singlewire® software

BUYER PERSONAS GUIDE

Table of Contents

Introduction..3

InformaCast Personas...4

IT Leadership

Overview..5

SPICED Insights...6-9

Safety Leadership

Overview..10

SPICED Insights...11-14

Operations & Facilities

Overview..15

SPICED Insights...16-19

Administration

Overview..20

SPICED Insights...21-24

Visitor Aware Personas...25

IT Leadership

Overview..26

SPICED Insights...27-30

Safety Leadership

Overview..31

SPICED Insights...32-35

Operations & Facilities

Overview..36

SPICED Insights...37-40

Administration

Overview..41

SPICED Insights...42-45

Introduction

What if you knew what your prospects needed before you even spoke to them? Could you have better conversations? Appear more knowledgeable? Reduce sales cycles? Win more deals?

This guide is built to help you do just that. It contains personas for four job functions that we commonly encounter during our prospecting. But these personas give you more than basic details about who these people are; they contain key insights structured to align with the SPICED framework to arm you with the information you need to have informed, productive conversations with your prospects.

You'll understand why prospects search out solutions like InformaCast and Visitor Aware, what their current set ups look like, the pain points they are experiencing, what they want to achieve with our solutions, and their buyer's journey. You'll be able to anticipate potential questions and even bring up concerns they may not have considered.

With this knowledge you'll make prospects confident they are selecting the right solutions to meet their needs. You'll be able to better position our solutions against competitors, and help prospects feel secure that they'll achieve success by moving away from their current status quo and implementing our tools.

INFORMACAST PERSONAS

Ian's job titles could include:

- Director of Technology/IT Director
- Manager Telecommunications Call Center
- UC Engineer
- Network Admin
- IT Supervisor
- System & Network Engineer
- Director of Information Technology
- IT/Tech Coordinator
- IS Administrator
- IT Support Specialist
- Telecommunications Analyst
- Client Services Technician

Ian, the industrious IT leader

As an IT leader, Ian is responsible for the overall technology infrastructure, network systems, data management, and the implementation and maintenance of software and hardware solutions within his organization. He ensures the reliability, security, and efficiency of all technological resources.

Ian's top concerns are:

1. **Replacing systems that are aging or at end of life** and finding solutions that offer greater compatibility with other systems.
2. **Finding better ways to integrate multiple systems** and reducing complexity within his environment.
3. **Implementing reliable solutions** that can scale to meet his organization's needs.
4. **Eliminating time-consuming manual tasks** and reducing inefficiencies.
5. **Working with a vendor that offers excellent support** and clear licensing models.

How to talk about InformaCast with Ian

1. Highlight InformaCast's **vast ecosystem of integration partners.**
2. Emphasize that the system is **easy to manage and reliable.**
3. Discuss how InformaCast is **built with scaling and future-proofing in mind.**
4. Underline **cost-effectiveness through consolidation** and limited maintenance.
5. Bring up Singlewire's **proven track record for customer support** and our vast library of documentation and resources.

Ian’s InformaCast SPICED Insights

1. Situation (Details about the current status)

Ian had a number of tools already in place, each with their own set of problems:

- Cisco Call Manager, which is aging and difficult to manage.
- An outdated paging system that can’t integrate and offers poor technical support.
- Mass notification that can’t integrate and doesn’t deliver messages consistently.
- A phone system with no paging integration, 2-way communication or 911 notification.
- And security systems (panic buttons, access control systems, fire alarm systems).

Most of his systems are disparate, leading to time-consuming, manual work, including:

- Managing distribution lists and memorizing phone codes for emergency protocols.
- Managing disparate communication methods (VoIP, multicast, overhead paging, text, email, separate websites).
- Managing multiple bell schedules with exceptions.
- Manually counting speakers and doing blueprints for new projects.

And his environment can be challenging to work with, hindering his ability to do larger scale. deployments, due to:

- Thick, solid block construction making wiring difficult.
- Mixed Cisco switch environments.
- WAN connection reliance for paging/bells (concern about outages).
- On-premise VMware infrastructure (expiring, considering cloud migration).
- Large security systems (10,000+ cameras, 5,000 access control systems).
- Remote/mobile employees.
- Different operating systems (Windows 11 incompatibility).
- Distributed sites/campuses (geographically dispersed, multiple buildings).
- Data retention issues.

