Procurement for e-Governance Projects

RFP Preparation
July 2022

pwc

Agenda

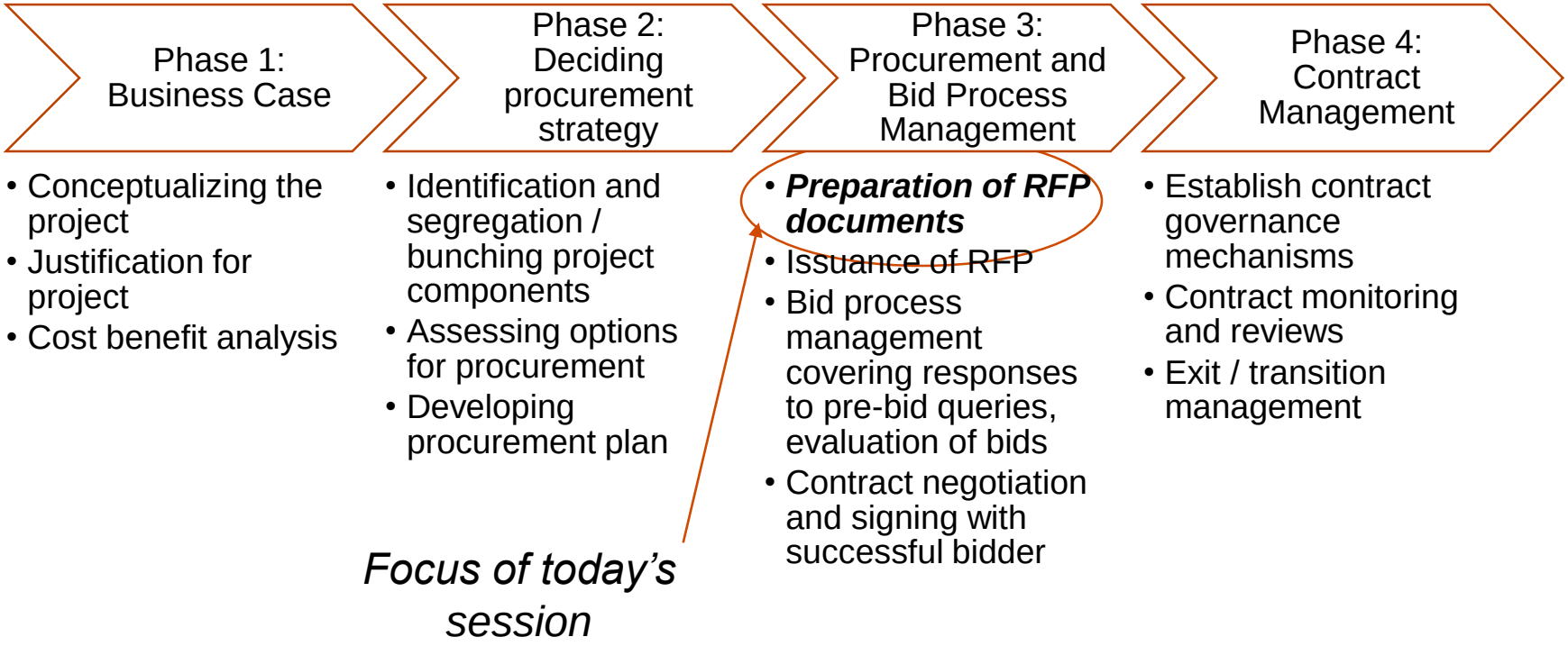
1

Setting the context

Procurement for e-Governance projects

What does it encompass?

Breaking down the phases and activities -



Requests for Proposals (RFPs) – An overview

A snapshot of the key components -

Invitation Letter

Instructions to Bidders and Bid Data Sheet (BDS)

- BDS covers qualification criteria (including eligibility, experience, financial standing, capabilities of proposed resources, etc.), bid submission details, EMD and bid security, evaluation criteria and process, proof of concept requirements, etc.

