Service | Innovation | Value

TELECOMMUNICATIONS TRANSFORMATION PROGRAM

Data Centre Networks

Industry Day

February 27, 2014

Shared Services Canada | Services partagés Canada

Canada

Data Centre Networks Industry Day

Industry Day Objectives

- Share plans with industry suppliers and engage in a dialogue regarding network service delivery options for the Government of Canada data centres
- Explain the proposed “Collaborative Procurement Solutions” approach
- Address the Cyber Security Supply Chain Threat
- Elicit feedback from industry on the deployment models, high availability options, emerging technologies, contract period and pricing options

Data Centre Networks Industry Day

Agenda

TIME	PRESENTER	DESCRIPTION
1:30 - 1:35 pm	**John Dullaert** *Director, Telecommunications Transformation Program, Shared Services Canada (SSC)*	Opening Remarks and Industry Day Objectives
1:35 – 2:05 pm	**Peter Littlefield** *DG, Data Centre Consolidation Program, SSC*	SSC Transformation Overview
2:05 - 2:45 pm	**Michel Fortin** *DG, Telecommunications Transformation Program, SSC*	*Data Centre Networks* – Inter-Data Centre Overview & Key Questions
2:45 – 3:00 pm	***Break***	
3:00 – 3:45 pm	**Michel Fortin** *DG, Telecommunications Transformation Program, SSC*	*Data Centre Networks* – Intra-Data Centre Overview & Key Questions
3:45 – 4:15 pm	**Brad McInnis** *Cyber Security Advisor, IT Security Strategic Relationships Office, Communications Security Establishment Canada* **Raj Thuppal** *DG, Cyber and IT Security Transformation Program, SSC*	Supply Chain Security Information (SCSI) Assessment
4:15 – 4:30 pm	**Tom Mercer** *Manager, Telecommunications Systems Division, Procurement and Vendor Relationships, SSC*	Collaborative Procurement Solutions Approach
4:30 – 5:00 pm	**John Dullaert** *Director, Telecommunications Transformation Program, SSC*	Questions and Answers, Recap / Closing Remarks

Service | Innovation | Value

TELECOMMUNICATIONS TRANSFORMATION PROGRAM
Data Centre Networks (DCN) Industry Day

Shared Services Canada (SSC) Transformation Overview

Peter Littlefield
Director General, Data Centre Consolidation Program, Transformation, Service Strategy and Design

February 27, 2014

Shared Services Canada (SSC) Transformation Overview

Agenda

- Industry Day Objectives / Key Messages
- SSC Strategic Vision and Principles
- Transformation Objectives
- Transformation Purpose
- Transformation Timeline and Phased Approach
- Current State of Data Centres and Networks
- Conceptual End State
- Business and Functional Requirements
- Engagement
- Wrap up

SSC Transformation Overview

Purpose of Industry Day

- To provide **background** on telecommunications transformation and the Data Centre Networks
- Highlight the alignment / integration with Data Centre Consolidation
- To **continue a dialog** with Industry to learn what are the best and most innovative options available in the market today that will support the Government of Canada's requirements for the Data Centre Networks
  - Obtain industry input on the strategy for:
    - deployment models
    - high availability
    - emerging technologies
    - length of contract
    - pricing model
  - Advice that could lead to better pricing (based on past experience)
  - Address questions regarding process
  - Set the stage for the one-on-one engagements

SSC Transformation Overview

Strategic Vision and Principles

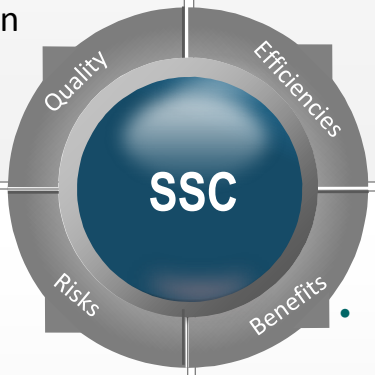
The Government of Canada (GC) will consolidate data centres and networks, transform telecommunications services, centralize their administration, and rationalize service delivery to achieve greater efficiencies, reduce costs, minimize risks, and improve security and service quality

Improve Service Quality

- Improve levels of service and security for all
- Modernize infrastructure and platforms
- Increase system availability, reliability, robustness and scalability
- Reduce dependence on physical location
- Implement ubiquitous personal mobility

Maximize Efficiencies

- Consolidate and converge to reduce duplication of infrastructure
- Standardize infrastructure and operations
  - Determine appropriate level of private sector engagement
  - Make effective use of shrinking information technology (IT) labour force



Minimize Risks

- Fewer and better quality facilities
- Increase information security
- Power supply diversification
- Centralize planning and recapitalization
- Address aging IT infrastructure
- Examine industry investment and risk sharing

Additional Benefits

- Significant environmental benefits
  - Reduce power demand
  - Reduce greenhouse gas emissions (cleaner power); reduce e-waste
- Enable Workplace 2.0
- Reduce travel costs (videoconferencing)

SSC Transformation Overview

Transformation Objectives

SAVINGS

Transformation will realize material cost savings and avoid future costs

SERVICE

Transformation will match service levels to partner priorities

SECURITY

Transformation will provision a secure environment to meet program needs

SSC Transformation Overview

Purpose of Transformation

SSC will transform the GC's aging IT infrastructure by delivering:

EMAIL

One Email Solution

Objective: *Migrate the GC to a single, outsourced, secure email system*

END USER DEVICE

Consolidated procurement of end-user device hardware and software

Objective: *Consolidate procurement of end-user devices & related software*

DATA CENTRE

A government-wide footprint of 7 data centres

Objective: *Consolidate the GC's 485 data centres into 7 modern and efficient facilities*

NET-WORK

A single government-wide telecommunications network

Objective: *Streamline and modernize the GC's telecommunications infrastructure and services*

SSC Transformation Overview

Email

2013-2014

- Strategy Development, Business Case and Plan
- Build and Migration to New Service (Waves 0 and 1)
- Migration to New Service (Waves 2 and 3)

Workplace Technology Devices

2013-2014	2014-2015	2015-2020
Service Strategy, Pilot, and Preliminary Business Case	Current State, Business Case and Plan	Implementation

Focus of Today's discussion

Data Centres

2012-2013	2013-2020	
Current State, Business Case, Detailed Inventory and Plans	Data Centre Foundations: Facilities, Platforms and Infrastructure	Migration to New Data Centres (Multiple Waves)

Telecommunications

2012-2013	2013-2020
Current State, Business Case, Detailed Inventory and Plans	Inter-building (wide area network [WAN]) - integrated and aligned with data centre consolidation plan
	Intra-building (local area network [LAN]) - integrated and aligned with data centre consolidation plan
	Telecommunication services transformation – data, voice, video and call centre services

Cyber and IT Security

2011-2012	January – April 2012	2013-2014 and ongoing
Canada Cyber Security Strategy		Security Operations Centre
		Supply chain integrity process and infrastructure cyber recall system
		Government of Canada Secret infrastructure
		IT Security Services

SSC Transformation Overview

Transformation Phased Approach

UNIT OF TRANSFORMATION WORK:

Data Centre Consolidation (DCC): ***Server***

Telecommunications Transformation Program (TTP): ***Building***

1. Establish Overall Approach

- Produce **Reference Architecture**
- Establish **Core Services** roadmap
- Develop "Migration Factory" approach
- Define consolidation sequence – Competing factors
- Determine sourcing strategies
- Develop security by design

2. Pre-planning

- Produce detailed current state / asset and application information
- Develop detailed partner requirements
  - Business cycles
  - Application refresh plans
  - Overall readiness
- Define all Data Centre and Telecom Services
- Develop Consolidation Priority List (CPL)
- Conduct Procurement (including P3, etc.)

3. Planning

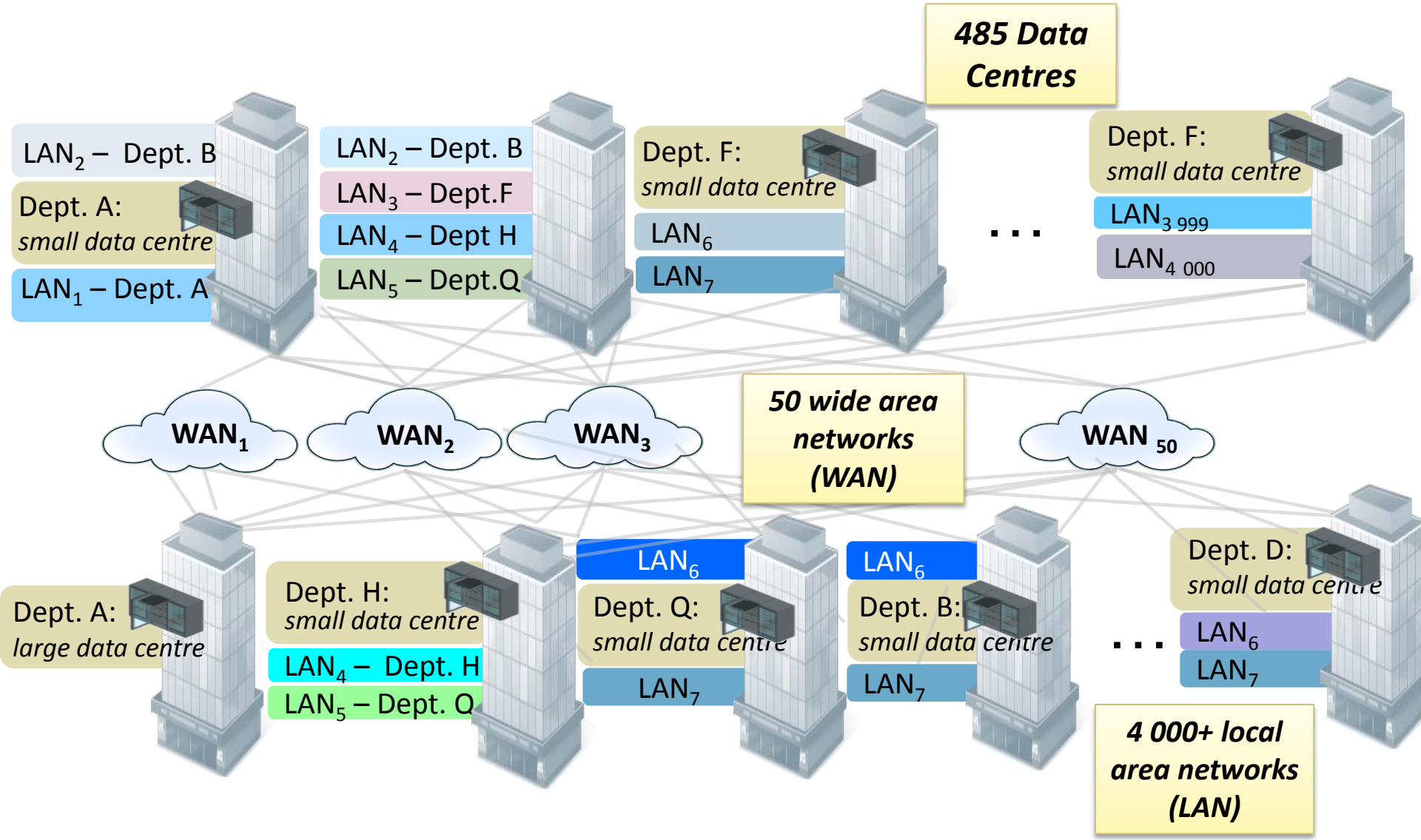
- Define org structure
- Define migration and receiving teams
- Develop HR Management and Talent Plans
- Projectize by priority/CPL
- Identify application interdependencies and infrastructure requirements
- Align network consolidation plan with data centre and application migration requirements

4. Execution

- Establish enterprise data centres and GCNet
- Build new operations organization
- Establish all ITSM tools and processes
- Build migration and receiving teams
- Perform quality control
- Assist partners in the migration of all business applications
- Install and configure new infrastructure
- Close ("shred") data centres as they are vacated

