Resilient and Secure Platform

IPO Meeting on ICT Strategy and AI

K. Kalejs – Director PCT IS Division

Thursday, May 24, 2018
Current context

- A continuously evolving threat landscape for the PCT
RSP - Background

- **The PCT is a cornerstone**, it provides > 70% of revenue.
- **Resilience** of the PCT’s services is critical to the business operations of PCT applicants and Offices.
- **Service interruptions** have the potential to lead to backlogs at WIPO, as well as backlogs and/or loss of rights for WIPO’s customers.
- Medium to large scale **service disruptions** are likely to damage WIPO’s reputation and income.
- PCT infrastructure is sharing its core services with other WIPO corporate services. **Any potential threat impacting WIPO** (cyber-attack, natural disaster, major technical failure) **may therefore impact the PCT.**
RSP = Resilient and Secure Platform

- Capital Master Plan Approval for Phase I: 2018-2019 8 million CHF
- Increasing the security of the systems storing and processing WIPO’s sensitive and critical PCT data;
- Increasing the availability and resiliency of WIPO’s critical PCT business processes and related systems;
- Improving the data identification, classification and protection;
- Improving PCT’s ICT agility and adaptability
Current architecture

WIPO CORE SERVICES

Filing

Process

Publication

PCT DATA

IP Offices

Agent / Applicants
Data Centers

Current

DC 1

3 km

DC 2
Data Centers

Future

Nearby

PCT DC1

>40 km +

PCT DC2

WIPO PCT
**RSP Benefit realization plan**

<table>
<thead>
<tr>
<th>Projects</th>
<th>Outcomes</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEAR DC</td>
<td>Dedicated &amp; Isolated PCT Data Center</td>
<td>S1: Reduced likelihood of malicious or unintentional disclosure or modification of unpublished application/registration/patent information</td>
</tr>
<tr>
<td>APPLICATION MIGRATION</td>
<td>Secured Desktop</td>
<td>S2: Reduced likelihood of cyber-attacks and reduction of impact from a successful cyber-attack</td>
</tr>
<tr>
<td>FAR DC</td>
<td>Data identification, classification &amp; protection</td>
<td>ST3: Improved supplier trust &amp; control</td>
</tr>
<tr>
<td>SOFTWARE TRANSFORMATION</td>
<td>PCT Service Integration &amp; Management Model (SIAM)</td>
<td>BC1: Reduced interruption time for PCT critical systems</td>
</tr>
<tr>
<td>ORGANIZATIONAL TRANSFORMATION</td>
<td>Redesigned architecture to optimize security, availability &amp; resilience of multiple DCs</td>
<td>SL1: Improved PCT critical systems service level</td>
</tr>
<tr>
<td>VDI</td>
<td>Remote Data Center</td>
<td>ST1: Improved customer experience</td>
</tr>
</tbody>
</table>

**Benefits**

- **S1**: Reduced likelihood of malicious or unintentional disclosure or modification of unpublished application/registration/patent information
- **S2**: Reduced likelihood of cyber-attacks and reduction of impact from a successful cyber-attack
- **S3**: Improved supplier trust & control
- **ST1**: Improved customer experience
- **BC1**: Reduced interruption time for PCT critical systems
- **SL1**: Improved PCT critical systems service level
- **SF1**: Improved WIPO reputation

**Tranche**

- **Tranche 1**
- **Tranche 2**
- **Tranche 3**
Cumulative benefit business impact

- ST1: Improved customer experience
- SF1: Improved WIPO reputation
- ST3: Improved supplier trust and control
- ST2: Increased Organizational Flexibility
- SL1: Improved PCT critical systems service level
- BC1: Reduced interruption time for PCT critical systems
- S2: Reduction of likelihood of cyber-attacks and reduction of impact from a successful cyber-attack
- S1: Reduction of likelihood of malicious or unintentional disclosure of unpublished application/registration/patent information
Program timeline

High Level Design → Detailed Design → Proof of Concept → RFPs → Implementation

- Technical transformation
- Organizational transformation

Lessons learned – Program challenges

- **Adapt to regular disruptions**: IT landscape evolving rapidly, the program had to adapt (trends on Cloud use, evolution of software architectures).

- **Improve our agility** in terms of sourcing strategy and application landscape, to avoid vendor lock-in and single points of failures.

- **Building our maturity** in terms of service management, vendor management, defining our process and procedures, building our knowledge of the local market.
Thank you!