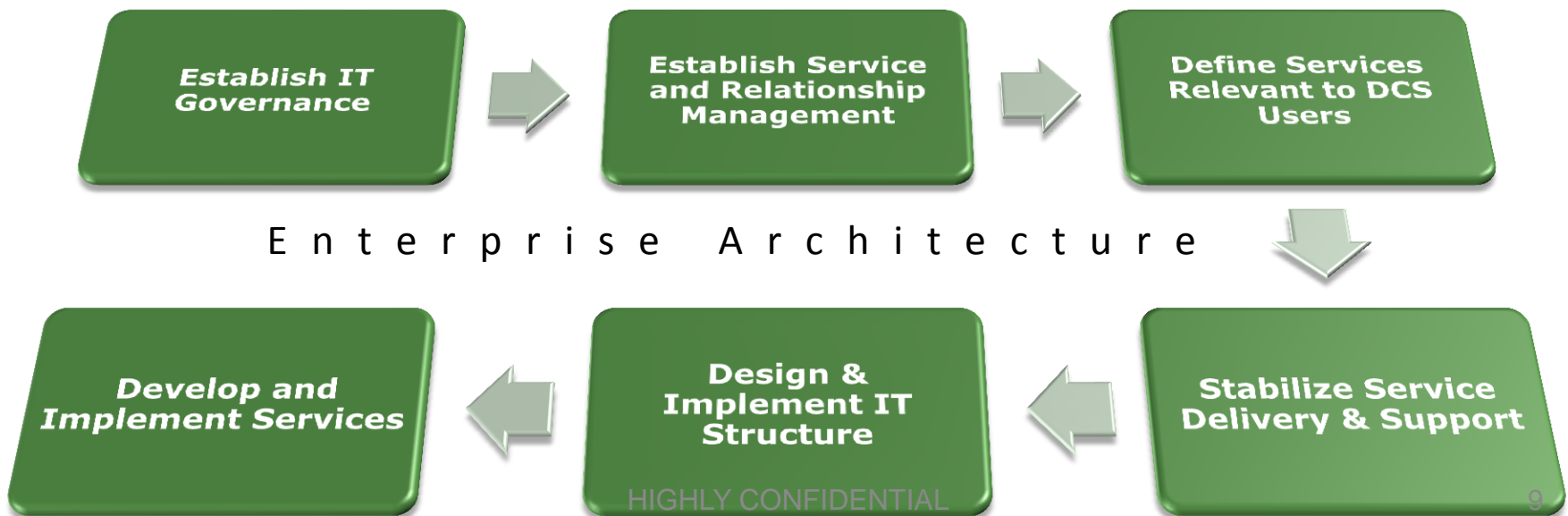


GPW IT will also add value if it matures to customer-centric process management ...





- *Use IT governance for both GPW workload and IT expense management issues and to govern IT's relationship with its business management owners and customers.*
- *Develop GPW user-relevant service definitions as the cornerstone of user responsiveness and relationship management to set and manage user expectations.*
- *Use product management and delivery management to develop responsive and cost-effective services, delivered seamlessly and efficiently to users.*
- *Combine Enterprise Architecture with business analysis and process management to improve services.*





Key Issues to be considered going forward:

1

Design a new relevant IT structure that caters to the needs of the Department.

2

Reduce the number of consultants while minimising the risk of sabotage to systems and services.

3

Implement IT Governance.

4

Design and automate best-practice security processes on systems.

5

Redesign a secured network and a consolidated, efficient and secure server environment.

6

Rationalise the application environment and consolidate more than 50 stand-alone applications.

7

Improve delivery by external service providers, especially with the State Information Technology Agency (SITA).

8

Establish enterprise architecture that will help to provide a single and correct version of data for management reporting.

