Threat Risk Assessment for Enterprise Mobility.

Recognizing and understanding threats so you can safeguard against them.

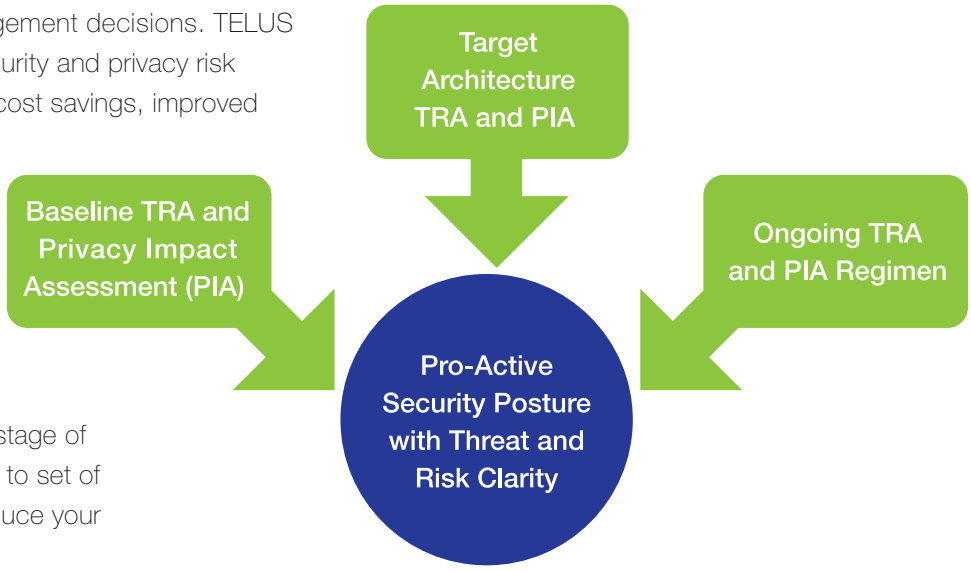
The Problem

The adoption of mobile applications, tablets, smartphones and other mobile devices in the work environment is growing exponentially. For many organizations, this can mean both an increased need for wireless infrastructure and increased exposure to security risks. As employees and customers demand robust and flexible solutions for greater sales and productivity, you may be tempted to rush into satisfying their demands. However, this can lead to security and privacy gaps that may not be immediately apparent, and could be exploited by attackers or internal /external users, unbeknownst to an organization.

These security and privacy gaps go beyond issues related to technology configuration. They may include gaps at the process and people management levels, which could translate into increased costs and compliance and regulatory requirements issues. Therefore, it is critical that you understand, categorize and address potential threats and risks in your mobile strategy. Then you can make the right decisions on where to allocate funds to develop and implement the correct security controls based upon your organization's risk tolerance and requirements.

The TELUS Solution

The TELUS Threat Risk Assessment (TRA) for Enterprise Mobility is a fundamental tool for risk management. It provides the basis for you plan and make sound risk management decisions. TELUS will assist you to better allocate your security and privacy risk management investments, providing net cost savings, improved security, privacy controls and, better compliance and reduced risk profile.



The output of the TELUS TRA allows you to understand the threat landscape as it relates to your enterprise mobility initiative and identify information security risks and gaps in your mobility solution at any stage of its development or operations. This leads to set of recommendations for safeguards that reduce your applicable risks to acceptable levels.

A TELUS Threat Risk Assessment focuses on:

- Security controls, policies, processes and standards within the IT area
- Governance and organizational security
- Asset classification and control included in the enterprise mobility solution
- Access control architectures and technologies
- Key mobile applications and supporting infrastructure design and requirements
- Incident management and response processes
- Understanding of the sensitivity of the information collected and used in the mobile process
- Configuration for security settings such as encryption, authentication, and enforcement

What to expect from the TELUS team.

- TELUS will provide a team of subject matter experts that understand risk, current best practices and compliance requirements.
- The TELUS team draws upon skill sets available from specialized and experienced information security professionals, and has developed a tried and tested methodology.
- TELUS can include ISO 27002, the Harmonized Royal Canadian Mounted Police (RCMP) and the Communications Security Establishment (CSE) methodologies as required, or adjust its own methodology to meet your organization's specific objectives.
- A point in time or multi-year program that provides your organization clarity on the risks and threats associated with your specific enterprise mobility posture and plans enabling decisions that are informed and security capabilities that are aligned.

Why TELUS?

We believe TELUS is uniquely qualified to help you take control of your mobile security needs. Advantages we offer include:

- **Depth and breadth of TELUS team experience:** Our team includes key TELUS team members involved in numerous large-scale projects focused on security architecture, managed services, ISO 27002 assessments and Harmonized Threat Risk Assessments. TELUS clients include many of Canada's largest banks, health care providers, governments, and insurance, retail and energy companies.
- **Leadership experience in risk management:** The TELUS Security Solutions Governance Risk and Compliance team has placed Chief Information Security Officers (CISO) at major insurance and financial organizations as security leadership resources to drive enterprise governance programs. Entrusted with the responsibility to implement and sustainable program, our CISOs are experienced leaders with proven track records.
- **Single mandate, true unbiased expert advisor:** TELUS Advisory Services focuses entirely on information security and privacy risk consulting. Our recommendations will never be tainted by conflicts of interest or the promotion of specific products. Our certified personnel are personally invested in a true reflection of the findings and are bound by a strict code of ethics.
- **Leadership in application security:** TELUS founded a dedicated practice in application security ten years ago. This team is one of the oldest and most established in North America. TELUS has a deep base of experience in large-scale applications within the financial, telecommunication and utility sectors.
- **Leadership in vulnerability research:** TELUS operates one of the largest focused vulnerability research teams in North America, with a dedicated staff of twelve personnel. The VR team focuses exclusively on validating and reproducing reported security vulnerabilities across a broad range of operating systems and application platforms. This unique capability provides crucial intelligence inputs into the infrastructure-level and application-level penetration testing practices used by TELUS.

Find out how TELUS can enable your business. Contact your TELUS Account Executive, call 1-866-GO-TELUS or visit **telus.com/businesssecurity**

TELUS