SSC Transformation Overview

Current State of Data Centres and Networks



SSC Transformation Overview

Conceptual End-state

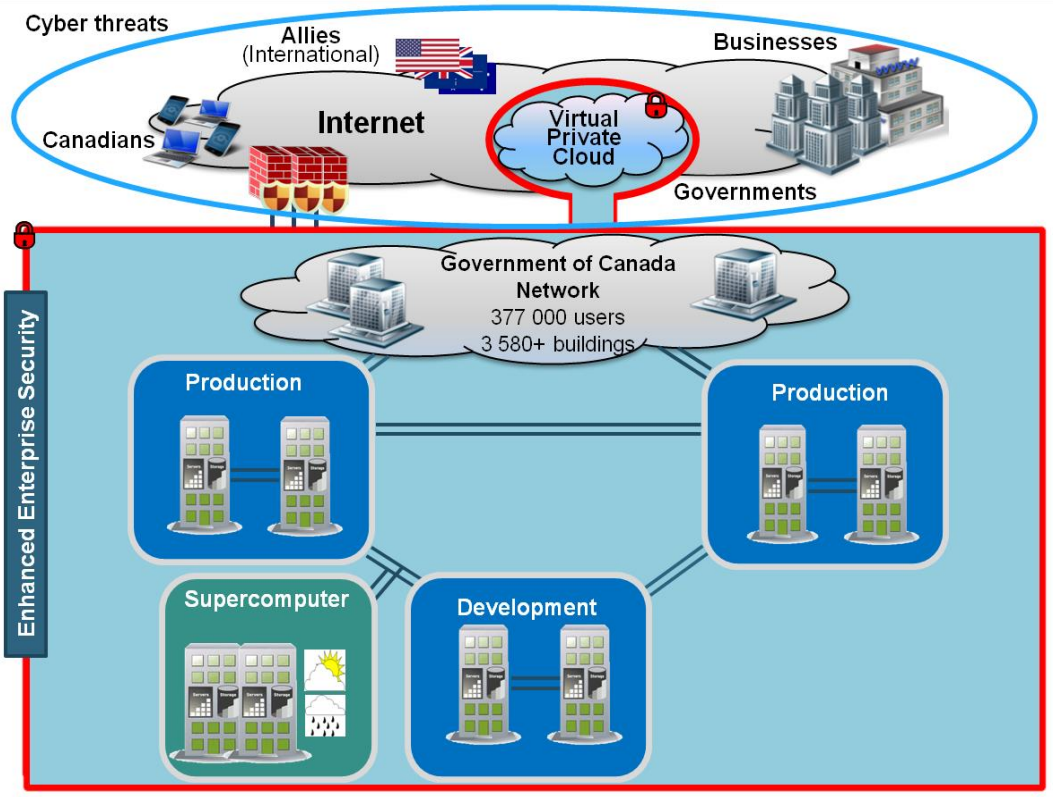
SECURITY

- All departments share one enterprise/common zone
- Access to sensitive departmental data is secured through restricted zones
- Developers do not have access to production infrastructure
- Classified information below Top Secret
- Consolidated, controlled, secure perimeters
- Balance security and consolidation
- Certified and Accredited infrastructure

CHARACTERISTICS

- Integrated (single, common, secure GC network will link all service delivery points)
- High performance
- Secure
- Cost-effective
- Standardized (based on open standards, modularized design)
- Mobile (wireless technology will be maximized where cost-effective)
- Responsive and resilient

Simpler, Safer and Smarter



CONSOLIDATION PRINCIPLES

1. As few wide area networks as possible
2. All departments share network access in multi-tenant buildings
3. Network equipment is shared
4. Telecom hubs (call managers, VC bridges) located in enterprise data centres or common points of presence
5. Inter-data centre connections should be diverse and fully redundant
6. Scalable and flexible infrastructure
7. Performance levels should be similar wherever possible
8. Contracts/services will be consolidated

BUSINESS INTENT

- Business to Government
- Government to Government
- Citizens to Government

SSC Transformation Overview

Data Centre Networks - Business Requirements

- **Support a wide variety of federal government programs** and applications ranging from corporate file stores and routine data exchanges, to real-time government-wide mission-critical military, policy, health and public safety information
- **Enterprise** infrastructure and service management to eliminate silos and **facilitate interoperability** across departments and agencies
- **Reduce duplication** and inefficiencies
- **Ensure high availability** for mission critical applications
- **Standardize service levels** to ensure a consistent delivery and availability of Data Centre services across all SSC partners and agencies
- **Built-in, on-going competition** to ensure best value, continuous improvement and innovation of services
- **Security**: Supply must meet the **Trusted Supply Chain Requirements** (identified in the "Supply Chain Integrity" presentation to follow)

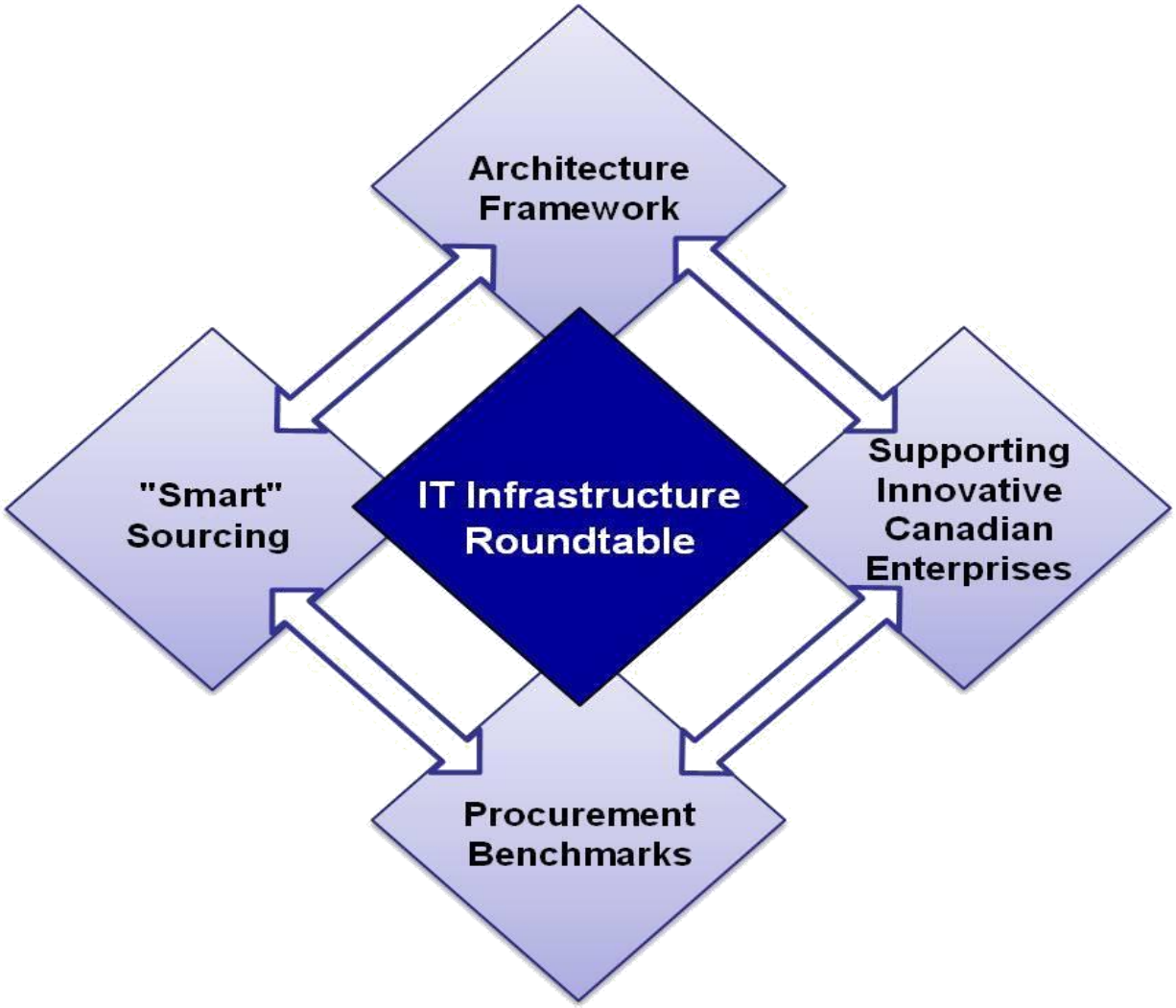
SSC Transformation Overview

Data Centre Networks - Functional Requirements

- **Supplier diversity for Inter-Data Centre Network connectivity**
- **Open standards** to allow for workload mobility / portability across suppliers
- **Certified compliance and compatibility** with SSC reference architectures
- Must support **self-service / self-provisioning** of data centre services
- Must support **just-In-time capacity**
- **Frequent market checks** to take advantage of technology, economic or market shifts
- **Provisions for annual price competition** to ensure best value to Canada
- Must support a **secure, multi-tenant environment** (GC Domains and Zones)

SSC Transformation Overview

Stakeholder Engagement - IT Infrastructure Roundtable and Advisory Committees



SSC Transformation Overview

Data Centre Networks - Engaging Industry for Feedback

- SSC will engage industry for feedback throughout the collaborative procurement process, which will result in:
  - A balance of industry capability with cost effectiveness
  - Allow for an exchange of information through discussion (during one-on-one sessions) with telecommunications experts that will ultimately inform telecommunications transformation strategies and procurement planning
  - Provide suppliers with the opportunity to share their knowledge with the Government of Canada on the following discussion topics (detailed slides to follow):
    1. **Deployment Models**
    2. **High Availability**
    3. **Emerging Technologies**
    4. **Contract(s) Period**
    5. **Pricing Models**

SSC Transformation Overview

Wrap Up and Questions

Questions?

(for suppliers only)

Service | Innovation | Value

TELECOMMUNICATIONS TRANSFORMATION PROGRAM
Data Centre Networks (DCN) Industry Day

Data Centre Networks Overview

Michel Fortin

Director General, Telecommunications Transformation Program

Transformation, Service Strategy and Design

February 27, 2014

Shared Services Canada | Services partagés Canada

Canada

Data Centre Networks Industry Day Overview

Objectives

- Provide an overview of the Telecommunications Transformation Program and Data Centre Networks, focusing on the key components of Data Centre Network services
  - Stream 1 – Inter-Data Centre Networks
  - Stream 2 – Intra-Data Centre Networks

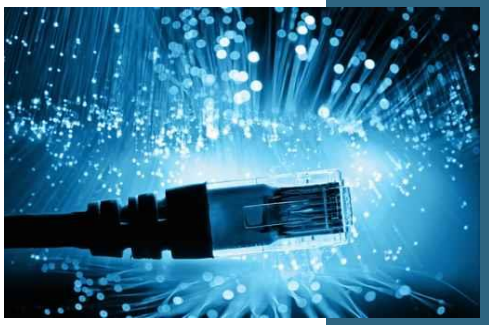
- Highlight considerations for future service provision of these services
  - Deployment model considerations
  - High Availability options
  - Emerging technologies
  - Contract period
  - Pricing model options

- Solicit feedback from industry

Telecommunications Transformation Program (TTP)

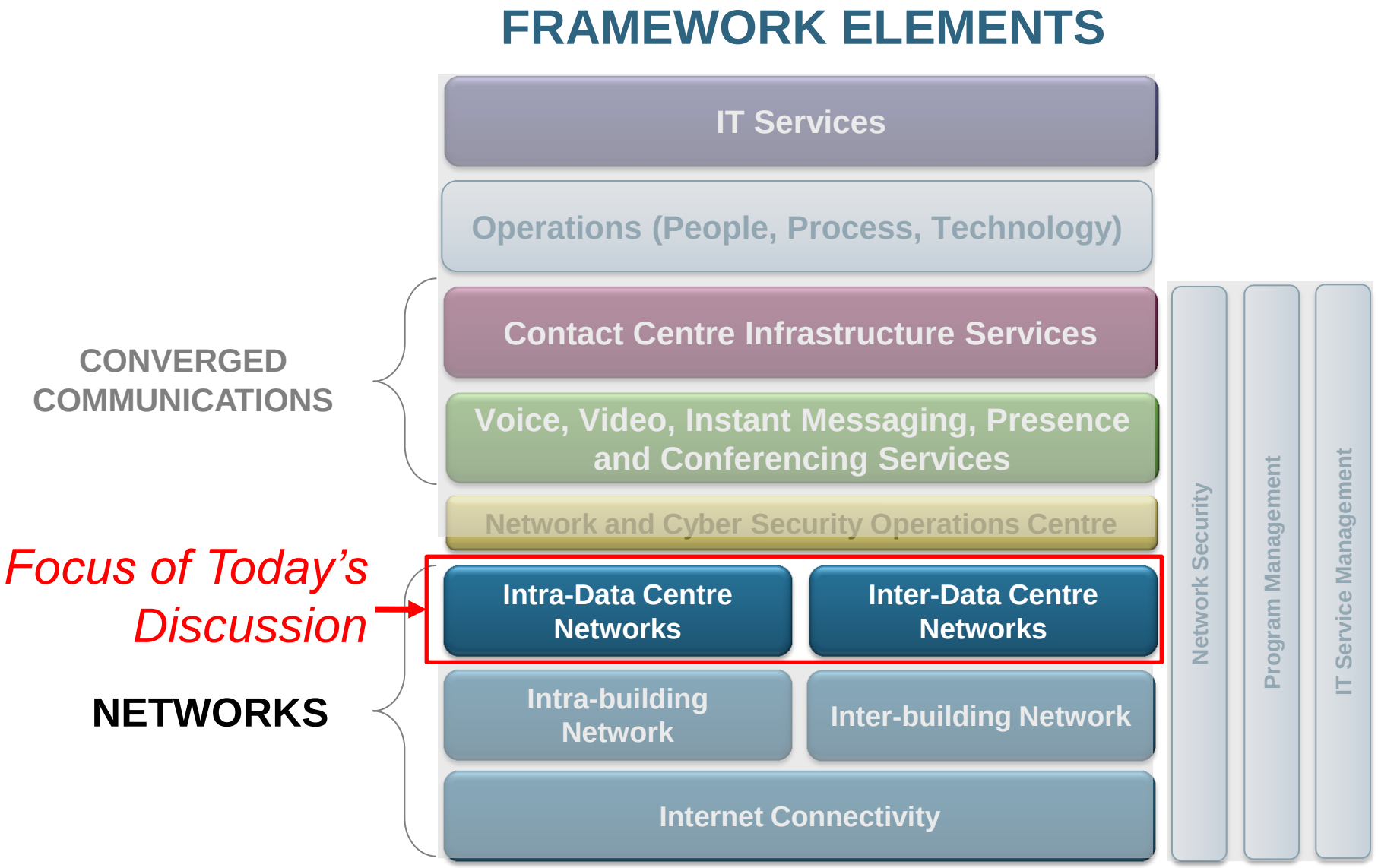
What is the TTP?