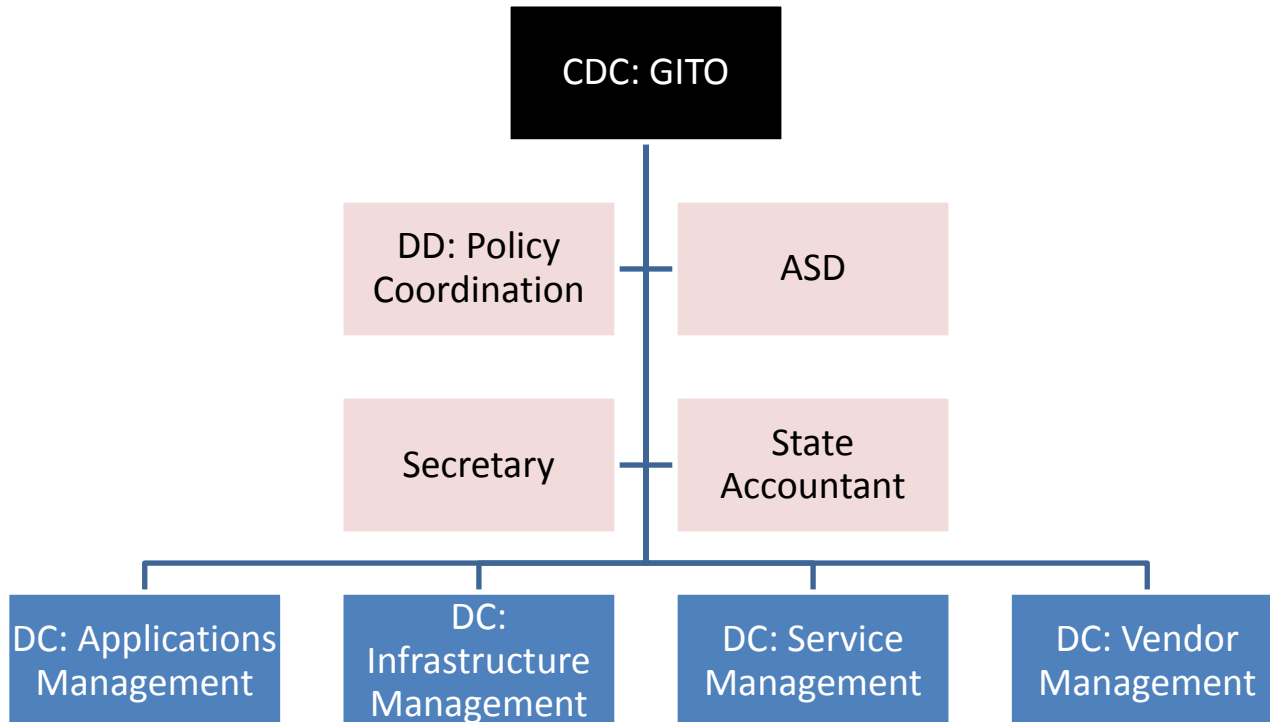
9

Timelines



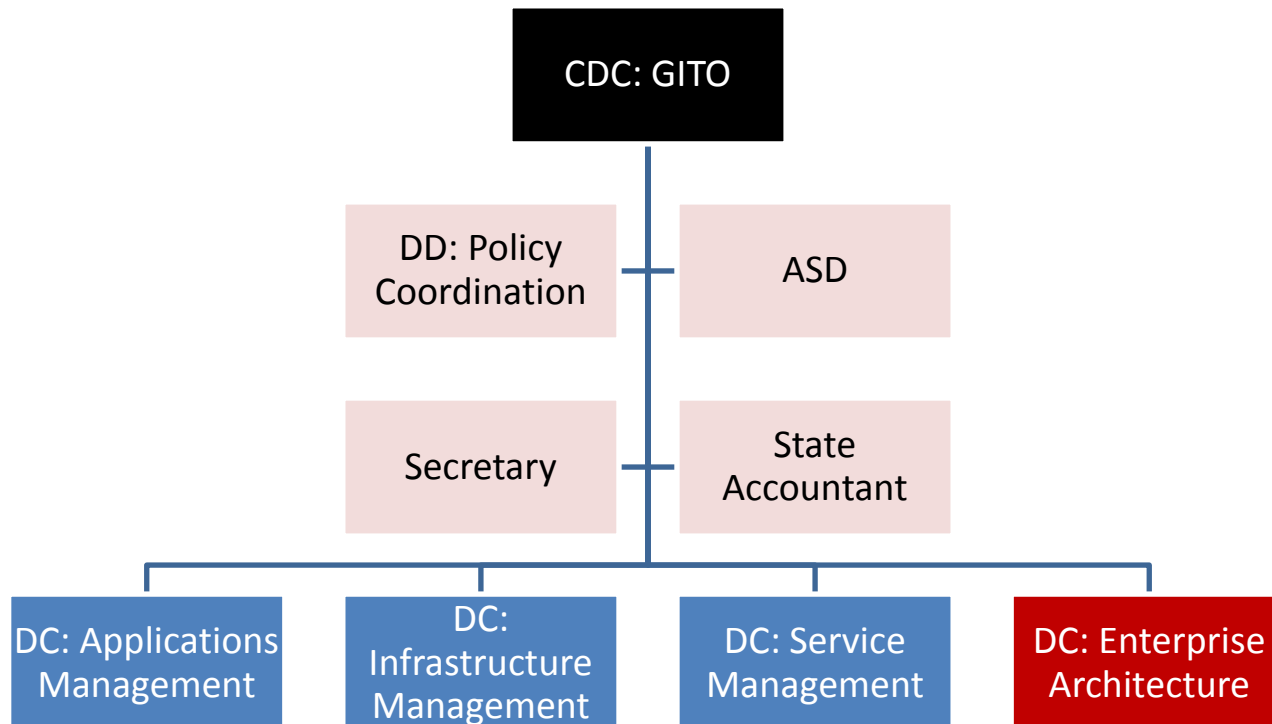


The approved structure was reviewed and found to be requiring