Proposal forms

- Technical and financial proposal forms
- Other declarations / undertakings

Terms of reference

- Background to the project
- Scope of work
- Key outputs and deliverables and timelines
- **Functional requirements specifications**
- **Technical / non-functional requirements specifications**
- **ICT iTRSastructure specifications, bill of quantity (BoQ) and bill of materials (BoM)**
- **Implementation and roll-out plan**
- **Other aspects (deployment, security, network, data digitization and migration, etc.)**

Contract documents

- Payment schedules
- Penalties and other clauses (liability, IPR, etc.)

To be clearly defined with sufficient detail – critical success factor for achieving value for money

Need for effectively defining scope and requirements

Numerous supply and demand side issues can be faced when the scope of work and requirements are not properly defined -

Supplier side

- Challenges in accurately ascertaining effort estimates – may result in higher quotes
- Challenges in achieving compliance to specific requirements
- Possible conflict with purchaser leading to potential litigation

Purchaser side

- Contract management may become challenging
- Potential time and cost escalations during implementation stage
- Goods/services procured may not be in line with actual requirements
- Potentially longer procurement timelines when numerous bidder queries are received

2

Functional Requirements Specifications

Understanding Functional Requirements Specifications (FRS)

FRS – What is it?

- Requirements describing what a system (including sub-systems / modules) must do and how it interacts with users

What does it communicate?

- To stakeholders – what they are going to get
- To developers – what they need to build
- To testers – what tests they need to perform

Consequently, some key principles for writing FRS documents include -

- Should be unambiguous to support traceability
- Should be uniquely identifiable
- Should be testable
- Should be well-structured

Understanding Functional Requirements Specifications (FRS)

What does it comprise?

- Operations and workflows the application must perform
- Formats and validity of data to be input and output by the application
- User interface behavior
- Data integrity and data security requirements
- What the application must do to meet safety and other regulatory requirements (if applicable)
- How the system validates user access/authorization for use and modification of the system

How to structure the functional requirements specifications (FRS)