- The TTP is responsible for the following:
  - The **transformation, planning and sourcing of telecommunications services** for the Government of Canada
  - The **strategies** for delivering those services, with a view to centralize their administration, rationalize service delivery to achieve greater efficiencies, reduce costs, minimize risks, and improve security and service quality
- One of the main objectives of the TTP is to **design and build an integrated telecommunications network** to support Government of Canada operations
- The TTP is comprised of many service elements with the principle elements being inter-building networks, local area networks, **data centre networks,** workplace communications services, videoconferencing and contact centre infrastructure services



Telecommunications Transformation Program

Conceptual Framework



Telecommunications Transformation Program

What is "Data Centre Networks"?

"Data Centre Networks" is an umbrella term that SSC uses to refer to the two(2) streams: Inter-Data Centre Networks and Intra-Data Centre Networks

1. **Inter-Data Centre Networks:** provides high capacity network **connectivity *between* data centres** to ensure **high availability** of mission-critical applications, as well as support for **business continuity**

2. **Intra-Data Centre Networks:** provides secure, low-latency connectivity between compute and storage devices ***within* each data centre**

Inter-Data Centre Networks

Overview

Inter-Data Centre Networks Overview

Purpose / Context

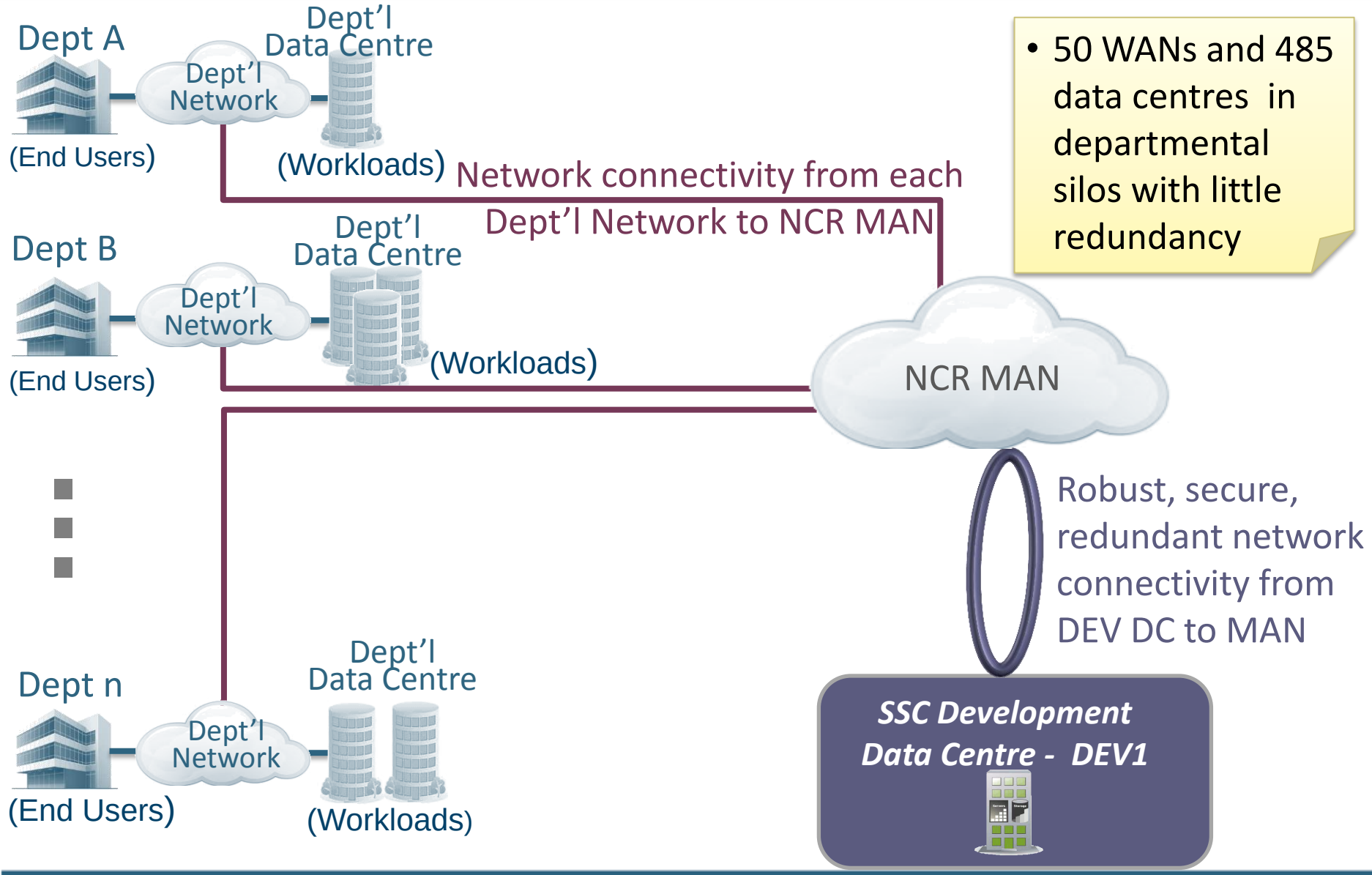
The Inter-Data Centre Networks will be used to provide high-capacity network connectivity within Canada:

- **To provide connectivity between enterprise Data Centres within pairs** to allow them to operate in tandem with duplicated / synchronized computing and storage infrastructure providing workload sharing and a highly available environment

- **To provide connectivity between enterprise Data Centre pairs** to provide backup, disaster recovery and business continuity