a minor fine-tuning ...





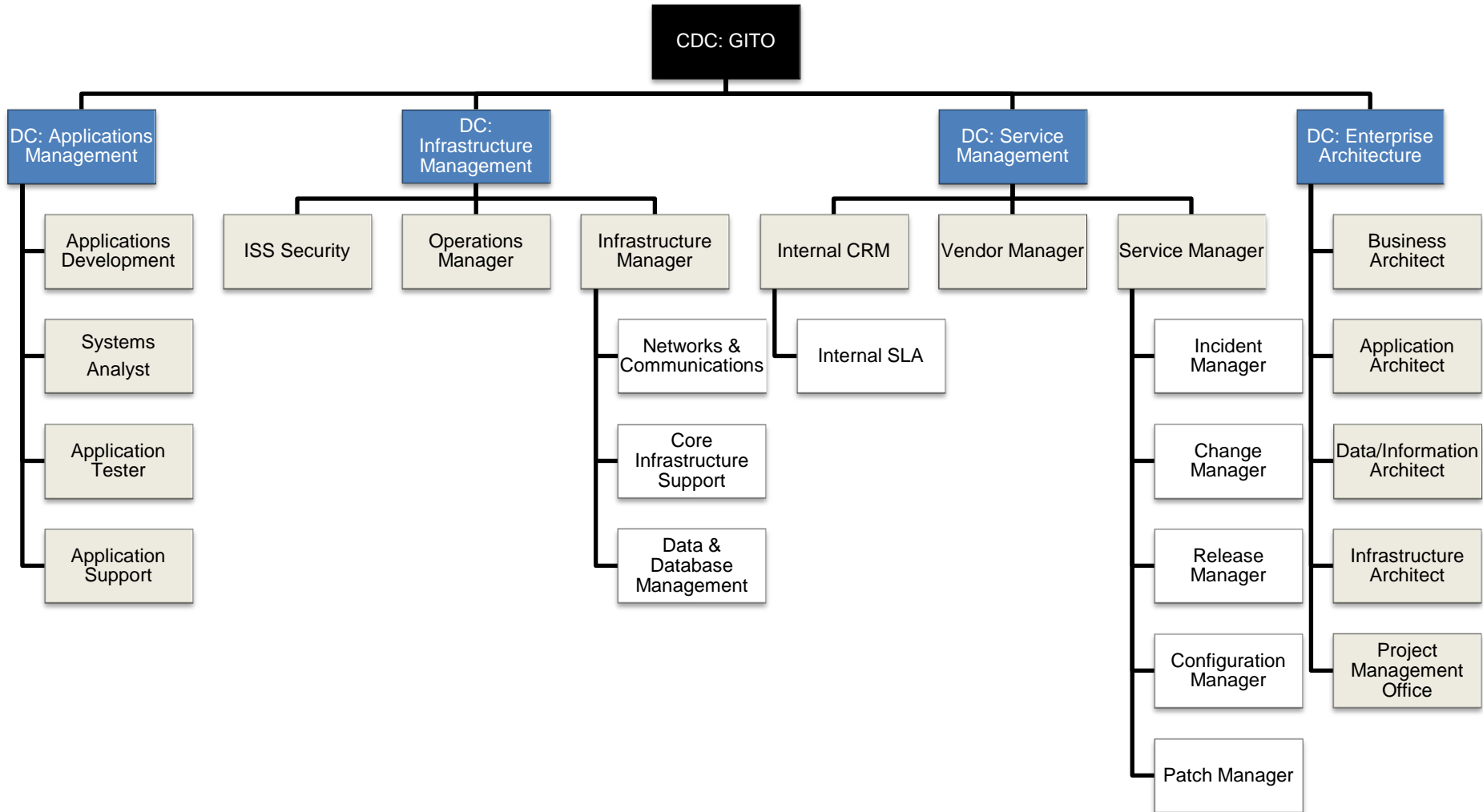
The approved structure was reviewed and found to be needing a minor fine-tuning ...



