



# **Intrado Life & Safety, Inc.**

## **Enterprise Services System**

System and Organization Controls Report (SOC 3®)

Relevant to Security

November 1, 2023 to October 31, 2024





# Table of Contents

	Page
Assertion of Intrado Life & Safety, Inc.'s Management	1
Independent Service Auditor's Report	2
Attachment A: Intrado Life & Safety, Inc.'s Description of the Boundaries of its Enterprise Services System	4
Attachment B: Principal Service Commitments and System Requirements	7



## Assertion of Intrado Life & Safety, Inc.'s Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Intrado Life & Safety, Inc.'s (Intrado) Enterprise Services System (system) throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Intrado's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Intrado's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

Intrado's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that Intrado's service commitments and system requirements were achieved based on the applicable trust services criteria.

April 25, 2025



## INDEPENDENT SERVICE AUDITOR'S REPORT

Board of Directors and  
Management of  
Intrado Life & Safety, Inc.

### Scope

We have examined Intrado Life & Safety, Inc.'s (Intrado) accompanying assertion titled "Assertion of Intrado Life & Safety, Inc.'s Management" (assertion) that the controls within Intrado's Enterprise Services System (system) were effective throughout the period November 1, 2023 and October 31, 2024, to provide reasonable assurance that Intrado's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus –2022)* in AICPA, *Trust Services Criteria*.

### Service Organization's Responsibilities

Intrado is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Intrado's service commitments and system requirements were achieved. Intrado has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Intrado is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

### Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirement were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Intrado's service commitments and system requirements.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Intrado's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

### **Inherent Limitations**

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

### **Opinion**

In our opinion, management's assertion that the controls within Intrado's Enterprise Services System were effective throughout the period November 1, 2023, to October 31, 2024, to provide reasonable assurance that Intrado's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

*Squire & Company, PC*

Squire & Company, PC  
Orem Utah  
April 25, 2025



## Attachment A: Intrado Life & Safety, Inc.'s Description of the Boundaries of its Enterprise Services System

### OVERVIEW OF OPERATIONS

#### Company Overview and Services Provided

Intrado Life & Safety, Inc. (Intrado or the Company) has provided software systems and services to the public safety community for over forty years. Intrado delivers solutions with speed, confidence, and clarity to connect those in need with those who can best help them. Intrado's solutions are designed to be robust, resilient, intuitive, and insightful, ensuring emergency responders can quickly react and quickly respond to urgent and life-threatening situations.

Intrado's mission is to achieve and maintain the trust of its clients and provide a robust security program that considers client data protection across:

- Corporate governance and regulatory compliance
- Recruiting, hiring, professional development, and employee security awareness compliance
- Risk assessment, risk management, and vendor risk management
- Internal control monitoring systems
- External threat and vulnerability management
- Physical access and security
- Enterprise IT network architecture, logical access, security management
- Change management

Intrado's various systems, applications, and program offerings rely on internal controls performed by the Enterprise Services system to meet its principal service commitments and system requirements.

### COMPONENTS OF THE SYSTEM USED TO PROVIDE SERVICES

#### INFRASTRUCTURE

Intrado performs key functions as its corporate headquarters in Longmont, Colorado. Intrado also operates a data center facility and owns all the infrastructure assets contained in the data center. Intrado is responsible for the physical security of its corporate headquarters and data center.

A portion of Intrado's enterprise network is hosted by cloud service providers, data centers, and by a cloud security service provider. These third-party providers are responsible for the physical security of virtual assets.

#### SOFTWARE

Intrado uses a variety of software applications to perform the following functions:

- Email/productivity



- Identity and access management
- Single sign-on
- Endpoint management
- Internet security
- Web application firewall
- Antivirus and endpoint detection and response
- Real-time comprehensive control capabilities for endpoints
- DNS security
- Threat and vulnerability scanning
- Automated patching
- Automated cloud-based workflow automation
- GRC management

## PEOPLE

The following teams support the Enterprise Services System as their job responsibilities require they have access to production systems, develop code to be included in the environment, or support operational and advisory functions.