Inter-Data Centre Networks Overview

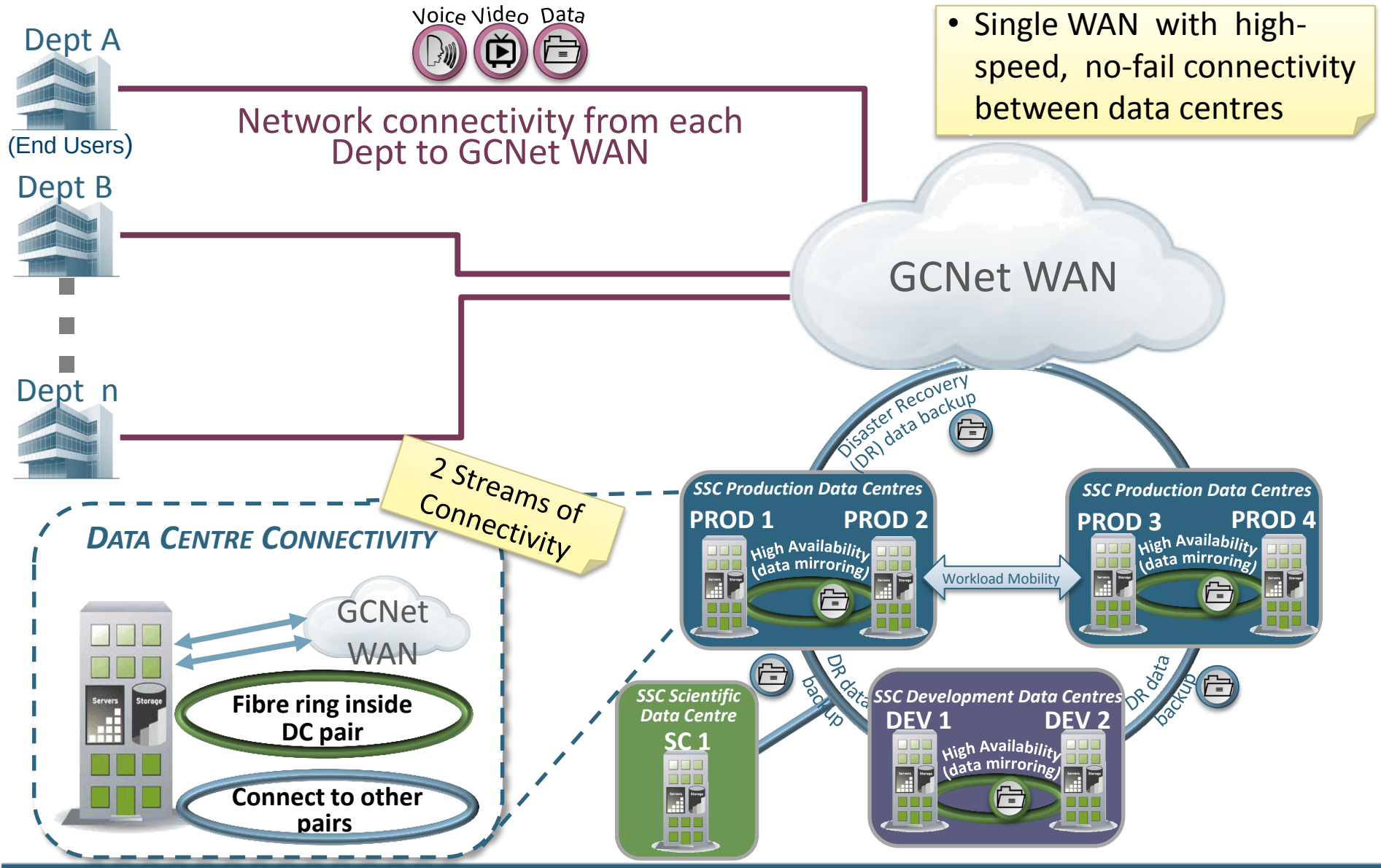
Current State



- 50 WANs and 485 data centres in departmental silos with little redundancy

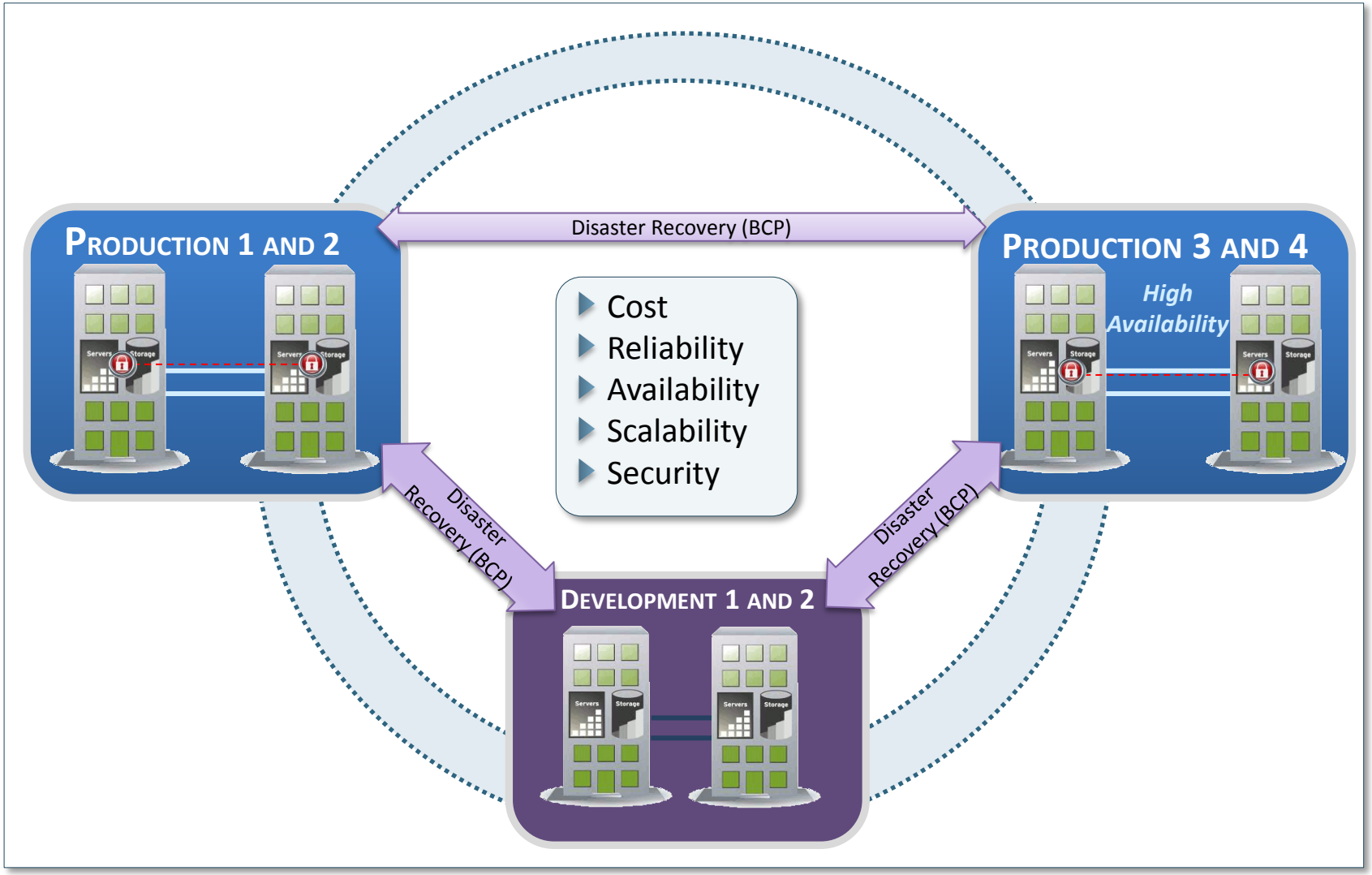
Inter-Data Centre Networks Overview

Target End State



Inter-Data Centre Networks Overview

Target State - Connectivity between Pairs

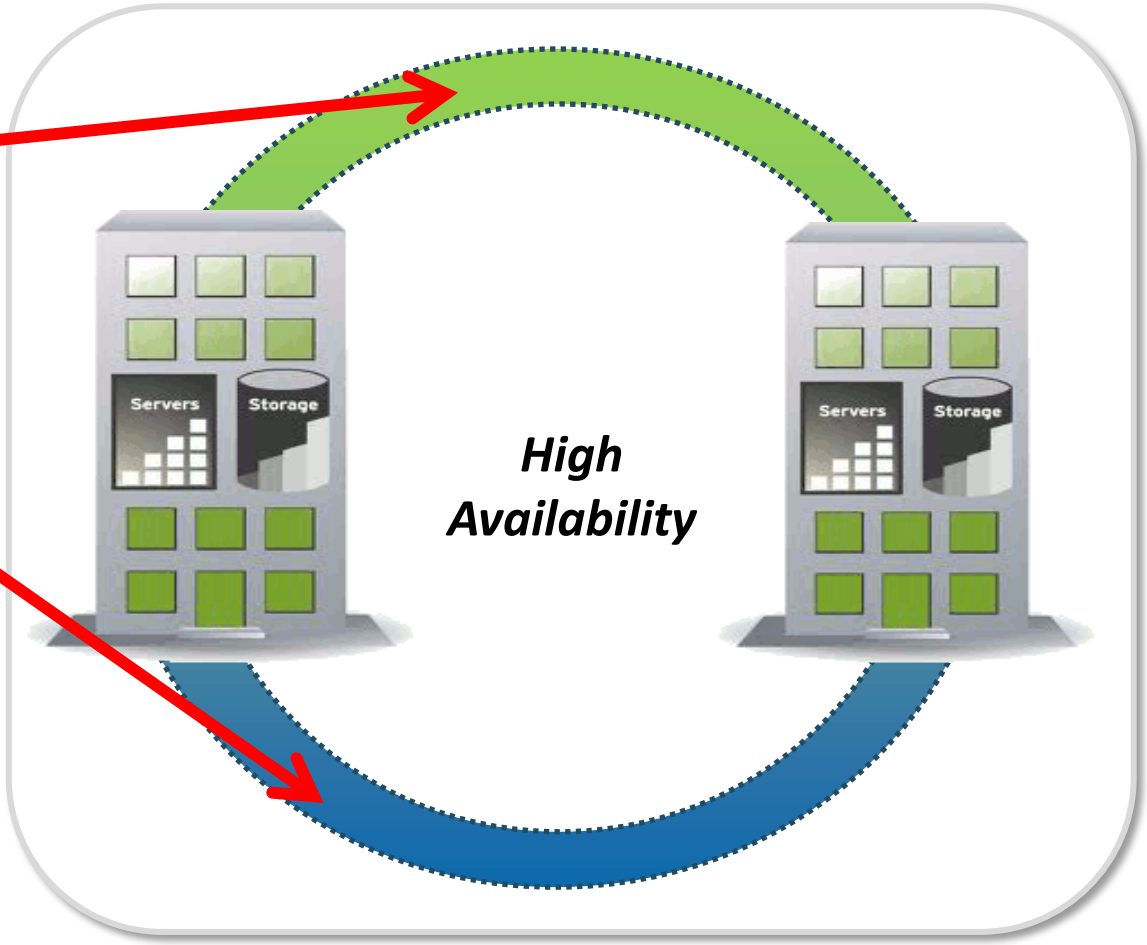


Inter-Data Centre Networks Overview

Target State - Connectivity between DCs within each pair

- The Data Centre Network within each pair is to provide capacity, agility and flexibility required by Enterprise High Availability applications

Two different service providers with two different paths



Inter Data Centre Networks Overview

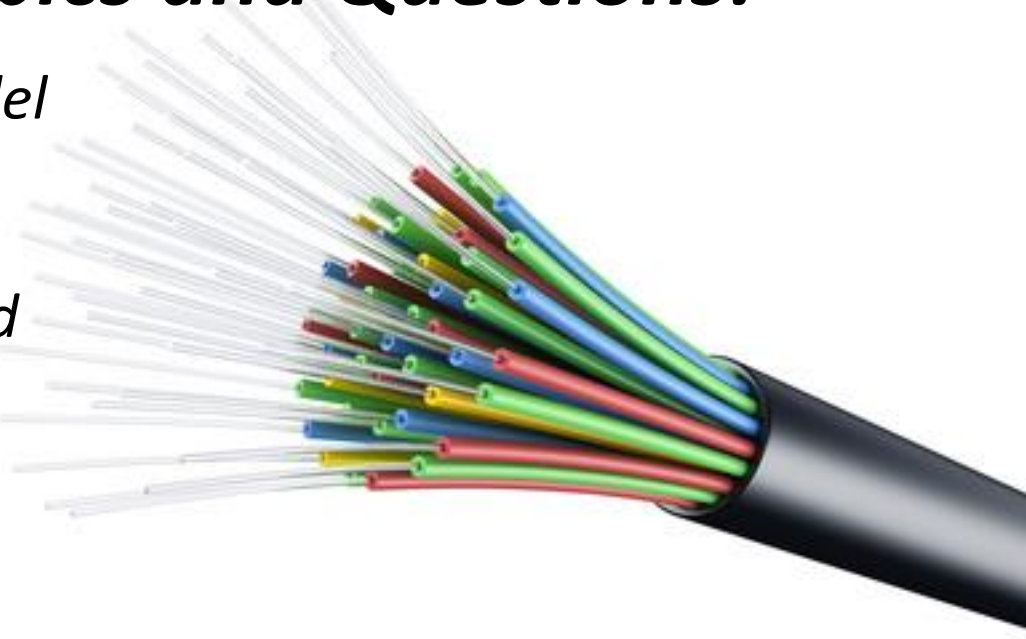
End State Requirements

- High-capacity, high availability Open Systems Interconnection (OSI) Layer 2 /Layer 3 services between Data Centres
- Service levels for applications and services requiring real-time sensitive networking (e.g. availability, latency, jitter)
- Traffic isolation and network resource tracking differentiated by security levels
- Compatibility with deployed and anticipated network technologies and protocols
- Monitoring capability to allow real time and historical analysis of network traffic and performance

Inter-Data Centre Networks

Key Discussion Topics and Questions:

1. *Deployment Model*
2. *High Availability*
3. *Contract(s) Period*



Inter-Data Centre Networks Discussion Topics

Deployment Model – Considerations

Discussion Topic 1

- What are the **benefits, technical challenges**, **requirements** and **recommended pricing model** for successful deployment and ongoing support of each deployment model?

1 *Outsourced / Fully Managed*

Third parties design, provide and operate the solution(s) through a managed service

EXAMPLE:
Lease fibre and infrastructure through a managed service and out-source design and operations

2 *Co-Managed / Hybrid*

SSC in-house resources deliver parts of the service on GC-owned infrastructure while the remainder is delivered by a third party vendor

EXAMPLE:
Buy infrastructure and lease dark fibre through a managed service and SSC in-house resources design and operate solutions

3 *In-sourced / In-House*

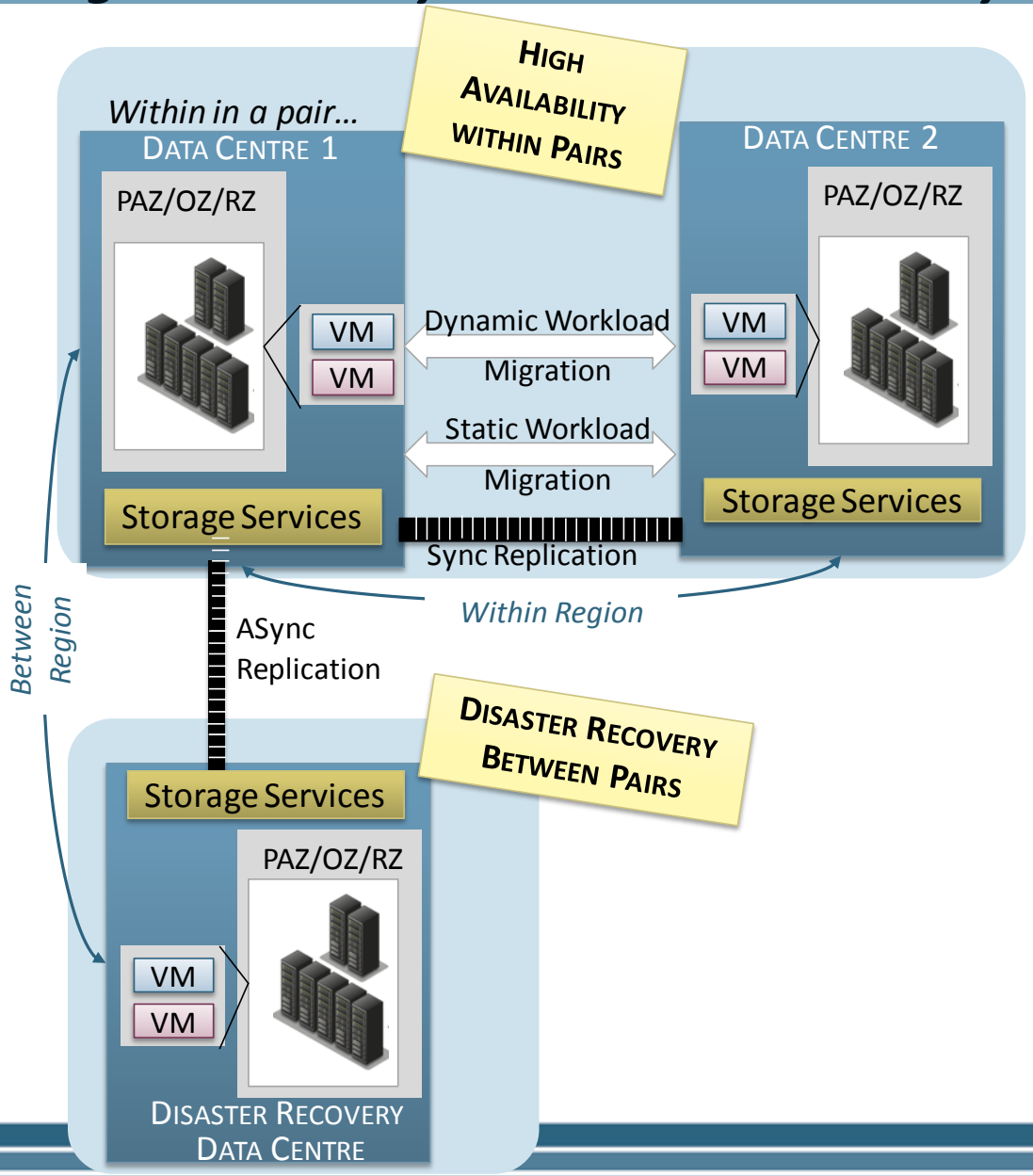
Design and deliver the solution by in-house SSC resources using SSC acquired infrastructure components

EXAMPLE:
Buy or lease fibre and/or infrastructure, and SSC in-house resources build and operate solutions