- **Vendor Management absorbed into Service Management in line with best practice.**
- **Submission being compiled for changing of Vendor Management post to Enterprise Architecture.**



Proposed Next Level





- Deputy Commissioner: Applications Management (shortlisting to be done)
- Deputy Commissioner: Infrastructure Management (shortlisting to be done)
- 14 x Level 7 Network Controllers (interviews complete, busy appointing)
- 10 x Level 7 Junior Programmers (interviews complete, busy appointing)
- 5 x Level 9 Project Administrators (shortlisting to be done)
- Deputy Director: Policy Coordinator (interviews to be done)
- ASD: Admin Secretary (shortlisting to be done)
- State Accountant (shortlisting to be done)
- Director: IT Security (advert with HR)



- Released 30 consultants on 15 June 2011.
- Annual savings of R25 million from August 2011.
- Savings to be used to fund goods and services.
- 50 consultants are still on board.
- There is a huge dependency on consultants on more than 54 legacy applications – they cannot be removed until new systems have been implemented.
- Target to reduce 10 more consultants by end of financial year.
- Other reductions will happen as new structure is implemented.



We are beginning to use the IT Balanced Scorecard to enhance skills and prepare for skills transfer.





We have reviewed the Auditor General's report ...

Establish an IT governance framework that supports and enables the business, delivers value and improves performance



... and found it necessary to attend to IT governance issues across all regions as a matter of urgency!



We are using key frameworks for IT Governance:



- An international unifying IT Governance Framework that integrates all of the main global IT standards.
- Provides a method to assess whether IT services and new initiatives meet business requirements and are likely to deliver the benefits expected.
- Helps to develop and document the appropriate organizational structures, processes and tools for effective management of IT.
- Provides an authoritative, international set of generally accepted practices that helps increase the value of IT and reduce related risks.