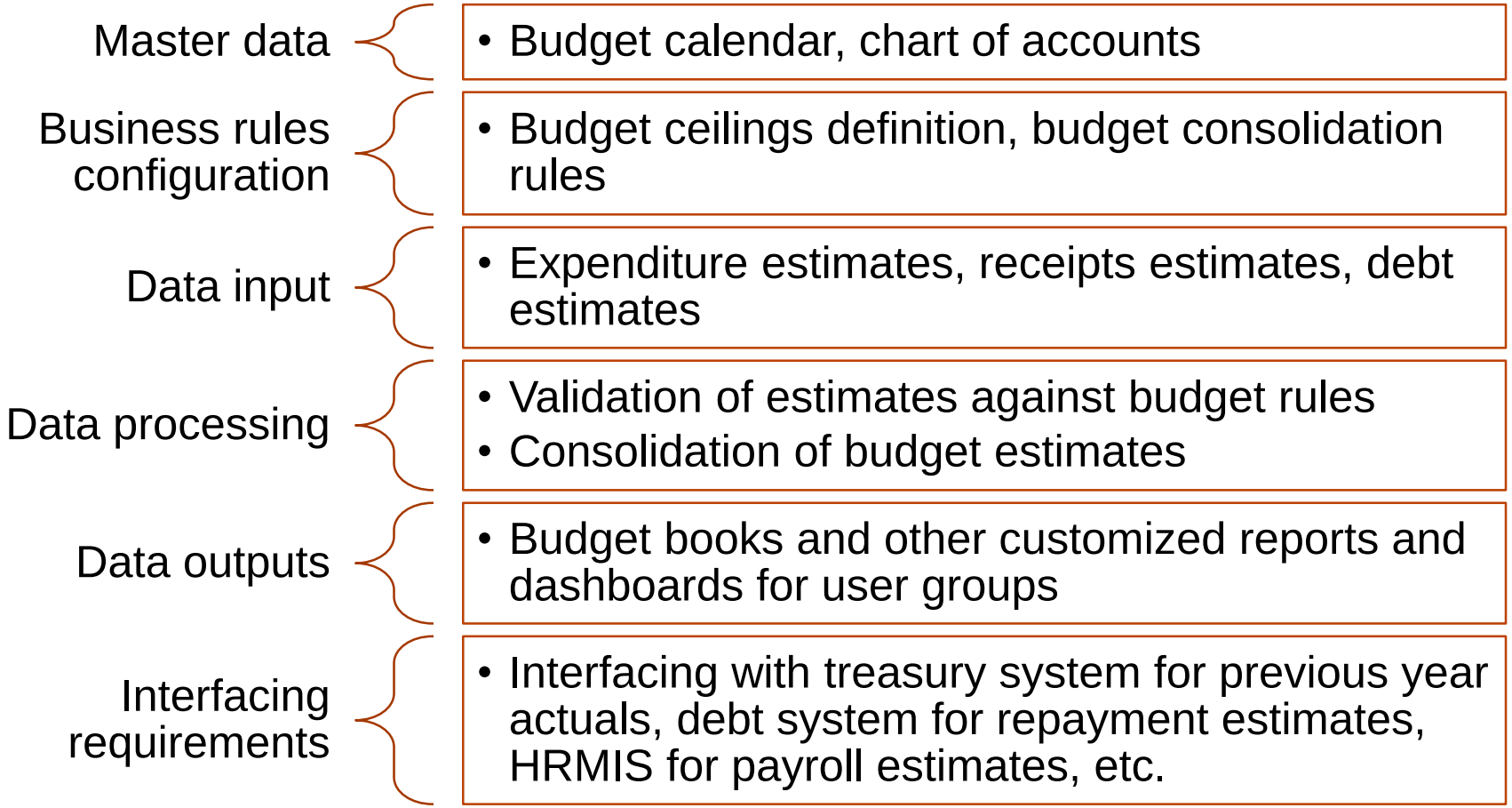
The FRS should be organized in a logical and hierarchical manner for each module / sub-module of the application -

Common requirements for all modules -
• Master data creation and maintenance • Form creation and maintenance • User access management • Security requirements • Business rules and workflow engine

Module specific requirements
• Master data relevant to the module • Data input requirements (specific forms, data fields, etc.) and validation controls for data input • Data processing requirements and business / workflow rules • Data reporting (output) requirements – custom and standard reports • Interfacing requirements (with other modules and external systems)

Illustrative example for FRS

Budget preparation module of IFMIS



Template for functional requirements specifications

S. No.	Module	Functional Requirement	Priority rating
			Mandatory / Essential
			Desirable

3

Technical Requirements Specifications

Understanding Technical Requirements Specifications (TRS)

TRS – What is it?

- Requirements describing attributes of an application such as reliability, performance, scalability, etc.

What does it cover?

- Performance and scalability
- Operating constraints
- Platform constraints
- Portability requirements and capability
- Reliability
- Security
- Usability
- Other legal requirements

Coverage – Technical Requirements Specifications (TRS)

Category	Good Practice
Capacity	•Memory requirements •Storage requirements •CPU requirements •Network requirements •Expected growth over time
Scalability	Scalability TRS's indicate how the environment will be scaled up/down. •Horizontal / vertical •Physical scalability
Availability	Availability TRS should define how the specific components in the environment will stay available in the event of component failure •Fault tolerance and HA/clustering requirements are defined in this category •Hours of operation •Location requirements – i.e. where the systems will need to be available?
Accessibility	Accessibility TRS describes how the installed systems and applications will be accessed.
Usability	Usability TRS describes what measures will be used to define if the new environment is usable. •Application look and feel •Localization / internationalization requirements
Failover / DR targets	This TRS describes the failover targets not only for the environment as a whole but for individual environment components.
Resilience	This describes the internal resilience for each component in the environment (hardware and software) and how it will behave in the event of an internal failure. E.g. How a system will react when a NIC fails.
Maintainability	This TRS describes how the environment will be maintained going forward. •Green zones definition. •patching cycles /schedules. •Batch run schedules •Backup cycles

Coverage – Technical Requirements Specifications (TRS) Contd.

