Technology Services Requisition (TRex) Smart Everything (SE)

Software as a Solution (SaaS)

Requirements Analysis Report

Version 1.0

4/22/2025

# Executive Summary

TRex develops smart devices to be used for homes, businesses, and in the medical industry. These smart devices include alarm systems, appliances, and human-worn devices. These devices collect personable identifiable information (PII), protected health information (PHI), credit card information, device, and security information, and contain other sensitive data. The devices can be configured to be linked to first responders, family members, or any authorized users a business and/or the owner of the device chooses.

The devices that deploy Trex’s software are configured to communicate with the Trex’s Smart Everything (Trex SE) Software as a Service (SaaS) platform that is hosted on the Azure Commercial Cloud Infrastructure as a Service (IaaS) platform. All Trex administrators log into the management plane of the Trex IoT SE using Trex’s active directory configured for multifactor authentication (MFA) using OKTA. Customers must use MFA and must provide their own identity provider (if applicable). All customer users will be configured to use MFA to gain access to the device as well as Trex SE, of their choice, no exceptions. FIPS 140-2 validated encryption is used throughout the environment and all events from each host within the environment are logged and sent to Splunk. Within the Trex SE platform, all technology is updated automatically using advanced programmable interfaces (APIs). The home and business devices will use their own internet service provider (ISP); however, due to the sensitive nature of the medical devices and their purposes, Trex will utilize Verizon ISP for internet connectivity with these devices. No data leaves the United States borders per service level agreements (SLA).

There are several dataflows within the Trex SE environment including customer data, update sources, logging/security, Trex administration, alerts, and external system data. The two main dataflows are the customer to devices, devices to Trex SE, and management plane to application plane. Customers interact with their devices through an ISP provider. Although customers can access some offline functionality, there must be an active and stable internet connection for the device to be able to pull and push accurate and current information from TRex SE. Smart devices respond to customer’s voices, fingerprints, and in the case of medical devices, physical attributes such as heart rate, blood sugar levels, blood pressure, etc. This information, once collected from the customer, is communicated with TRex SE through an encrypted tunnel using FIPS 140-2 validated encryption. TRex SE analyzes the data sent from the device to either warn the user about potentially harmful activities or statistics, or if a certain range will prompt the user to dial 911 immediately, and for some medical devices, the device will use E911 and dial for the customer. For home and business devices, TRex SE may make recommendations based on the customer’s use of the device as well as send health statistics of the device itself. For medical devices, TRex SE performs trend analysis to properly baseline the health of the individual using the device. This information is communicated to the user of the device but can also be communicated to authorized users, known as Viewers, of the information that the device produces. TRex admins are responsible for managing the TRex SE application. They perform several security and continuous monitoring activities.

# System Diagram

Refer to this [System Diagram](https://umuc365.sharepoint.com/:i:/s/AA-OperationRisingTideUS/EXWhKcfwwKlOnde1V9OaU04B04FBcVUs3s__r9nMUqnA8A?e=jkcjOk).

The system diagram presents a cloud-based architecture with components divided into the application plane and the management plane. It shows interactions between customers, smart devices, TRex SE, external systems, and administrators. TRex SE dataflows consist of customer-to-device side communication, device-to-TRex SE updates, and monitoring by TRex admins. The diagram displays security mechanisms that protect transmitted and/or stored data, such as boundary protection, FIPS 140-2 validated encryption and MFA. Secure access controls, real-time alerting, and trend analysis for medical and business/home devices are provided in the diagram to protect the processing of customer information in all interfaces and components.

# Cloud Controls Matrix Requirements

## [A&A: Audit & Assurance](https://csf.tools/reference/cloud-controls-matrix/v4-0/aa/)

* **The requirements for A&A-01 Audit and Assurance Policy and Procedures**
  + The organization should establish, document, approve, communicate, apply, evaluate, and maintain audit and assurance policies and procedures. These should define roles, responsibilities, and standards to be followed, frequency of assessments, documentation requirements, and reporting procedures. Policies should be updated at least annually to take into account changes in risk, regulations or the organization’s environment.
  + TRex has audit policies, but has not documented or communicated a formal Audit and Assurance Policy and Procedures document specific to the TRex SE platform. Current audit practices are applied inconsistently and their update occurs on an ad hoc basis without any documented standards and scheduled reviews. There is no record of an annual review or approval process for audit procedures.
* **The Requirements for A&A-02 Independent Assessments**
  + The organization should conduct independent audits annually using relevant industry standards.
  + In the 18 months past, there have been no third-party audits conducted on TRex SE and compliance gaps remain unsolved. Critical vulnerabilities remain unidentified in formal assessments.
* **The Requirements for A&A-03 Risk-Based Planning Assessment**
  + The organization should perform independent audits and assurance assessments based on risk-based plans and policies tied to organizational threats. To achieve this, an organization has to develop and maintain a risk-based audit plan consistent with the organization’s risk management framework and priorities. The process should include what frequency and scope should be used for audits, with the higher risk areas being audited utilising more resources.
  + TRex regularly conducts audits on the TRex SE platform, however, the audits are ad hoc and are not related to any critical risk, including Log4j 1.x vulnerabilities and unpatched OpenSSL components.