2. Pain (Challenges that made them seek a solution)

Ian's current organization is dealing with a number of issues prompting them to seek out a new solution, including:

- **Outdated/aging infrastructure** that is difficult to manage, integrate, and support.
- **The inability connect disparate systems** and achieve seamless communication.
- **Excessive manual effort** for user onboarding/updates, managing lists, bell schedules, and troubleshooting, which slows down operations and is prone to error.
- **Lack of centralized control** to manage all communications from a single platform, which is inefficient and opens up the potential for missed messages.
- **Poor technical support** from providers leading to prolonged issues and downtime.
- **Facing increasing costs** from maintaining multiple, disparate systems.

These issues also mean Ian's organization is exposing itself to potential risks, including:

- **Missing critical information** during emergencies due to disparate systems and inconsistent message delivery.
- **Critical system failures** due to aging hardware and WAN connections.
- **Security vulnerabilities** caused by outdated systems and manual processes, especially concerning data retention and access control.
- **Insufficient means to demonstrate compliance** with safety or audit requirements.

3. Impact (What they want to achieve with our solution)

Ian is looking for a solution that will have a significant impact on his organization's operations. He wants to:

- **Improve efficiency and streamline operations** through automation, consolidation and simplification into a "single pane of glass", and faster deployment and scaling.
- **Reduce costs and optimize resource allocation** by moving to the cloud and avoiding future maintenance and upgrade issues.
- **Enhance reliability and uptime** through consistent message delivery, improved system stability, and proactive issue resolution with responsive technical support.
- **Achieve future-proofing and adaptability** through compatible operation systems and technologies, scalable infrastructure that supports growth, and flexibility to integrate with new platforms.
- **Receive positive feedback from end users** regarding reliability and ease of use.

4. Critical Event (Deadline to achieve their desired Impact)

There are several factors driving Ian's need to implement a new solution:

- **Systems reaching end-of-life** need to be replaced to maintain critical functions and avoid system failure.
- **Budget cycles and expiring contracts** provide a limited window find and implement new solutions without interrupting service or incurring cost increases.
- **System scaling and deployment demands** driven by project deadlines necessitate immediate solutions to ensure stability while also leaving room for testing and rollout.
- **Migration to new technologies,** like cloud calling platforms, create immediate need for compatible notification solutions that offer the required integration capabilities to ensure core communication functionality can continue.
- **Ongoing technical problems** impact daily operations and IT team bandwidth. These issues can escalate, leading to larger system failures or communication breakdowns.

5. Decision (What's required to purchase)

For Ian to make his decision, he often needs to receive buy-in from multiple internal stakeholders. This includes:

- **Senior leadership** (e.g., Superintendent, CTO)
- **Finance teams** (for budget approval)
- **Department heads/end users** (e.g., Safety & Security, Facilities)
- **Integrators or consultants** (for technical evaluation)

The internal approval process includes several steps:

- Needs assessment.
- Technical evaluation of solutions from multiple vendors.
- Internal discussions with departments that will use the solution.
- Proof of concept testing or pilot programs.
- Formal presentation and approval by a board or executive committee.

This process can take months or over a year, and can stall out for multiple reasons:

- **Budget cycles:** Waiting for the next fiscal year's budget allocation.
- **Complexity of integration:** Unexpected technical hurdles or the need for extensive network reconfiguration.
- **Internal consensus:** Difficulty getting all stakeholders (especially those reliant on the old system) to agree on a new solution.
- **Resource limitations:** IT staff being overwhelmed with existing tasks, delaying evaluation or implementation.
- **Vendor support/responsiveness:** Delays in getting clear answers or effective troubleshooting from prospective vendors.

In addition, while Ian is determined to find a solution to his organization's problems, there are key obstacles that would prevent him from working with certain vendors:

- The cost does not fit into his budget.
- The solution offered is overly complex which will drain his limited resources.
- The vendor does not provide excellent support or training.
- The vendor does not give him a full understanding of the solution's capabilities and its integration potential.