Category	Good Practice
Latency	This TRS covers any latency requirements within the environment. •Network latency timings to which locations E.g. For users located in US the system should respond in less than 100ms
Interoperability	Defines how the designed environment will interact with other new systems or legacy systems. •It should include the type and direction of interaction in the new environment.
Longevity	•Defines the expected lifespan of the designed systems. •EOL for each component •EOSL for each component
Strategy Compliance	If the designed environment is to fit into a wider IT landscape this TRS describes how the new environment will conform to the IT strategy.
Monitoring	This TRS will describes how the new environment will be monitored. •Monitoring tools •Monitoring thresholds
Manageability	Describes how the new environment will be managed and should include definition of the tools and methods used. •MIS reporting requirements.
Recoverability	This TRS covers who the data in the environment will be recovered. •Should include description of the backup cycle and methods and tools which will be employed to backup the environment.
Reliability	This TRS defines the expected reliability of the planned environment. •MTTF – meantime to failure •MTTR – mean time to recovery
Concurrency	This TRS should describe the number of instances of the application or the number of user who can use the system without causing an performance impact.

Coverage – Technical Requirements Specifications (TRS) Contd.

Category	Good Practice
Security	This TRS describes what security tools , methods and procedures will be used in the new environment. •It should also describe how the environment will fit into the wider IT security standards.
Audit Compliance	Defines how the new environment will conform to audit compliance requirements. •Audit files / fields •Audit log requirements
Throughput	What will be the expected throughput of the planned environment. •Number of transactions to be processed in a given time.
Performance	Will define how the designed environment will perform •Response times •Screen refresh rates •Query response times
Supportability	This TRS will describes how the new environment will be supported •3rd party SLA •Standard support tools •Bespoke tools and scripts
Portability	Describes how the new environment may be moved.
Integrity	The integrity TRS covers how the environment will react to bad data •Fault trapping •Bad data trapping •Data integrity
Testability	This TRS defines the testing requirements for the planned environment. •Scope of tests •Who will sign-off the tests •How the environment will be tested

4

ICT Infrastructure Specifications

ICT infrastructure typically procured for e-Governance projects –

Can be new or replacement hardware

Servers

- Application servers
- Database servers
- Testing servers, etc.

Storage products

Networking infrastructure

End-user infrastructure

- Desktops
- Printers
- Laptops
- Other peripherals

Defining ICT infrastructure specifications

General good practices and principles -

Most turnkey RFPs receive highest number of pre-bid queries on ICT infrastructure and SLAs – defining specifications efficiently will help streamline bid process management

- Specifications should not have brand names or reference to proprietary features
- Should be included where quantity and specification are measurable
- Should be up-to-date and relevant to business context
- Should take into account existing ICT infrastructure and replacement potential to optimize costs
- Should be defined for common parameters that can be used for comparison
- Should not be skewed towards any specific product or feature

Defining ICT infrastructure specifications

Some illustrative parameters for Bill of Material

Note: Make and model is typically proposed by the bidder

For servers	SAN Storage	Load Balancer
• Quantity • Make and Model • Year of Introduction • Operating System along with version (if applicable) • Processor and Number of Cores Offered (if applicable) • Architecture (RISC/EPIC/CISC) (if applicable) • RAM/HDD/LAN Ports/ HBA (as relevant)	• Quantity • Make and Model • Capacity • Fibre channel ports • Redundancy • Virtualization support	• Quantity • Make and model • Throughput • Scalability • Processor and Number of Cores Offered (if applicable)

5

Service Level Definition and Management

Service Level Management

Some key definitions -

Service Level: A Service Level defines the quality and quantity of service, in a measurable and objective way.