Inter-Data Centre Networks Discussion Topics

High Availability and Disaster Recovery

Discussion Topic 2



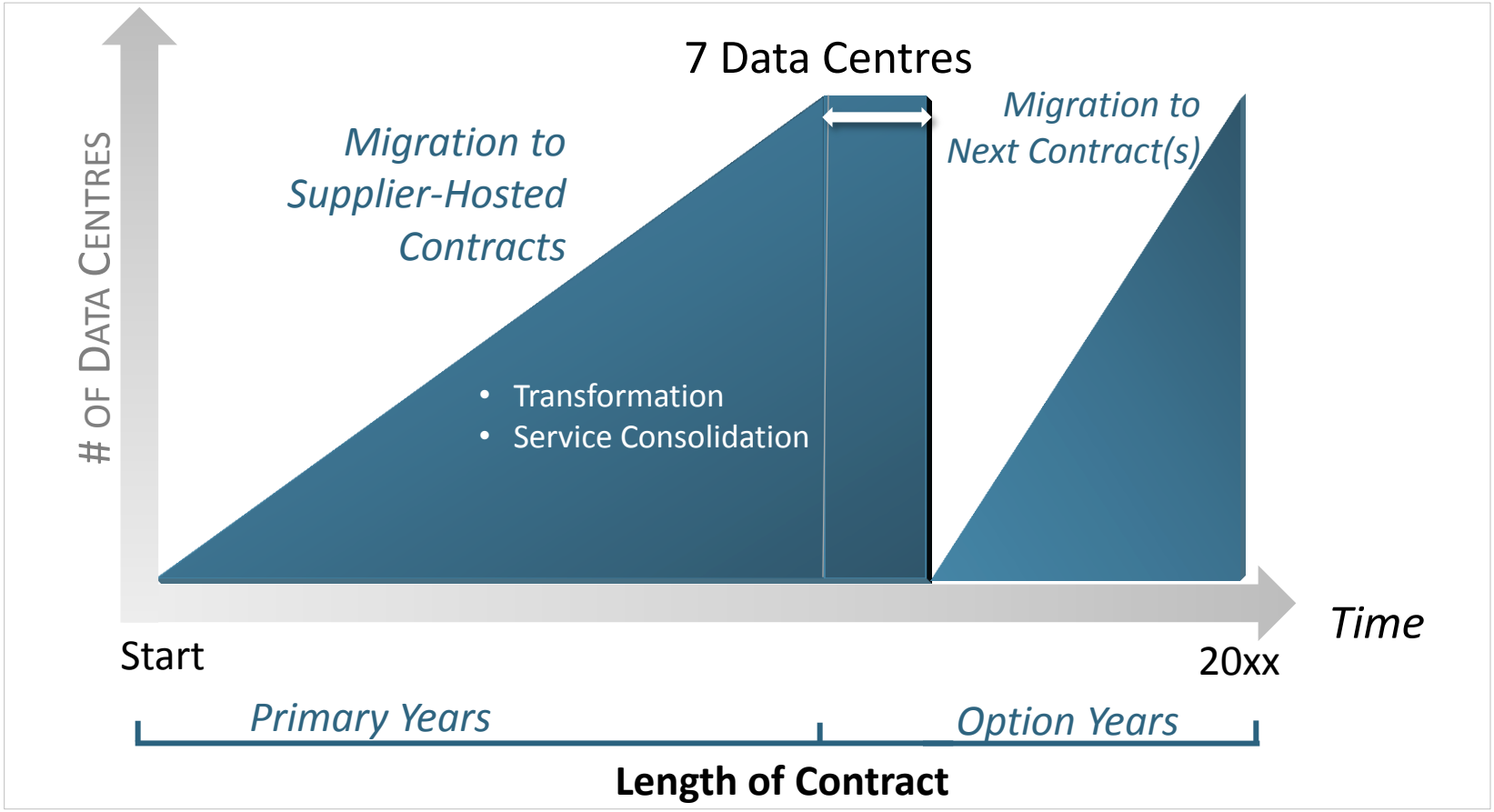
1. For high availability, are two suppliers recommended for the "no fail" connections between the paired Data Centres (DCs)?
2. What is the maximum distance allowed between DCs to deliver High Availability services and meet service levels?
3. What is the recommended architecture for connecting a DC pair?
4. How would you address the Disaster Recovery/Business Continuity requirements between the DC pairs?

Inter-Data Centre Networks Discussion Topics

Contract Period

Discussion Topic 3

- Recommended contract length(s) (including option years)?



Inter-Data Centre Networks Discussion Topics

Key Questions for Industry Feedback

OPERATIONAL/TECHNICAL:

1. For high availability, are two suppliers recommended for the “no fail” connections between the paired DCs?

2. What other measures, other than redundant links, should the Crown look at to safeguard the integrity of the data between the data centres (encryption and various security levels)? What are the impacts of using encryption on an inter-data centre link?

3. What are the recommended service levels for these links and the cost implications?

4. Are there technical restrictions or limitations with respect to the type of data being transmitted/ exchanged over these links ?

Inter-Data Centre Networks Discussion Topics

Key Questions for Industry Feedback *(continued)*

OPERATIONAL/TECHNICAL:

5. What footprint would you require at our DCs for your equipment?

6. What is the maximum distance recommended between High Availability DCs to deliver services and meet service levels?

7. What value-added services (if any) would you recommend being incorporated?

Inter-Data Centre Networks Discussion Topics

Key Questions for Industry Feedback *(continued)*

PROCUREMENT:

1. What are the technical challenges and recommended pricing model for a successful deployment and ongoing support of a fully managed (out-sourced) Inter-DCN?

2. What are the pros and cons of a fully managed vs. hybrid vs. in house model Inter-DCN?

3. Identify the advantages and disadvantages for:
   - Buying fibre and infrastructure, and building and operating solutions in-house
   - Buying infrastructure and leasing dark fibre through a managed service and designing and operating in-house
   - Leasing fibre and infrastructure through a managed service and out-sourcing design and operations

Inter-Data Centre Networks Discussion Topics

Key Questions for Industry Feedback (continued)

PROCUREMENT:

4. Please provide your recommendations on contract length. What are the advantages and disadvantages with this duration? What Pricing Model would be most beneficial to Canada? Are regular pricing reviews at fixed intervals over the period of contract(s) advisable?

5. Provide recommendations for requirements to maximize competitiveness and minimize costs. What are the factors that drive rates up?

6. What recommendations can be provided on the approach for the technical evaluation of supplier proposals?

Break – 15 Minutes

Coffee and refreshments are available in the lobby.

Please return to your seat by 3:00 p.m.

Intra-Data Centre Networks

Overview

Intra-Data Centre Networks Overview

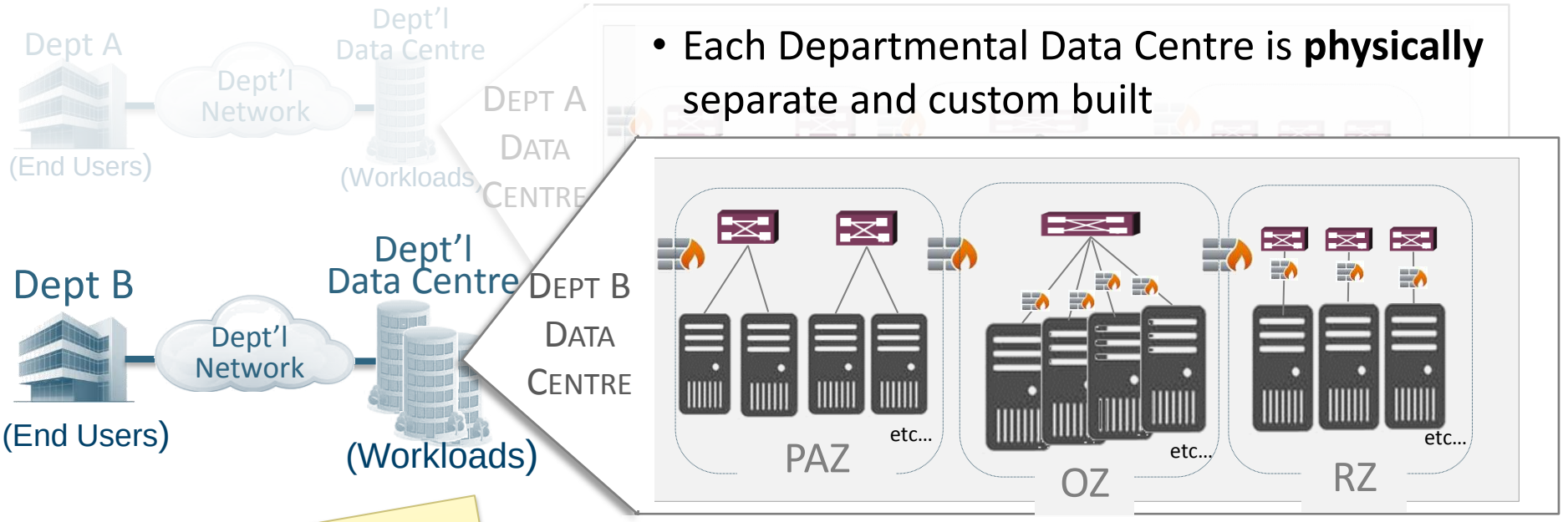
Purpose / Context

- The Intra-DC Network plays a critical role in the evolution of the SSC Data Centre and will:
  - Provide a transport service to the data centre and foundational elements
  - Provide users with access to on-demand data centre services and resources through a virtualized network infrastructure
  - Provide a secure technology infrastructure and environment to meet program needs and increase confidentiality and integrity of information
- The Intra-DC Network will be fully established in alignment with current Data Centre Consolidation Plans

Network infrastructure needs to be reliable, scalable, resilient and highly available

Intra-Data Centre Networks Overview

Current State



- Each Departmental Data Centre is **physically** separate and custom built

- 50 WANs and 485 data centres in departmental silos with little redundancy

- Common Characteristics / Issues:
  - Physical Redundancy and Separation
  - Duplication / Replication
  - Frequent under utilisation
  - Non Standard architecture, equipment, etc…
  - Separate physical firewalls and load balancers

LEGEND:

PAZ = Public Access Zone
OZ = Operational Zone
RZ = Restricted Zone

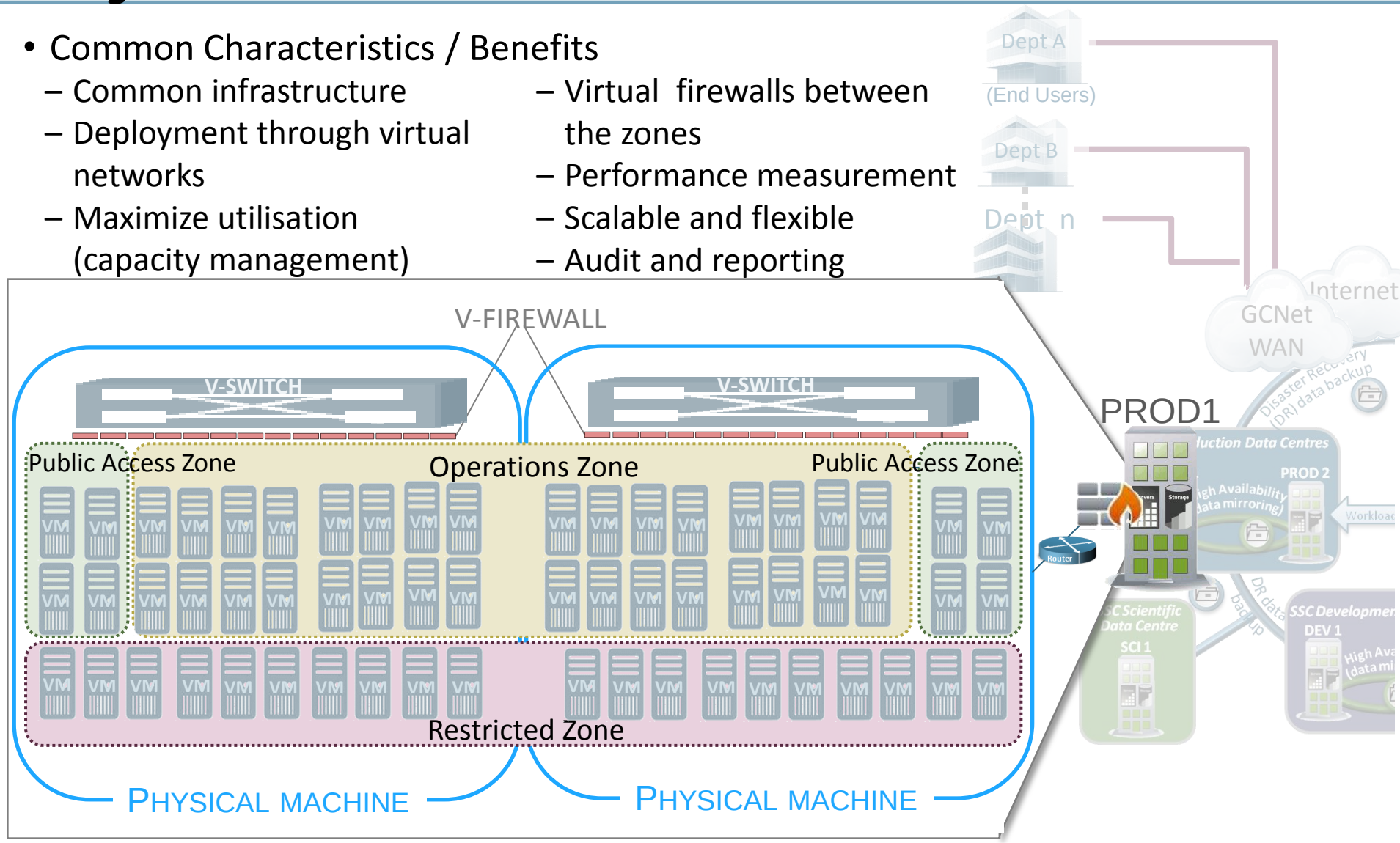
Switch
Processor
Firewall

Dept'l Network
Provides connectivity within single department (multiple sites)