## [CEK: Cryptography, Encryption & Key Management](https://csf.tools/reference/cloud-controls-matrix/v4-0/cek/)

* **The Requirements for CEK-01 Encryption and Key Management Policy and Procedures**
  + Policies for encryption and key management need to be established, documented and reviewed by the TRex annually, in line with standards such as NIST SP 800-57.
  + There are no annual policy reviews for TRex and the practices are outdated. Current processes are based on manual key rotation and lack the use of FIPS 140-3 validated HSMs.
* **The Requirements for CEK-03 Data Encryption**
  + TRex should use certified cryptographic libraries for encrypting sensitive data at rest and in transit.
  + TRex transmits unencrypted PHI over TLS 1.0 through legacy medical devices, and archived logs at Azure Blob Storage also lack encryption.
* **The Requirements for CEK-05 Encryption Change Management**
  + A formal process must be established by the TRex to review, approve and communicate changes for encryption technologies.
  + The ad hoc updates implemented on critical components such as OpenSSL by TRex have no proper documentation and can lead to configuration drift and compliance failure.

## [IAM: Identity & Access Management](https://csf.tools/reference/cloud-controls-matrix/v4-0/iam/)

* **The Requirements for IAM-01 Identity and Access Management Policy and Procedures**
  + The organization should establish, document, and annually review IAM policies and procedures aligned with standards like NIST SP 800-63.
  + Although IAM policies are present in TRex, there are no annual reviews, which makes the current practices outdated. Current policies do not enforce phishing-resistant MFA for administrative accounts.
* **The Requirements for IAM-04 Separation of Duties**
* To combat misuse of privileges and improve oversight, the organization should separate conflicting roles.
* Since TRex developers have both code deployment and Splunk admin access, it violates the separation of duties principles and introduces more security risks.
* **The Requirements for IAM-05 Least Privilege**
* The organization should grant minimal access required for roles to perform their functions.
* TRex has set overly permissive Azure Blob Storage roles that let non-administrative personnel read and modify protected health information.

## [LOG: Logging and Monitoring](https://csf.tools/reference/cloud-controls-matrix/v4-0/log/)

* **The Requirements for LOG-01 Logging and Monitoring Policy and Procedures**
  + The organization should establish, document, and annually review policies for logging and monitoring aligned with standards like NIST SP 800-92.
  + TRex has no annual policy review, and as a result, there are different periods for log retention, and no defined alert thresholds. There is no formal process for detecting Splunk log tampering.
* **The Requirements for LOG-02 Audit Logs Protection**
  + To prevent tampering or deletion of audit logs, TRex should store audit logs in immutable storage, provide access controls, and encryption.
  + Unauthorized modifications are not prevented for Splunk logs, which are stored without write-once-read-many (WORM) policies**.**
* **The Requirements for LOG-03 Security Monitoring and Alerting**
  + The organization should carry out real-time monitoring and automatic alerts for anomalies.
  + Trex has no alerts configured for suspicious activities like repeated failed login attempts or log deletion.

## [TVM: Threat & Vulnerability Management](https://csf.tools/reference/cloud-controls-matrix/v4-0/tvm/)

* **The Requirements for TVM-01 Threat and Vulnerability Management Policy and Procedures**
  + TRex should create, document, and then review policies and procedures annually to prioritize, identify, and remediate vulnerabilities.
  + TRex does not have annual policy reviews, which results in delayed patching of critical vulnerabilities.
* **The Requirements for TVM-03 Vulnerability Remediation Schedule**
  + The organization should define processes for scheduled and emergency patching based on risk.
  + TRex does not have a formal SLA for the remediation, and many critical vulnerabilities are unpatched for long periods.
* **The Requirements for TVM-08 Vulnerability Prioritization**
  + The organization should prioritize vulnerabilities using a risk-based model aligned with organizational impact.
  + Patching is an ad hoc process for TRex that is not aligned with any significant threat identified in the environment

# Recommendations

## Recommendation

* **A&A-01**
  + TRex must develop and formally document an **Audit and Assurance Policy and Procedures** document applicable to the TRex SE platform annually.
    - TRex can accomplish this by updating the TRex SE Security Policy to mandate yearly reviews. To facilitate regulatory changes, TRex should schedule Q1 policy reviews with the Legal and Compliance team. The version history and cycle of the review should be tracked by documentation systems.
* **A&A-02**
  + At least annually, TRex must document an Independent Assessment Policy that describes the criteria and process that must be followed to provide impartial, standards-based audits.
    - TRex can accomplish this by including third-party audit requirements in the TRex Vendor Management Policy. An audit schedule and collection of evidence should be developed in a compliance calendar. Log system and security documentation must be given audit access via a secure channel.
* **A&A-03**
  + TRex should align audits with threat intelligence and identified vulnerabilities.
    - TRex can accomplish this by integrating NIST Risk Management Framework into the Risk Management Policy. TRex should conduct quarterly threat workshops to update audit priorities based on current risk assessments. Vulnerability scanning tools should be used to map vulnerabilities to the audit scope and prioritization on remediation efforts based on risk levels.