Service Level Objective (SLO): is the set of purposes or objectives sought to be achieved through defining and prescribing the Service Levels for an initiative or organization.

Service Level Agreement (SLA): is an agreement between the Service Provider and the Service Seeker that defines the Service Levels, the terms and conditions for enforcing the Service Levels and the remedies in case the Service Levels are not fulfilled.

Service Level Management (SLM): is an institutional arrangement that ensures effective implementation of the Service Levels and enforcement of the SLA

Service Level Management

Typical challenges faced -

Non-alignment of SLAs with business goals

Unrealistic definition of SLAs

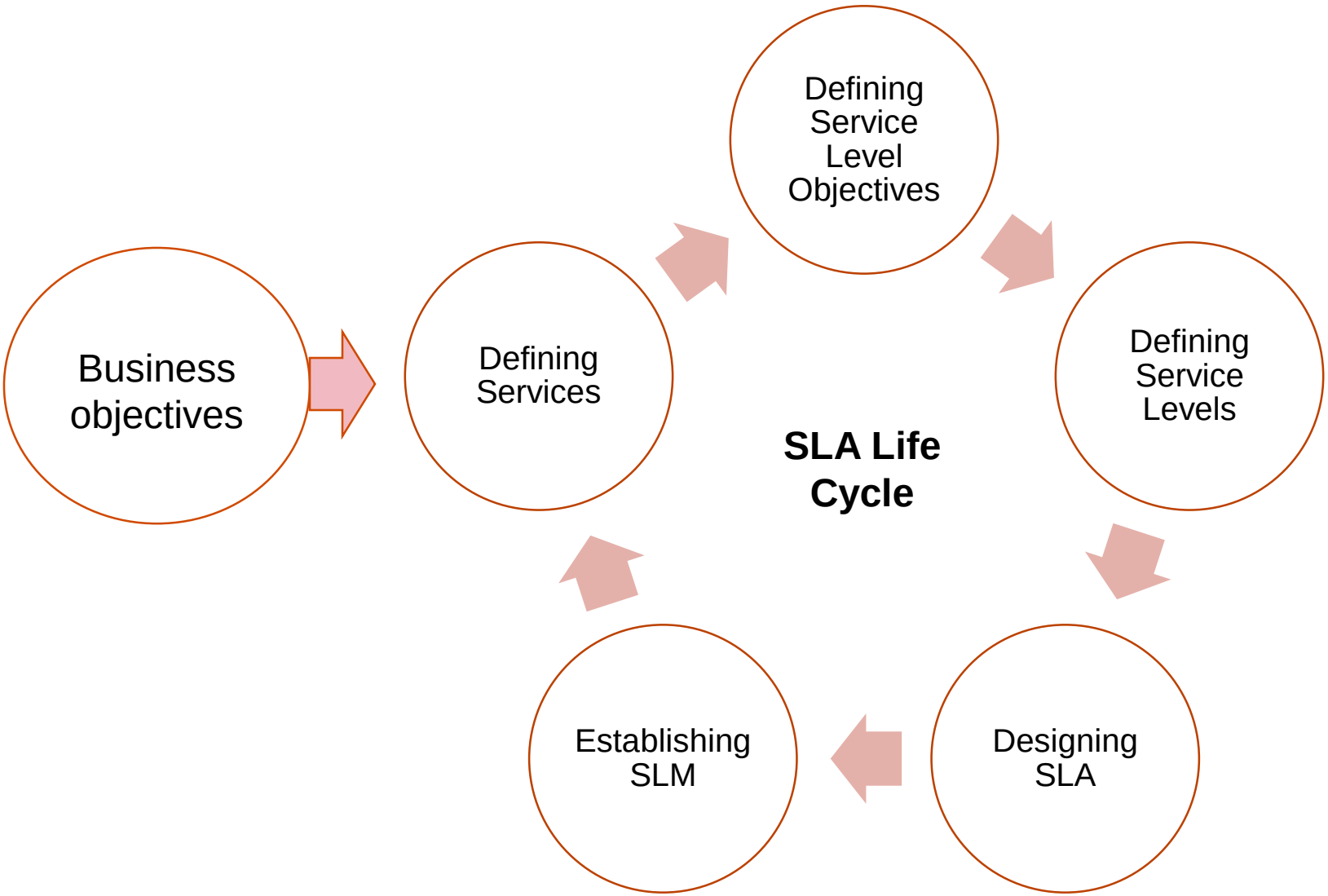
Challenges in measurability of SLAs

Limited capacity for effective SLA monitoring

Limited understanding of cost implications of SLAs

- 99.999% availability – 5 minutes unplanned downtime for a year
- 99.9% availability – 1 day of unplanned downtime for a year

SLA Lifecycle



Defining Service Levels

The components of the Service Level Definition are:

- **Service Level Parameters:** measurable attributes of the service, which will provide a reliable and objective estimate of the quality and quantity of service
- **Service Level Metrics:** A set of norms prescribed against each service level parameters to provide baseline performance expected from Vendor
  - Baseline: Acceptable level of service by the vendor
  - Lower: Degraded level of service, for which vendor may be penalized
  - Higher (optional): Higher level of service for which vendor may be incentivized
  - Breach: Highly degraded level of service / material breach, which may invite termination contract
- **Service Level Measurement Method:** Precise, reliable and consistent method by which the service level parameter can be measured
- **Service Level Enforcement Method:** Method by which the service level agreement can be enforced (deduction from payments, penalties etc)

Defining Service Levels

Illustrative examples for various scope components -