Intra-Data Centre Networks Overview

Target State - Virtualized Environment

- Common Characteristics / Benefits
  - Common infrastructure
  - Deployment through virtual networks
  - Maximize utilisation (capacity management)
  - Virtual firewalls between the zones
  - Performance measurement
  - Scalable and flexible
  - Audit and reporting



Intra Data Centre Networks Overview

End State Requirements

- Provide network access to business workloads, Internet access, shared applications in cost-effective and secure manner
- Infrastructure must be flexible, scalable and “future proof”
- Must support multi-tenancy and controlled access to data (must provide capability to have organizations/users access virtual slices of compute, storage and network that are kept private from other organizations/users)
- Support an open architecture to ensure flexibility and compatibility

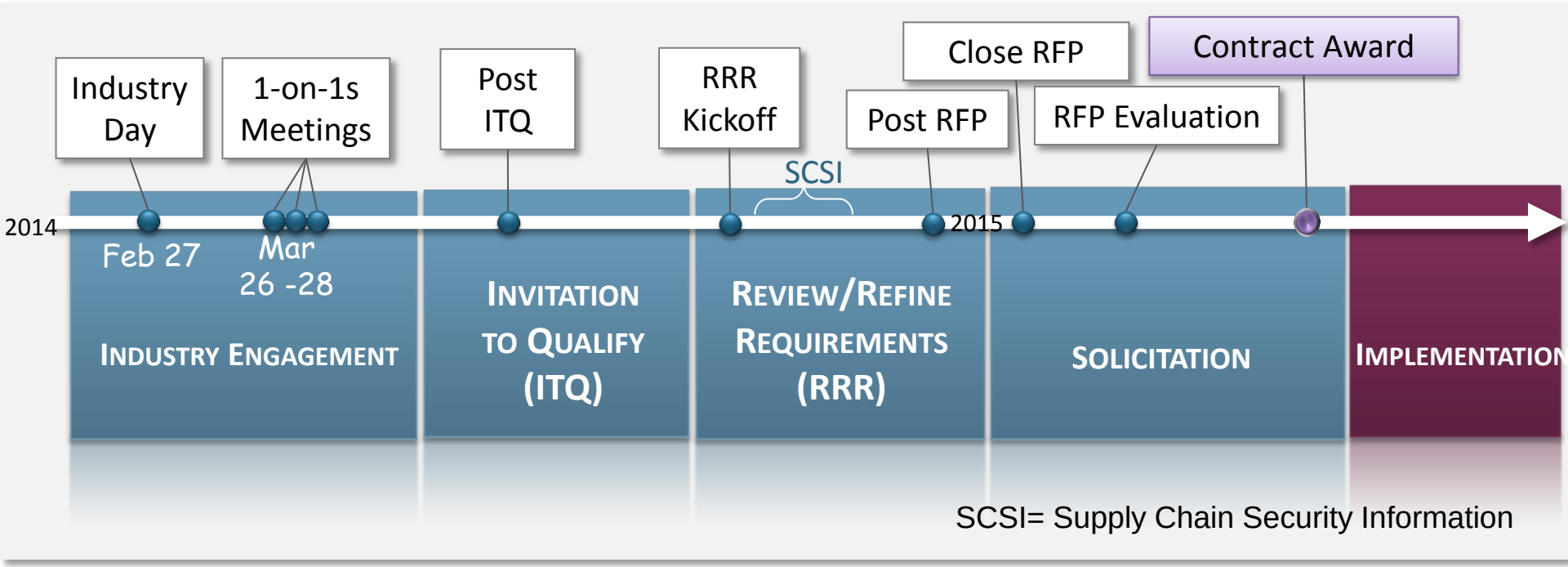
Intra Data Centre Networks Overview

End State Requirements *(continued)*

- Provide high availability access to IT systems, applications and information and provide IT Service and Business Continuity for mission critical applications
- Network equipment must be able to support cloud services and service virtualization
- Support the ability for orchestrating deployment of compute and storage services
- Flexible and responsive network infrastructure to meet changing business needs including the ability to dynamically adapt to meet network traffic demand

Data Centre Networks Overview

Procurement Timeline to Contract Award(s)



- Both streams of Data Centre Networks (Inter and Intra) will align with the proposed procurement schedule, but will be considered separate procurements

- Supply Chain Security Information (SCSI) assessment will be conducted during the RRR phase to ensure all IT Products meet Canada's security and supply chain standards (more detail will be provided in the following SCSI presentation)

Intra-Data Centre Networks

Key Discussion Topics and Questions:

1. Deployment Model
2. Emerging Technologies
3. Pricing Methodology
4. Contract(s) Period

Intra-Data Centre Networks Discussion Topics

Deployment Model

Discussion Topic 1

- What are the **benefits, technical challenges**, **requirements** and **recommended pricing model** for successful deployment and ongoing support of each deployment model?

1 *Outsourced / Fully Managed*

A third party designs, implements and operates the solution in GC Data Centres

EXAMPLE:
Third party vendor provides infrastructure components, designs, implements and operates solution

2 *Co-Managed / Hybrid*

SSC in-house resources deliver parts of the service on GC-owned infrastructure while the remainder is delivered by a third party vendor

EXAMPLE:
Solution delivered by third party vendor and SSC in-house resources implement and operate

3 *Insourced / In-House*

Solution designed and delivered by in-house SSC resources using SSC acquired infrastructure components

EXAMPLE:
Buy infrastructure components/solution and SSC in-house resources build and operate it

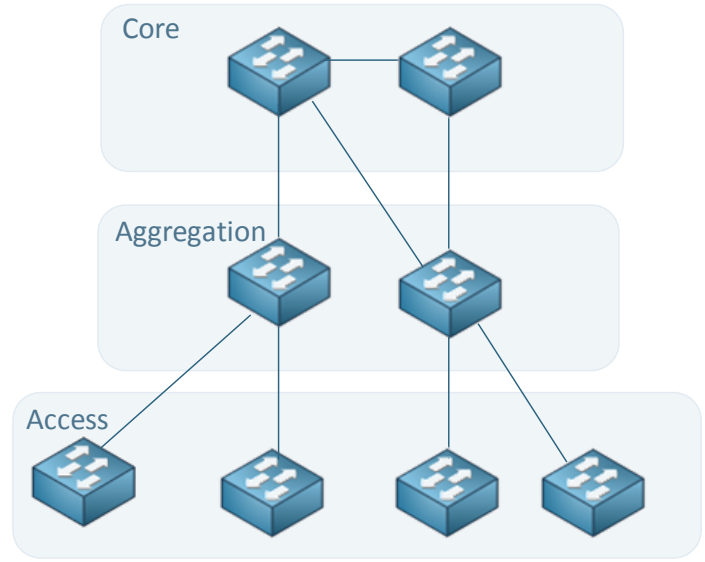
Intra-Data Centre Networks Discussion Topics

Emerging Technologies

Discussion Topic 2

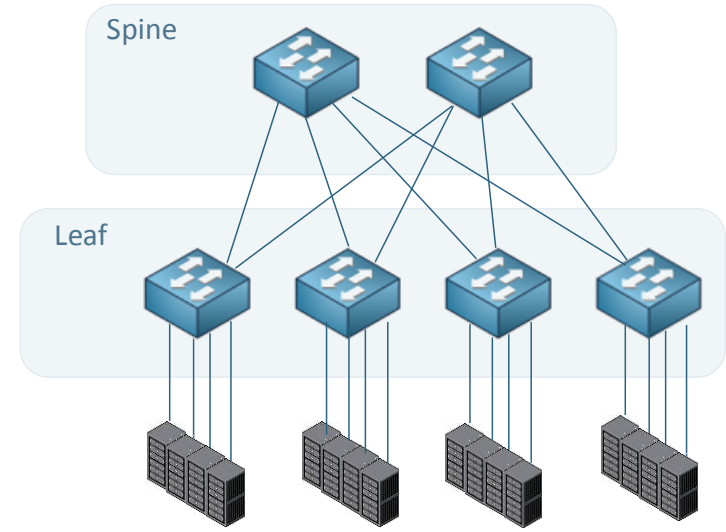
- To ensure “future proofing”, what are the possible technology or service enhancements over the next 5 to 10 years that need to be considered?
- Are the services and equipment scalable and able to support future Software Defined Network (SDN) requirements, and how?
- How can we keep technologies up to date given the length of transformation?
- What are the implications if there is a requirement to have an identical solution in each of the data centre pair?

3 Tier Infrastructure



VERSUS

Leaf and Spine Infrastructure

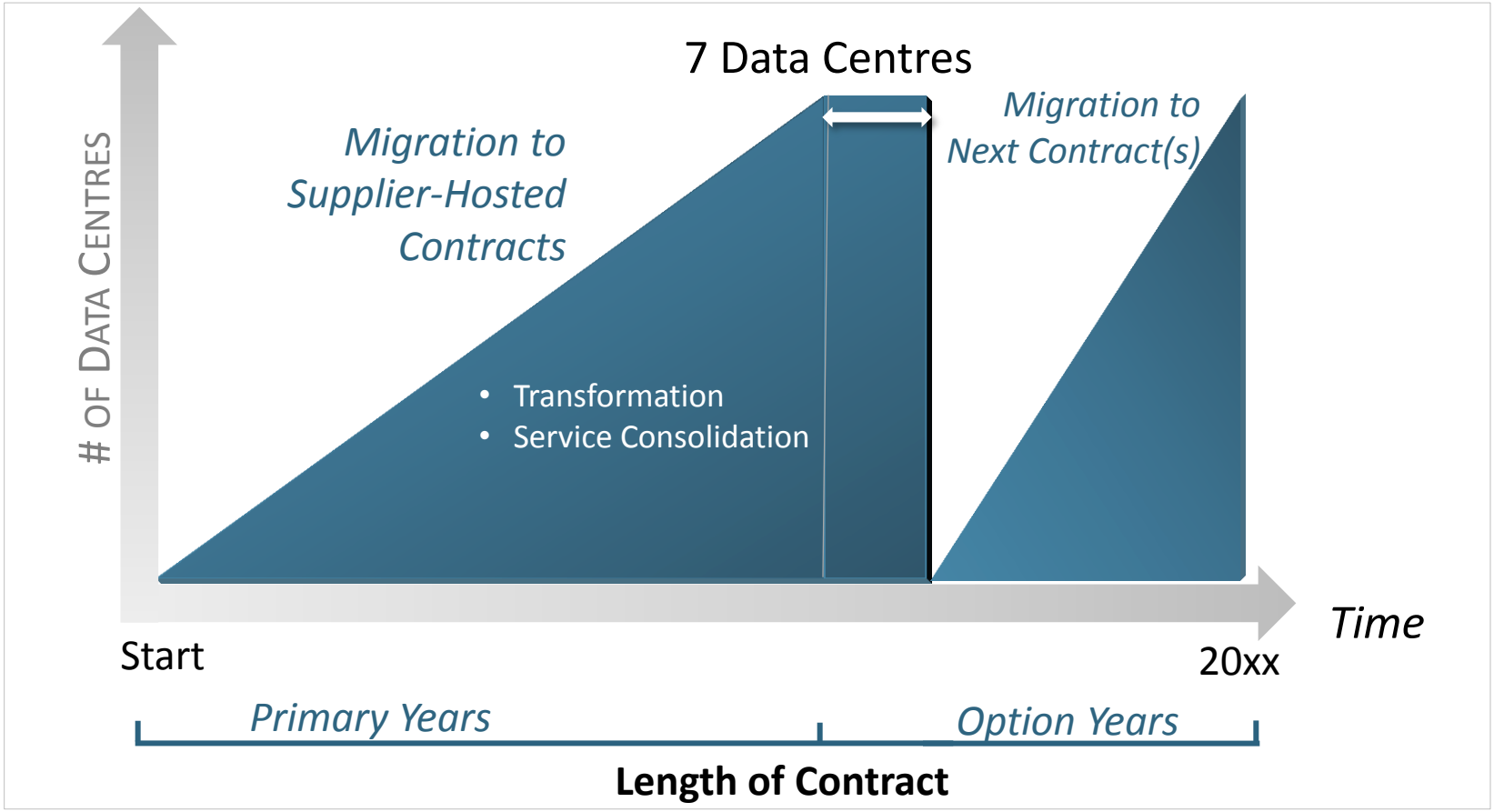


Intra-Data Centre Networks Discussion Topics

Contract Period

Discussion Topic 3

- Recommended contract length(s) (including option years)?