ISO 27000

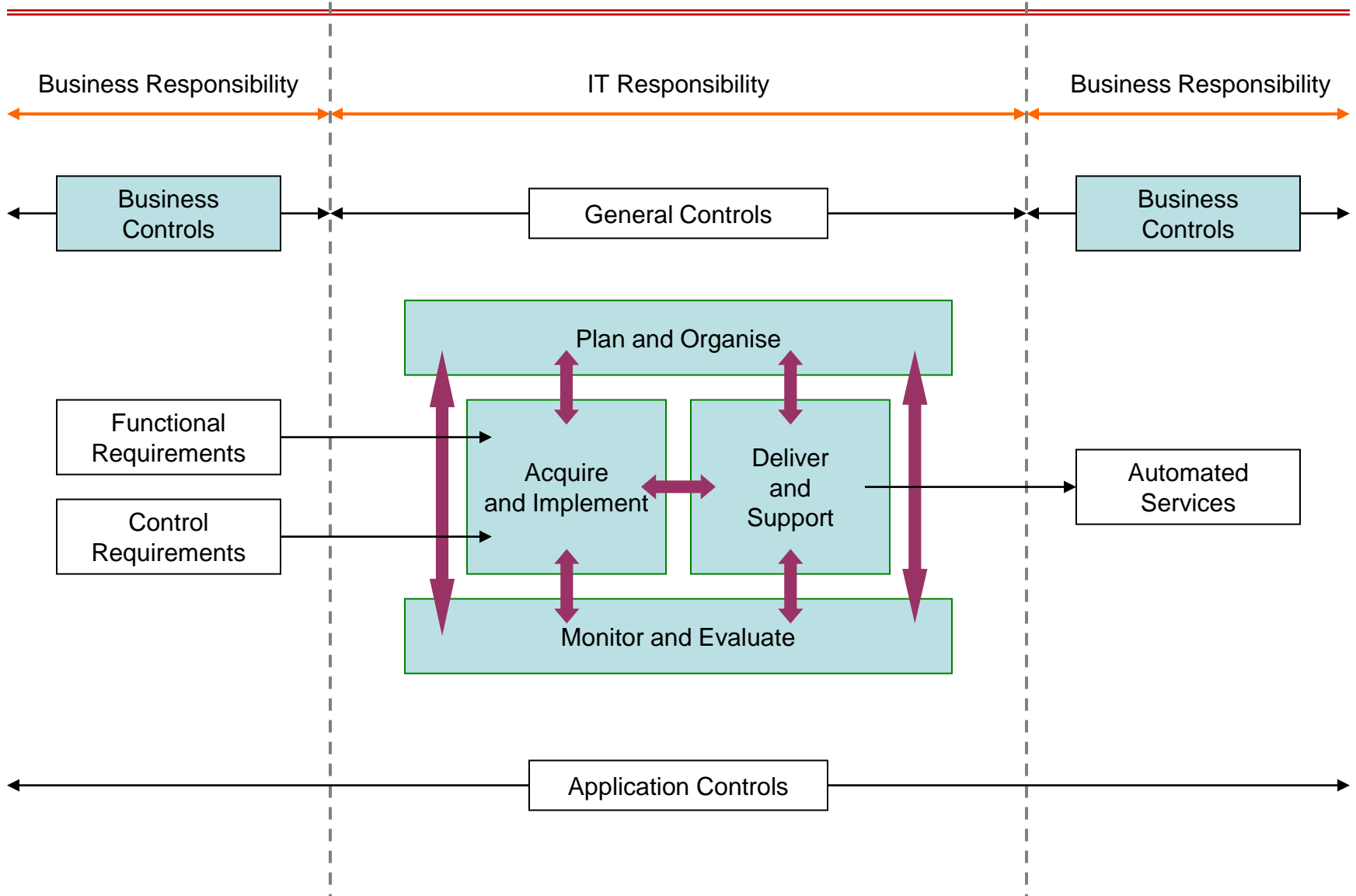
- An internationally recognized Information Security Management Standard.
- A defined process to evaluate, implement, maintain, and manage information security.
- A set of tailored policies, standards, procedures and guidelines.
- Certification allows organizations to demonstrate their own information security status.
- Certification shows "due diligence".

