



July 13, 2021

Micheal Augusti  
Ascom Healthcare  
Head of Key Accounts, North America

**Re: Unified Security Platform - National Institute of Standards and Technology – Risk Management Framework Engagement**

To Whom it may Concern:

To meet cybersecurity requirements within US Federal and Defense environments, Ascom Healthcare (“Ascom”) has engaged with SecureXperts to obtain cybersecurity consulting services to assess and evaluate organizational compliance with the National Institute of Standards Special Publications Risk Management Framework, or (“RMF”).

Since October 21, 2020 Ascom and SecureXperts have build a technical reference architecture to test the Ascom portfolio (Telligence, Unite, Digistat, and mobility) against next generation cybersecurity vulnerabilities against stringent security baselines developed by the US Department of Defense, Health and Human Services, and the National Institute of Standards and Technology.

These security baselines include evaluation and assessment of management, technical, and operational controls and detailed information security artifacts that provide vendor agnostic third party independent verification and validation that proper security objectives are met and reported. This project is expected to conclude in Q3 of this year.

**Security Determination**

SecureXperts has concluded that Ascom is presently in compliance with the RMF security baseline and potential vulnerabilities have been mitigated by configuration changes or compensating control that meets security objectives of the RMF assessment.

Any additional findings (if any) will be resolved using an documented plan of action and milestone on any area having critical, high, or medium risk using the Common Vulnerability Scoring System (CVSS) by the United States Computer Emergency Response Team (US-CERT).

SecureXperts has also concluded at this current reference point in time there are no immediate threats or significant vulnerabilities in the Ascom System that would prohibit the certification of and accreditation using the RMF.