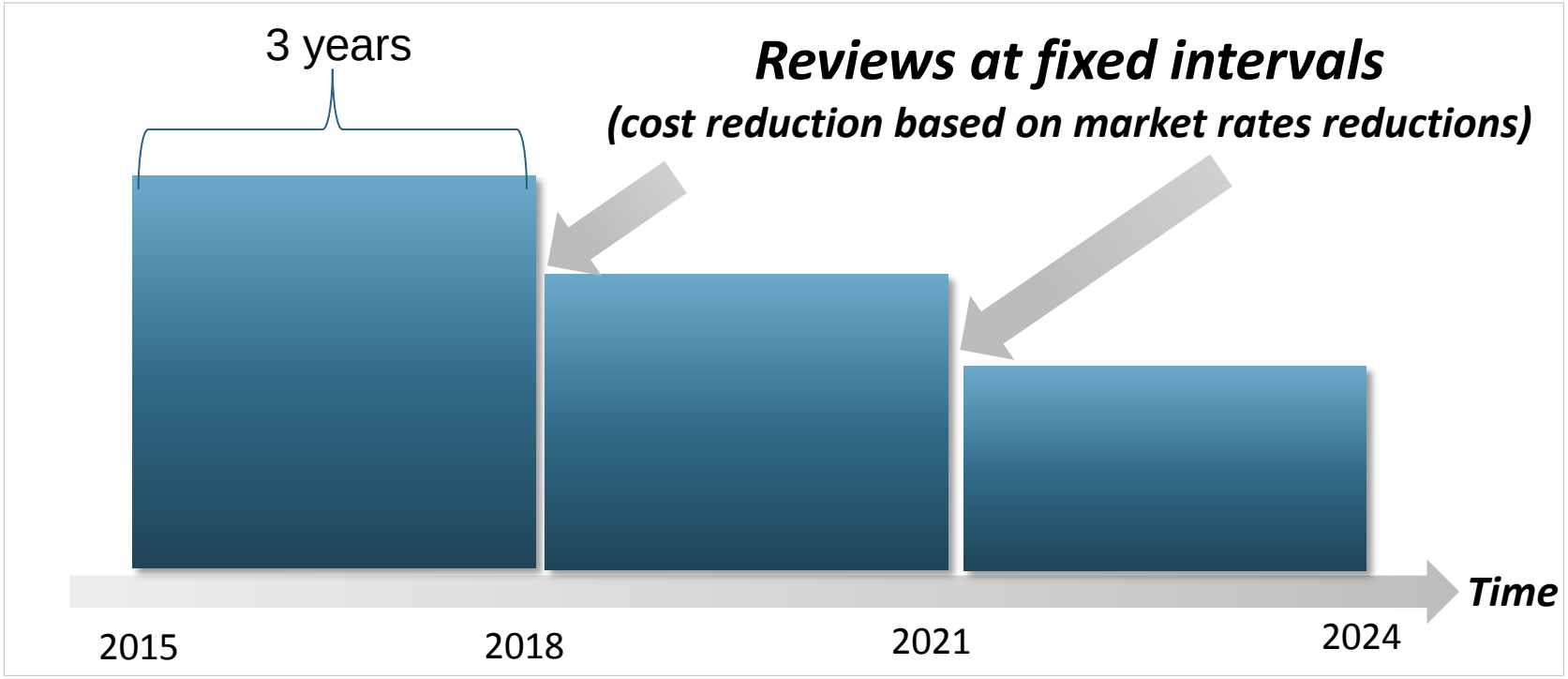


Intra-Data Centre Networks Discussion Topics

Pricing Model Options

Discussion Topic 4

- Numerous pricing model options possible (fixed, variable, etc.)
- Are pricing reviews at fixed intervals (based on market benchmarks) over the period of contract(s) advisable?
- What are the factors that drive the rates up?



Intra-Data Centre Networks Discussion Topics

Key Questions for Industry Feedback

OPERATIONAL/TECHNICAL:

1. Can services be provided by multiple suppliers using multiple vendors' equipment within DC pairs (High Availability)? Across DC pairs (Business Continuity)? Is it a recommended approach ?

2. Are the services and equipment scalable and able to support future Software Defined Network (SDN) requirements, and how?

3. What are the possible technology or service enhancements over the next 5 to 10 years that we may need to consider in our requirements? How can emerging trends/technologies be incorporated into the proposed solutions? How can we keep technologies up to date given the length of transformation?

Intra-Data Centre Networks Discussion Topics

Key Questions for Industry Feedback *(continued)*

OPERATIONAL/TECHNICAL:

4. What service delivery model would you recommend and why ?

5. What value-added services would you recommend that we should be incorporating?

6. What are some of the strategies to migrate from today's environment to the future environment?

7. What are the perceived barriers to success and risks that require mitigation strategies?

Intra-Data Centre Networks Discussion Topics

Key Questions for Industry Feedback (continued)

PROCUREMENT :

1. What are the technical challenges and recommended pricing model for successful deployment and ongoing support of a fully managed Intra-DCN ?

2. What are the pros and cons of a fully managed vs. hybrid vs. in-sourced model (including hardware and software)? What are some security implications of a hybrid model?

3. For the hybrid or in-sourced models, please comment on the approach of buying/leasing a solution, rather than equipment. What are the pros and cons of buying vs. leasing a solution/equipment (particularly in the case of in-sourced services)?

4. Provide feedback on the ability to inter-operate based on industry "open" standards within a multi-vendor network services integration. What are the technical challenges when it comes to management?
   - In-house managed
   - Out-sourced managed

Intra-Data Centre Networks Discussion Topics

Key Questions for Industry Feedback (continued)

PROCUREMENT :

5. Provide feedback on proposed procurement approach and timelines, considering existing systems and services

6. Should we have only one prime provider for all enterprise data centres?

7. What Pricing Model would be most beneficial to Canada? Are regular pricing reviews at fixed intervals over the period of contract(s) advisable?

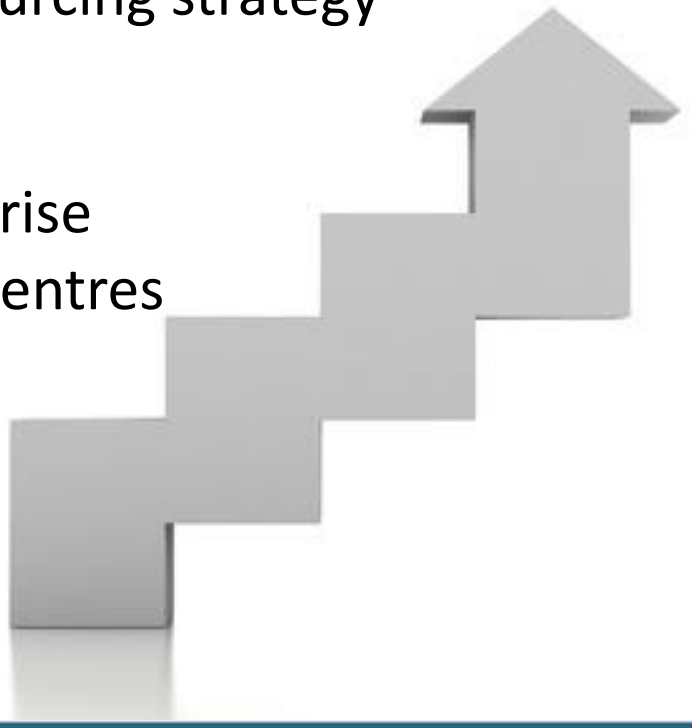
8. What recommendations can be provided on the approach for the technical evaluation of supplier proposals?

9. Provide views or feedback on proposed procurement timelines

Data Centre Networks Industry Engagement

Next Steps

- Industry one-on-one engagements will be held March 26th - 28th to obtain feedback on the discussion topics
- Evaluate input feedback received to refine inter and intra data centre procurement and sourcing strategy
- Proceed with procurement for enterprise solutions to support enterprise data centres in a timely manner



Data Centre Networks Industry Engagement

Wrap Up and Questions

Questions?

(for suppliers only)

Cyber & Supply Chain Threats to the GC

Data Centre Networks
Industry Day

February 27, 2014

Brad McInnis, Communications Security Establishment Canada

Canada

CSEC: What We Do

- CSEC: Canada's national cryptologic agency
- Our Mandate
  - Foreign Signals Intelligence
  - IT Security
  - Support to Lawful Access
- 'B' Mandate
  - To provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada

CSEC: IT Security Program

- We help prevent, detect and defend against IT security threats and vulnerabilities
- CSEC provides unique technical expertise, capabilities and classified information that we use to complement commercial security technologies available to IT security practitioners
- We use our own methods and operations to detect and defend against threats that are not in the public domain

Effects of Market Forces on Technology

- Market forces favour commercial and personal technologies over requirements for security features
- Our society is almost totally dependent on software and hardware commercial technology providers from global markets
- New products and new versions of products are rapidly produced
- No regulatory framework exists for hardware/software safety and security
- Traditional government policies and processes impose security requirements after products and systems have been developed
- Few incentives for commercial technology developers to invest in security

Technology Vulnerabilities

- **"People write software sloppily. Nobody checks it for mistakes before it gets sold"**
  - **Peiter Zatko (Mudge), WhiteHouse Cyber-Security Summit (2000)**

- **Unintentional vulnerabilities or weaknesses**
  - **Design flaws**
  - **Implementation errors**

- **Cyber Threat – A threat actor, using the Internet, takes advantage of a known vulnerability in a product for the purpose of exploiting a network and the information the network carries**

- **Intentional vulnerabilities or weaknesses**
  - **Predetermined deliverables can be implanted in a product with or without knowledge of company.**

- **Supply Chain Threat – a product can be easily tampered with in the supply chain to later facilitate a cyber-intrusion against that product in order to exploit a network and the information the network carries**

The Evolving Cyber-Threat

- Today, malicious cyber activities are directed against Canada and our closest allies on a daily basis

- Threat actors range in sophistication from malfeasant hackers to organized crime groups, to terrorists to nation states

- Canadians trust the GC to defend Canada's cyber sovereignty and protect and advance our national security and economic interests

An Issue of National Security

- Risks from vulnerable technologies
  - **Covert and persistent access by cyber threat actors in GC departmental networks threatens the sovereignty of GC information and the continuity of government operations**
  - **Cyber threat actors are effective at exploiting inter/intra-connected network element technologies and management systems used to administer and operate network infrastructures**

- Risks from an overly complex and decentralized threat surface
  - **Consolidation of GC telecommunications services through GCNet WAN is a prerequisite for manageable cyber protection & defence**
  - **Security through obscurity is not a viable long-term strategy to deter cyber threat actors**

- Risks from the supply chain
  - **Increases opportunities for threat actors to circumvent GC cyber security measures**
  - **More difficult for the GC to detect and remediate**

GC Shared Services Procurements

- Shared Services Canada and CSEC are working in partnership to eliminate or significantly reduce risks to the GC from cyber threats & global supply chain vulnerabilities

- CSEC will provide follow-up briefings on supply chain risk mitigation to interested suppliers for GC shared services
  - Companies must be willing to sign a CSEC non-disclosure agreement to receive this information

- Security requirements for cyber-protection, cyber-defence and supply chain risk mitigation must be met by suppliers in order to successfully bid on GC shared services initiatives
  - As the IT Security authority for the GC, CSEC will seek long-term partnerships with successful suppliers
  - CSEC will assist Shared Services Canada in the pedigree analysis of supply chain information provided by respondents

- Examples of these requirements can be found on CSEC's website under Technology Supply Chain Guidance