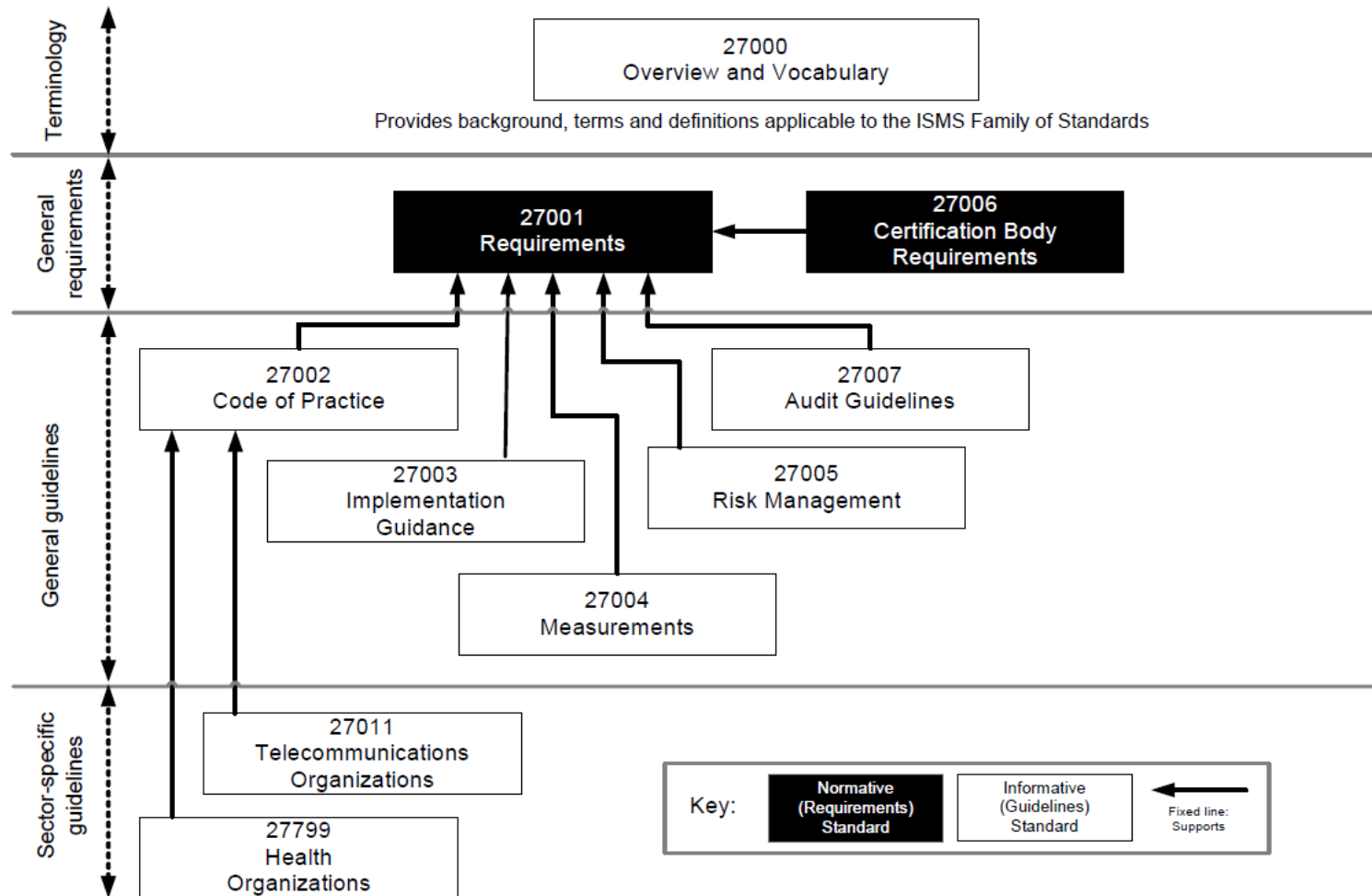


- A comprehensive, consistent and coherent set of best practices for IT Service Management and related processes:
 - Incident management
 - Problem management
 - Configuration management
 - Change management
 - Release management
 - Service desk function



COBIT will be at the heart of improving processes, data, security and much more







Planning to get external assistance to link the IT Security Policy to other Government-sanctioned security policies. Implement and automate the following related policies in greater detail

