

**HCTM Application Criticality Model**

***Version 1.04***

**Table of Contents**

1 Background 4

2 Application Criticality Model 4

2.1.1 Data sensitivity: 4

2.1.2 Application accessibility: 4

2.1.3 Application privileges: 5

2.1.4 Availability: 5

2.1.5 Business Context: 5

2.2 Application Criticality Calculation 5

2.3 Criteria Weighting 5

2.4 How to Use Application Criticality Criteria 5

Document Revision History

| Version | Modification | Date | Author |
| --- | --- | --- | --- |
| 1.04 | Completed internal reviews. Still waiting to add Bosch HCTM data classification policy related details. | October 13, 2014 | Chandu Ketkar  Carl Schwarcz |
|  |  |  |  |

# Background

Software security processes (reviews, assessments, etc.) are not free and contribute to the cost of creating and maintaining software applications. It is therefore appropriate to create a risk-based approach to building security during the software development life cycle (SDLC). A risk-based approach allows us to make effective use of resources (people, tools, and processes) required to establish and maintain the appropriate level of security in an application portfolio.

This document describes a custom application criticality model for HCTM applications. This model will allow Bosch’s HCTM group to implement a risk-based approach for implementing security in its application portfolio. The purpose of the criticality model is to:

1. Establish a HCTM-wide framework for measuring application criticality
2. Bring consistency and objectivity to the measurement of application criticality within the HCTM business context, and
3. Provide an application criticality score to identify the required security activities in the application’s SDLC.

The criticality factors identified in the application criticality model are based on inherent characteristics of an application (its business requirements, deployment model, its regulatory environment, and so on) and are *not dependent* on the implementation factors such as the insecure design and/or the insecure implementation of the application.

A companion Excel workbook (“HCTM Application Criticality Model.xlsx”) is also delivered with this document. This Excel workbook contains the model for calculating application criticality.

# Application Criticality Model

The custom application criticality model proposed for the HCTM’s application portfolio is anchored in five main application characteristics categories:

### Data sensitivity:

If an application is required to store and/or process sensitive data such as any non-public personally identifiable data (NPPI) or data that is subject to regulatory compliance (such as PCI or HIPPAA) then it has direct implications on the severity of the business impact in case of a security breach. HCTM’s data classification policy is used to drive the questions and responses in this category.

### Application accessibility:

Whether an application is required to be accessible remotely over a public network, or required to be accessible locally over a private network or required to be running on a device that can be physically accessed, has implications on the ease with which it can be attacked. For example, an application open to remote users over a public network is likely to be attacked with more ease than an application that is accessible to internal users or a private network.

### Application privileges:

If an application or its components are required to be running as a privileged user (either a privileged system user or a privileged framework user) then in case of a compromise, an attacker can inflict more damage.

### Availability:

A security breach on an application with high availability requirements is likely to have more business impact than an application with lower availability requirements.

### Business Context:

Business context characteristics measure the importance of the application from a business viewpoint. If an application is a marquee application then any security issues with the application may expose the business to reputational and/or financial damage.

## Application Criticality Calculation

The application criticality raw score is calculated as follows:

* Each criteria upon which the application criticality depends, is given a weight factor. The weight factors for all criteria add up to 100%
* Each application is ranked for each criterion. The nominal ranking score is from 1 (lowest score) to 5 (the highest score)
* A weighted score is computed from the nominal scores.
* The weighted score on a scale of 1 to 5 is scaled to the percentage scale.

The application criticality raw score is then categorized into **Critical**, **High**, **Medium**, and **Low** categories. The type and depth of security activities/analyses required to make an application secure should depend on the application criticality.

## Criteria Weighting

The criteria weighting is done as follows:

* The weight is assigned to each of the categories (e.g. Data sensitivity, Access, Privilege, etc.) of criteria.
* The criteria in each category are assigned an individual weight. The sum of weights of criteria within a category adds up to the weight of the category.

## How to Use Application Criticality Criteria

The accompanying Excel workbook has the model for measuring application criticality. Here we will describe each criterion and explain its semantics and how it impacts the model.

1. Does the HCTM application use a multi-tenant datastore (meaning it stores data for more than a single client) or single-tenant data store?   
     
   A multi-tenant datastore increases the risk of privilege escalation attacks. For example, if an HCTM application stores/processes data for more than one customer then if there is a security issues (such as SQL injection), it may allow an attacker to access data for users pertaining to many customers. A single-tenant datastore does not eliminate the privilege escalation risk; however, it reduces the impact since the attacker cannot access data for more than one customer.
2. Using HCTM's data classification policy as a guide, what is the highest classification of data stored or processed by the application?  
     
   TBD (Will be written one we have reviewed the HCTM data classification policy)
3. Does this HCTM application or the data it handles subject to security requirements due to governmental regulation (such as HIPAA or HITECH) or industry standards (such as PCI)?  
     
   If the application stores/processes data that is subject to regulatory compliance requirements, then any security issue in the application may expose Bosch to regulatory/legal risk. As an example, the HCTM Desktop application stores and processes a patient’s PHI data and if such data along with the patient identification information is disclosed, it will expose Bosch to regulatory risk.
4. What is the most easily accessible manner to use the HCTM application?  
     
   This question assesses the accessibility requirements of an HCTM application. If an application is an internal application then its attack surface is going to be much smaller than if the application is Internet facing. If an application is an internal application, the risk is smaller than if an application were accessible over the Internet.
5. Does the HCTM application send sensitive data to the client for display, storage, or other reasons?   
     
   If an HCTM application is required to store sensitive data at a client (e.g. browser), then the data must be adequately protected otherwise it may be disclosed to unauthorized users. For example, if sensitive data is displayed or stored at a client browser (HTML-5 supports local storage as an example), then a cross-site scripting attack may cause such data to get exposed.
6. Does the HCTM application run on a device that allows users physical access (such as a smart phone or some other device)  
     
   If an application is running on a physical device that can be easily accessed by attackers, then it opens the application to many more attack vectors than if the application were running on a protected server. Such attack vectors include (but not limited to) an attacker downloading the firmware, reverse engineering the firmware, inspecting on-device databases and so on.
7. Does the HCTM application interface with one or more external systems (e.g. EMR systems) for data exchange?  
     
   If the HCTM application is required to interface with an external system such as an electronic medical record (EMR) system and exchanges PHI data (such as the HL7 application), then it increases risk of sensitive data exposure. This data could be exposed in transit or otherwise at the server if proper security controls are in not in place.
8. Do any components of the HCTM application or the application itself run as a privileged user (a system user or a framework user) that have root level or other privileged access to system and/or framework resources?  
     
   If some components of the application (of the HCTM application itself) are required to run as a privileged user, then it will likely increase the impact of some type of security vulnerabilities. This is because if an attacker can exploit the application (e.g. by using a command injection vulnerability) then the attacker can cause far more damage since the attacker can execute privileged system commands and access privileged system resources.
9. What are the availability requirements on the HCTM application?  
     
   If an application is required to be available or has stringent availability requirements, then any security issue that could potentially make the application unavailable, and likely to cause a significant business impact.
10. If the HCTM application were to be hacked or compromised in some fashion, would the level of business impact?  
      
    This criterion assesses the business impact if the application were to be hacked or if it were to receive unfavorable publicity due to security issues. There could be many reasons why an application is important from business viewpoint. These reasons could go well beyond the use of sensitive data. The model captures such overriding business reasons for the application criticality.