Service | Innovation | Value

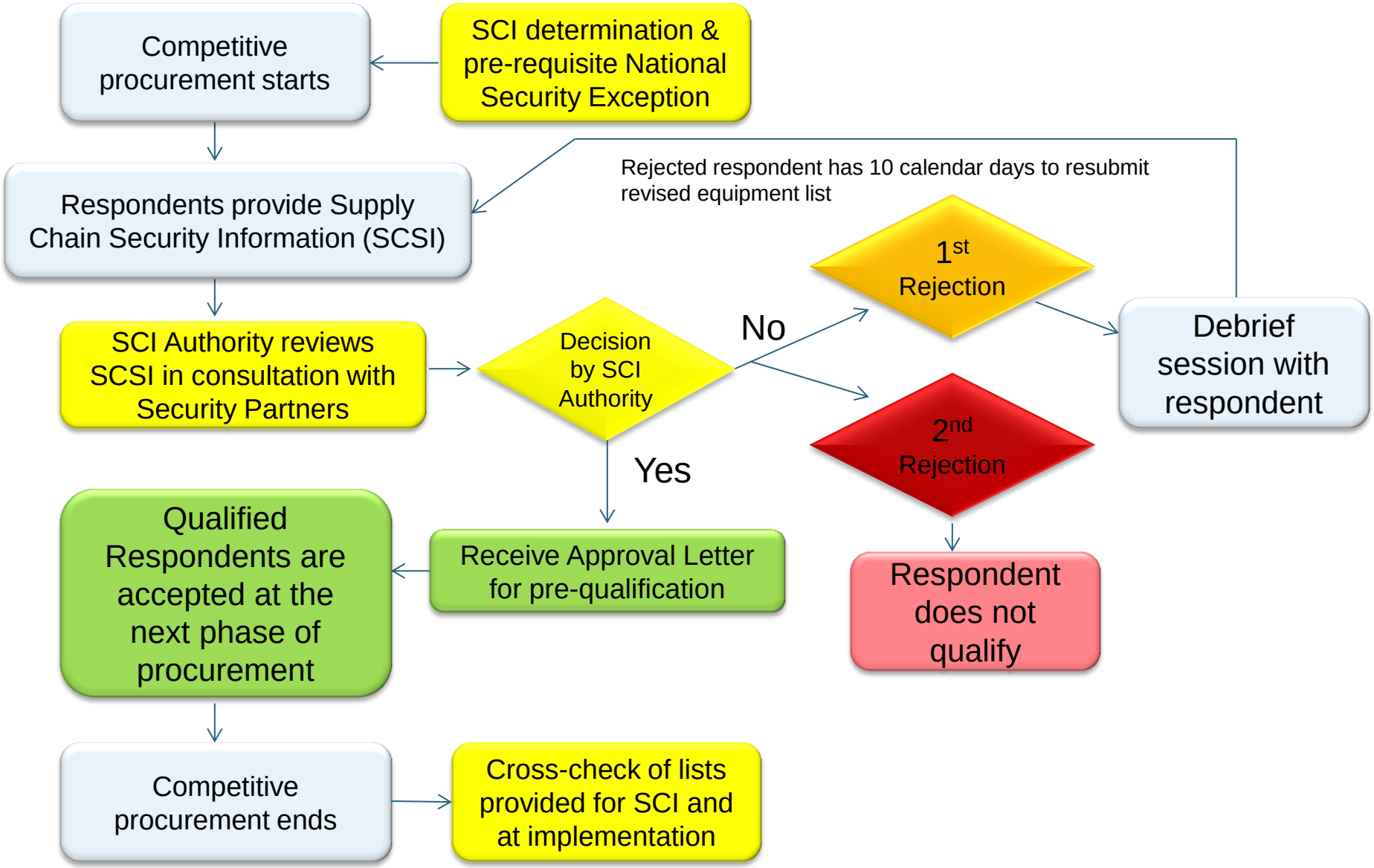
Supply Chain Integrity (SCI)

Data Centre Networks Industry Engagement Day

February 27th, 2014

Raj Thuppal, Director General, Cyber and IT Security Transformation Program

SCI in Competitive Procurement



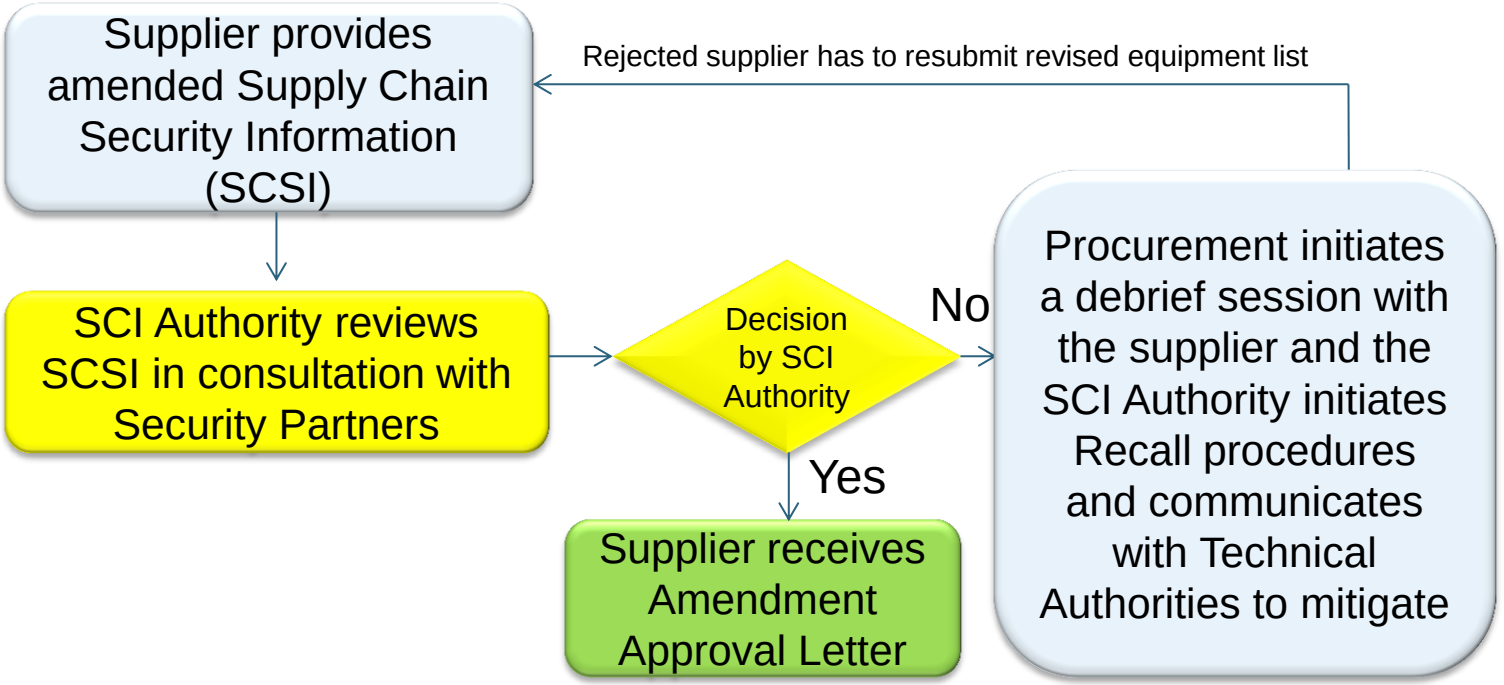
Required Information from the Respondents

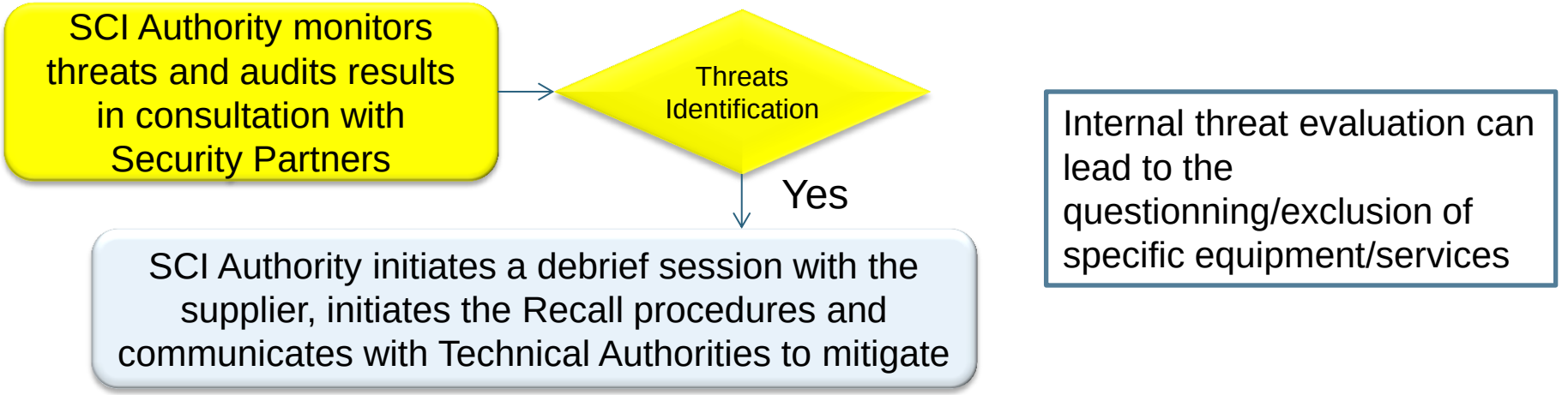
- Once the SOW is finalized, GC will request that the respondents provide their Supply Chain Security Information. More specifically, when it applies, the GC will be requesting the following detailed information:

1. List of equipment used to deliver the service (vendor, manufacturer, model number, software load version – to be determined).
2. List of subcontractors (names of companies and the location from where these services are delivered – to be determined).
3. Network diagrams (to be determined).
4. All of the above applies for sub-contractors and partners (sub-contractors and their own sub-contractors). This should include all companies who will be sub-contracted to provide equipment or services as part of the Data Centre Networks project.

On-going Supply Chain Integrity Auditing

On-going SCI auditing from the moment the contract has been awarded until it ends.





Internal threat evaluation can lead to the questionning/exclusion of specific equipment/services

Service | Innovation | Value

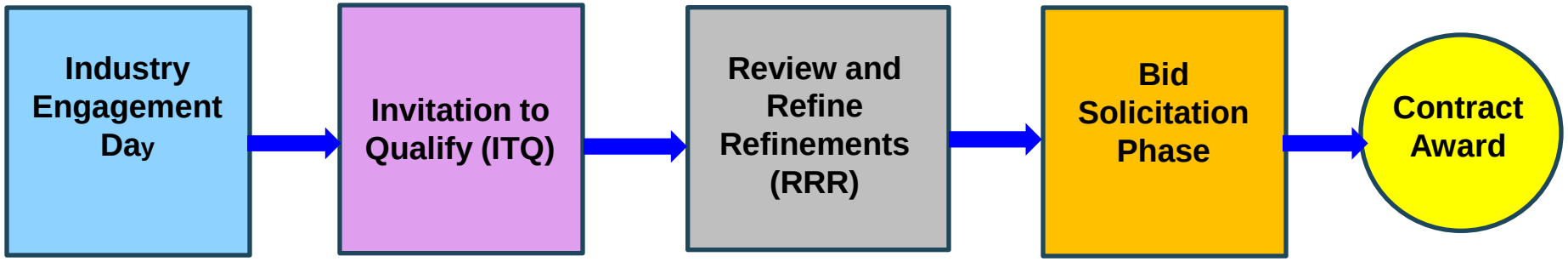
Data Centre Network Services

Collaborative Procurement Solutions Approach

Tom Mercer
Shared Services Canada
Manager
Procurement and Vendor Relationships Directorate

February 27, 2014

Collaborative Procurement Solutions Approach



Invitation to Qualify (ITQ)

Invitation to Qualify (ITQ) Phase

- The purpose is to qualify suppliers who have demonstrated and proven skills and experience in implementing and providing Data Centre Network (DCN) services for both Inter-Data Centre Networks and Intra-Data Centre Networks solutions.
- Evaluation criteria will focus on the supplier's capabilities and experience to deliver DCN services.
- Suppliers who meet the mandatory ITQ evaluation criteria will be deemed successful "Qualified Respondents (QRS) and will proceed to the RRR phase.
- Canada will inform Qualified Respondents that, in the "Review and Refine Requirements Phase", a draft Statement of Work (SOW) will be provided to them and at that time.

Review and Refine Requirements (RRR)

Review and Refine Requirements (RRR) Phase

- Canada will provide the Qualified Respondents with a draft RFP(s).
- Canada will interact with Qualified Respondents to seek feedback and clarification on Canada's requirements to refine the RFP(s) (e.g. workshops, one-on-one sessions, Q's and A's).
- A Supply Chain Security Information (SCSI) assessment will also be started during this stage.

Bid Solicitation Phase

Bid Solicitation Phase

- Canada may issue one or more formal Request for Proposal(s) (RFP(s)) to the Qualified Respondents who have participated in the ITQ and RRR Phases
- Each Qualified Respondent will be permitted to formally bid on the requirements set out in the RFP(s).

Contract Award

Contract Award and Implementation

- Contract Award will occur after completion of the Bid Solicitation Phase
- One or more contracts may be awarded depending on the Request for Proposal(s)

Service | Innovation | Value

Data Centre Networks Industry Day

Questions & Answers

Shared Services Canada | Services partagés Canada

Canada

Service | Innovation | Value

Data Centre Networks Industry Day

Recap / Closing Remarks

Shared Services Canada | Services partagés Canada

Canada