Service category	SLA and metric	Service category	SLA and metric
Data digitization	Accuracy per batch – ratio of errors to records	Service levels	Data exchange availability (exclude scheduled downtime)
	Timeliness – delays in batch completion		Helpdesk response time (based on ticket categorization)
	Uptime / Availability (exclude scheduled downtime) – as % of total operating business hours		Bug fixes / issue resolution time
Service levels	Page loading time	ICT infrastructure and network	DC / DR availability
	Data upload time		Network availability (peak and non-peak hours)
	Form submission time	Capacity building and change management	% positive feedback from respondents
	Notification time		Documentation management

Defining Service Levels – Illustrative example

Service Metrics Parameters	Baseline		Lower performance		Breach		Measurement method
	Metric	Credit	Metric	Credit	Metric	Credit	
Technology – Performance Related							
Capacity of the Application Server	10000 service transactions per hour	6	No tolerance for lower performance. Zero credit will be given for performance below baseline		<6000	-6	Measurements from the Enterprise SLA Monitoring System at the State Data Centre
Uptime of Servers	> 95%	12			<96%	-8	
Uptime of Internet services	>98%	4			>95%	-4	
Time to restore Data Centre from failure	<1 hour	5			>3 hours	-5	

Service Level Enforcement

SLAs can be most effectively enforced by linking the payments to the Service Provider to the degree of compliance with the SLA

Deduction Method:

- Vendor gets 100% payments (monthly / quarterly / milestone) for full compliance to the SLA
- For lower performance from SLA, specified percentage is deducted. Higher performance may be incentivized by bonus payments

Addition Method:

- A percentage of the payment (e.g. 40%) to the SP is made dependent on the fulfillment of Service Level Matrix
- All SLPs are assigned credits for baseline, lower, higher and breach metric. Credits will depend on the priority of the SLP
- Scores prescribed for baseline performance will add up to 100%

Thank you

pwc.com