## Recommendation

* **CEK-01**
  + TRex must standardize cryptographic implementations and formalize the review of the encryption policy on an annual basis.
    - TRex can accomplish this by updating the Data Protection Policy to mandate yearly reviews and automated key rotation. Audit of key configurations against NIST guidelines should be made regularly. A consistent key lifecycle management should be provided by deploying a centralized key management service.
* **CEK-03**
  + TRex must enforce modern encryption standards for all sensitive data handling.
    - TRex can accomplish this by defining clear encryption standards in the Cryptographic Policy, including deprecation timelines for weak protocols. Regular scanning should be implemented to detect unencrypted PHI in transit and at rest. Medical devices should use a validated cryptographic module and all cloud storage should implement proper encryption.
* **CEK-05**
  + TRex should implement structured change management for all cryptographic components.
    - TRex can accomplish this by deploying governance tools to track encryption changes and updates. The Change Management Policy should require formal change requests for cryptographic updates. The Change Advisory Board should review the algorithm upgrades, and automated change logging should be implemented on the key management systems.

## Recommendation

* **IAM-01**
  + Annual IAM policy reviews must be formalized for TRex, and the organization should adopt modern authentication standards.
    - TRex can accomplish this by updating the IAM Policy to mandate yearly reviews and align with NIST SP 800-63B. TRex should conduct regular workshops with IT and Security teams to implement FIDO2 MFA and role-based access control. Authentication policy enforcement should be automated through Azure AD to prevent weak password usage.
* **IAM-04**
  + TRex needs to define and control role-based boundaries across all operational environments.
    - TRex can accomplish this by adding clear role separation clauses to the HR Policy that prevent developers from managing access controls. Role-based access control should be implemented in Splunk to prevent administrators from modifying audit logs. Break-glass accounts should be created and strictly controlled for emergency access to critical systems.
* **IAM-05**
  + TRex has to provide granular access controls to all sensitive data repositories.
    - TRex can accomplish this by defining specific privilege tiers in the Data Access Policy with clearly defined access levels. Appropriate tools must be used to identify and remediate excessive permissions every quarter. Administrative tasks should be deployed with Just-In-Time access to minimize standing privileges.

## Recommendation

* **LOG-01**
  + TRex should establish how frequently annual policies should be reviewed and define log retention and alerting standards.
    - TRex can accomplish this by updating the Logging Policy to mandate 7-year retention for HIPAA compliance and annual reviews. Workshops should be conducted to align log formats across all systems. Centralized logging policy enforcement should be implemented through appropriate tools.
* **LOG-02**
  + TRex should store logs in an immutable, encrypted storage with limited access.
    - TRex can accomplish this by requiring WORM storage and strong encryption in the Data Integrity Policy. Object locking should be implemented to prevent log tampering. Access to logs should be restricted by role-based Access Control.
* **LOG-03**
  + Real-time alerts should be set up for critical security events in TRex.
    - TRex can accomplish this by defining alert thresholds in the Incident Response Policy. Integration between security systems should be established for anomaly detection. There should be configured alerting mechanisms that would alert the appropriate person in case of potential security incidents.

## Recommendation

* **TVM-01**
  + TRex should formalize annual policy review and integrate standardised vulnerability scoring.
    - TRex can accomplish this by updating the Vulnerability Management Policy to mandate annual reviews and establish SLAs for critical vulnerabilities. Regular exercises should be conducted to practice responses to severe vulnerabilities. Automated tools should be used in vulnerability reporting and compliance checks.
* **TVM-03**
  + TRex should have a tiered remediation schedule for vulnerability severity.
    - TRex can accomplish this by defining clear SLAs in the Incident Response Policy. An automated reminder for approaching deadlines should be established for task ownership and tracking. Critical systems should be patched automatically.
* **TVM-08**
  + TRex must put in place a structured risk scoring model used to prioritize vulnerability remediation.
    - TRex can accomplish this by aligning prioritization with the Risk Assessment Framework. The mapping of vulnerabilities to business impact should be done so that resources are allocated properly. Threat Intelligence should be correlated with vulnerability to enhance the accuracy of risk assessment.