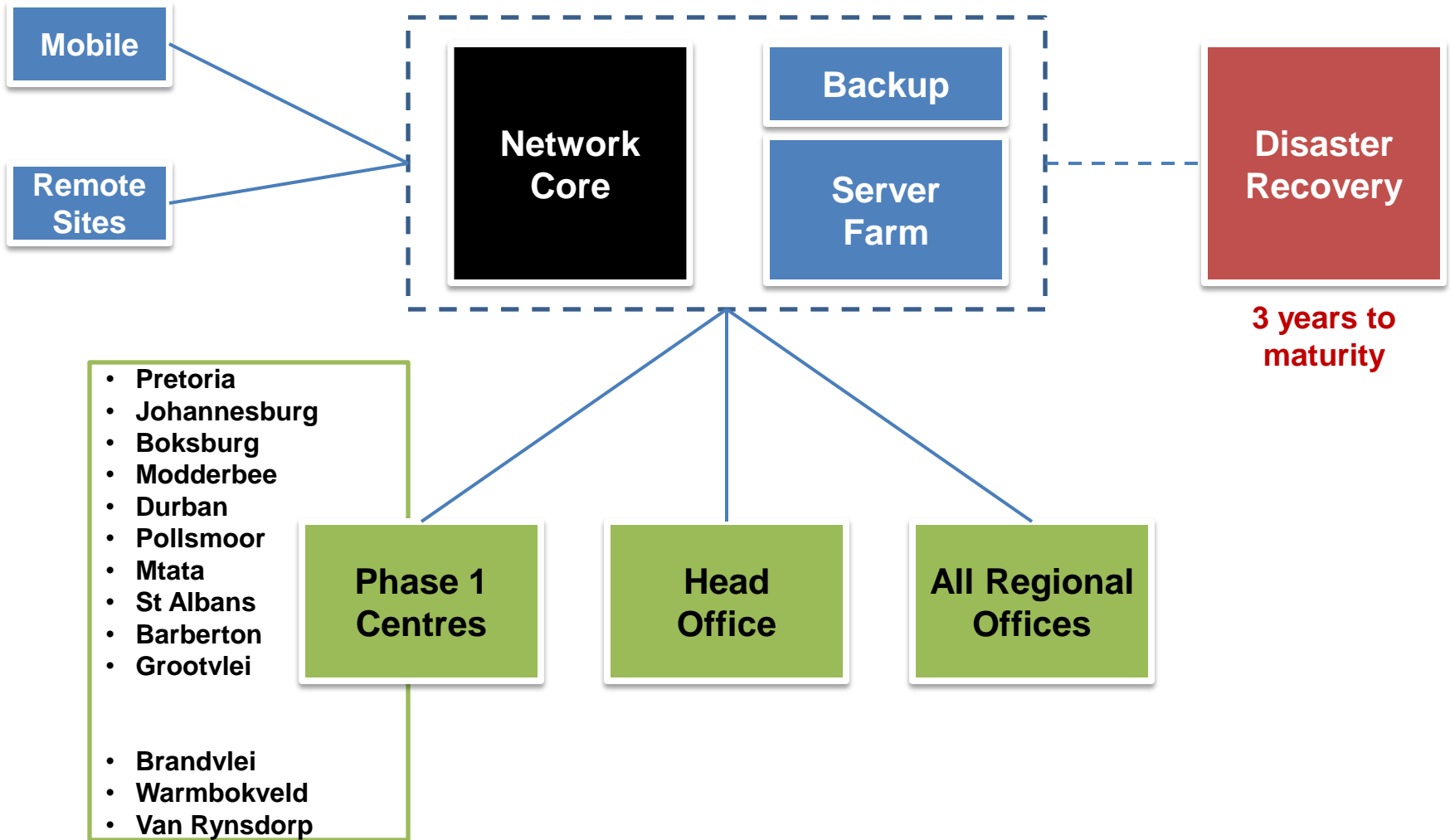
1. **Security Infrastructure Policy**
2. **Systems Configuration Policy**
3. **Systems Maintenance Policy**
4. **Systems Change Control Policy**
5. **Systems Monitoring & Auditing Policy**
6. **Data Protection Policy**
7. **Media Protection Policy**
8. **Application Security Policy**
9. **Risk Assessment Policy**
10. **Security Assessment Policy**
11. **Personnel Security Policy**
12. **Acceptable Usage Policy**
13. **Security Training Policy**
14. **Password Policy**
15. **Authorization, Identification & Authentication Policy**
16. **Account Management Policy**
17. **Physical Access Policy**
18. **Incident Response Policy**
19. **Contingency Planning Policy**
20. **Secure Acquisitions Policy**



1. The design of the new national core of the network (at a new location) is complete.
2. The design for the new Microsoft server environment at the new DCS data centre is complete.
3. The design includes provision for around 15,000 desktop units across the entire department that are connected to the new data centre.
4. The design of the new server environment for legacy systems (e.g. A&R) at the new DCS data centre is complete.
5. The design of the network and server security infrastructure is complete.
6. The Disaster Recovery Plan will be rolled out in phases, starting with an automated backup system at the new DCS data centre.