Executive Management – provides general oversight, strategic planning of operations, legal, and regulatory requirements.

Product Management – understands market and customer needs, defines product roadmaps, prioritizes feature development.

Product Development/Engineering – delivers responsive systems complying with functional specifications.

Quality Assurance – verifies systems comply with design specifications through functional testing procedures.

Technical Operations – provisions, installs, configures, operates, monitors, and maintains Intrado applications in production environments.

Customer Support – provides education and instructional material on uses and capabilities of Intrado applications.

Information Security – defines and communicates enterprise security controls, manages security defenses and monitoring tools, leads response for security incidents.

Physical Security – manages Intrado facilities to protect personnel, visitors, and infrastructure.

## PROCEDURES

Intrado has documented formal information security policies and standards designed according to business objectives and the following security industry frameworks: ISO 27001/2, NIST SP800-53 rev5, and NENA 75-001. Intrado applies a risk-based approach to selecting and developing internal controls.



After relevant risks have been identified and evaluated, internal controls are established, implemented, monitored, reviewed, and improved to meet the overall objectives of the organization. Formal IT policies, standards, processes, and procedures include, but are not limited to:

- Personnel security
- Access control
- Asset management
- Communication security
- Cryptography
- System configuration and monitoring
- Change management
- Incident management
- Business continuity
- Disaster recovery

All teams are expected to adhere to Intrado's policies, standards, processes, and procedures, which define how services should be delivered. These documents are located on the Intrado intranet and accessible to all staff. Control activities have been implemented to help ensure that actions are carried out properly and efficiently.

Intrado communicates specific procedures to clients via individual service-level agreements, various online publications, and reference guides.

## **DATA**

Data includes but is not limited to, system and network logs for the following:

- Network traffic
- Firewalls
- Web and application servers
- Databases
- Security infrastructure
- Antimalware systems

The boundaries of the system include the infrastructure, software, people, procedures, and data related to the Enterprise Services System administered by personnel assigned to operate the system of internal controls. Systems, applications, and programs offered by Intrado are supported by the Enterprise Services System. Specific controls related to Intrado's products, systems, applications, and programs, are not included within the scope of this report.





## Attachment B: Principal Service Commitments and System Requirements

### Overview

Intrado establishes operational requirements that support the achievement of its security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in enterprise-wide policy and procedure documents, website, and client contracts. Information security policies define an enterprise-wide approach to protecting systems and data. These include how the Enterprise Services system is operated, how internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented to carry out specific manual and automated processes to operate and develop the Enterprise Services system.

Intrado uses advanced technologies in conjunction with administrative, technical, and physical controls to ensure the security of its Enterprise Services system. Intrado's security commitments are documented and communicated to its clients in Master Service Agreements (MSAs) and other system, application, program, and client-specific agreements. These security commitments are standardized and include, but are not limited to, the following:

- Implementing system architecture and data segregation permitting Intrado personnel and client users to access only the production systems and data they have been allowed to access, using the principle of least privilege in the case of Intrado personnel.
- Maintaining administrative and logical safeguards to protect customer data following Intrado's information security requirements.
- Implementing formal access control processes for requesting, approving, provisioning, and de-provisioning personnel needing access to production and/or development systems.
- Utilizing formal human resource processes defining job requirements, conducting background checks, providing compliance training--including security awareness training--and establishing a formal code of conduct.
- Implementing enterprise IT networks and management, security monitoring, and endpoint protection.
- Maintaining change management processes to provide secure infrastructure modifications and/or software development processes to ensure consistent quality, confidentiality, integrity, and availability of services.
- Using appropriate encryption technologies to protect customer data at rest and in transit.
- Implementing threat and vulnerability management, incident management, and breach notification processes.
- Contingency planning and business continuity.

The boundaries of the system include the infrastructure, software, people, procedures, and data related to the Enterprise Services System administered by personnel assigned to operate the system of internal controls. Systems, applications, and programs offered by Intrado are supported by the Enterprise Services System, and thus the specific controls related to these systems, applications, and programs are not considered within the scope of this report.