7. The design of the new network includes Virtual Private Network (VPN) functionality, meaning that we'll be able to have secured connectivity with high Quality of Service (QOS).
8. The design for the new Head Office network and the big centres is complete.
9. The design of the network of smaller centers is still in progress.
10. The design of the aligned Brandvlei and Warmbokveld networks is complete and ready for procurement.
11. Cabling for Eastern and Northern Cape is being processed.
12. Engaging SITA to move DCS to new efficient SITA network.
13. Engaging SITA on Virtual Private Network (VPN).





There are a number of QUICK WINS that can be delivered in the next year:

Governance
Implementation

Security
Automation

Improved
Connectivity

Improved
Backup

Business Process
Management

Business
Intelligence

Software as a
Service

Collaboration:
Single sign on



- Service level agreements are not signed on time and this has led to late payments and under-spending by the Department.
- The Auditor General has cited the department for SITA service level agreements without penalties.
- There is unsatisfactory technical assistance on projects done jointly with SITA.
- Meetings with SITA at a higher level, where the National Commissioner is involved, are taking place.



A structured approach will have to be used to start somewhere with data governance as infrastructure is being upgraded. Data Governance will cover the following areas:

No.	Data Management Function	Areas Covered
1.	Data Governance	Planning, supervision and control over data management and use.
2.	Data Architecture Management	As an integral part of the enterprise architecture.
3.	Data Development	Analysis, design, building, testing, deployment and maintenance
4.	Database Operations Management	Support for structured physical data assets.
5.	Data Security Management	Ensuring privacy, confidentiality and appropriate access.
6.	Reference & Master Data Management	Managing golden versions and replicas.
7.	Data Warehousing & Business Intelligence Management	Enabling access to decision support data for reporting and analysis.
8.	Document & Content Management	Storing, protecting, indexing and enabling access to data found in unstructured sources.
9.	Meta Data Management	Integrating, controlling and delivering meta data.
10.	Data Quality Management	Defining, monitoring and improving data quality



Actions	Target	Target Date
Design a new relevant IT structure that caters to the needs of the Department.	<ul style="list-style-type: none">All 4 DC positions filledThe remainder of new structure 50% filled	<ul style="list-style-type: none">31 March 201230 September 2012
Reduce the number of consultants while minimising the risk of sabotage to systems and services.	50% reduction	31 March 2012
Implement IT Governance.	35% implemented	31 March 2012
Design and automate best-practice security processes on systems.	60% implemented	31 March 2012
Implement a secured network and a consolidated, efficient and secure server environment.	<ul style="list-style-type: none">Design 100% completed30% implemented	<ul style="list-style-type: none">31 March 201131 March 2012
Rationalise the application environment and consolidate more than 45 stand-alone applications.	100% rationalised environment	29 February 2012
Improve delivery by external service providers, especially with the State Information Technology Agency (SITA).	<ul style="list-style-type: none">Business agreements complete with SITASLAs signed and payments effected	<ul style="list-style-type: none">31 December 201131 August 2011
Establish enterprise architecture that will help to provide a single and correct version of data for management reporting.	<ul style="list-style-type: none">Initiation and planning 100% complete15% implementation	<ul style="list-style-type: none">31 March 201230 November 2012



correctional services

Department:
Correctional Services
REPUBLIC OF SOUTH AFRICA

Ha khensa – Dankie – Enkosi
Ke a leboha – Ngiyabonga – Thank you
Ndo livhuwa – Ke a leboga.

2011/2012

DCS PRIORITY FOCUS AREAS

- Reduced overcrowding and improved conditions of detention
- Improved state of DCS facilities
- Effective leadership and management
- Professionalised Correctional Services and Corrections Academy
- Partnerships for delivery of rehabilitation
- Standardisation and management of DCS performance indicators
- Efficient and effective spending of public money
- Effective people management and appropriate organisational structure
- Appropriate Correctional Services image and branding
- Common understanding of the core business of the department
- Effective Correctional Sentence Plans
- Effective Security
- Involvement of offenders in corrections programmes
- Focus on development and care programmes
- Protection of human rights of inmates, particularly of special categories of inmates

**A year of action to ensure all people in
South Africa are and feel safe**



correctional services

Department:
Correctional Services
REPUBLIC OF SOUTH AFRICA

HIGHLY CONFIDENTIAL