Sam's job titles could include:

- Emergency Manager
- School Safety Analyst
- Assistant Director of Campus Safety
- Risk Manager
- Supervisor for the Office of Communications Engineering

Sam, the strategic safety leader

As a safety leader, Sam is dedicated to developing, implementing, and overseeing safety protocols, emergency response plans, and security measures at their organization. Sam's primary focus is on ensuring the well-being of people and assets, managing crisis communications, and maintaining compliance with safety regulations.

Sam's top concerns are:

1. **Replacing existing systems that are insufficient** for rapid, widespread emergency communication.
2. **Finding ways to track staff movement,** confirm safety or know someone's location.
3. **Consolidating multiple, unintegrated communication/alerting platforms** that require separate logins to speed up response times and coordination, especially with external agencies.
4. **Implementing solutions that go beyond the basics,** won't be underutilized, and have minimal technical flaws or limitations.
5. **Meeting regulations for workplace violence** and injury/illness prevention, and prevent legal/reputational damage from an inadequate response.

How to talk about InformaCast with Sam

1. Highlight how InformaCast can **send alerts across numerous channels** (text, email, overhead PA, desktop, mobile app, digital signage).
2. Emphasize that messages are delivered extremely fast with **easy ways to initiative alerts.**
3. Discuss how InformaCast can **send messages to specific buildings, rooms, or groups.**
4. Underline tools for **accountability and reunification.**
5. Focus on InformaCast's ability to **seamlessly connect with existing security systems.**

Sam's InformaCast SPICED Insights

1. Situation (Details about the current status)

Ian had a number of tools already in place, each with their own set of problems:

- Emergency communication systems that have basic or limited functionality.
- Panic button systems that are underutilized, don't send effective audio alerts, and often are activated accidentally.
- Multiple, disconnected alarm systems.

Sam's ability to keep his organization safe and operational is hindered by a number of challenges, including:

- Manual lockdowns with limited follow-up communication.
- Lack of accountability during fire drills and evacuations.
- No formal, actionable safety plan.
- False alerts from panic button activations.
- Lack of clear communication protocols for non-emergency situations.
- Limited ability to coordinate with external agencies.

And his environment can be challenging to work with, due to:

- Varied communication needs for different staff and organization members.
- Loud environments and employees who can't easily access computers.
- Frequent fires and weather threats (need for effective critical communication).
- Social media spreading rumors and confusion about potential threats.
- Remote/mobile employees that are hard to reach.

2. Pain (Challenges that made them seek a solution)

Sam's current organization is dealing with a number of issues that are prompting them to seek out a new solution, including:

- **Ineffective emergency communication** leading to confusion and delays.
- **Inability to accurately track individuals** during emergencies (e.g., fire drills, evacuations) and confirm their safety.
- **Recent incidents** that exposed gaps and challenges with procedures and tools.
- **Manual and reactive safety protocols** for lockdowns with insufficient follow-up communication and a lack of formal, actionable safety plans.

- **Limited interoperability** that makes it difficult to coordinate effectively with external agencies (e.g., county dispatch).
- **False alarms and misuse,** especially from panic buttons, leading to unnecessary disruptions and potential desensitization.

These issues also mean Sam's organization is exposing itself to potential risks, including:

- **Delayed response** due to ineffective communication and outdated protocols.
- **Lack of situational awareness,** which prevents a clear understanding of unfolding events, and hinders effective decision-making.
- **Legal and reputational damage** due to an inability to communicate effectively or manage emergencies effectively.

3. Impact (What they want to achieve with our solution)

Sam is looking for a solution that will have a significant impact on his organization's operations. He wants to:

- **Reach every person and device** in his organization with rapid, clear communication.
- **Account for every individual** during emergencies and leverage maps to deliver faster responses.
- **Simplify activation of emergency procedures,** reducing false alarms, improving lockdown procedures, and strengthening coordination with external agencies.
- **Achieve better situational awareness** with tools for location mapping, event logging, and providing clear, actionable information to responders.
- **Integrate with existing security systems** (access control, cameras, fire alarms) and communicate with external agencies.
- **Meet regulatory requirements for workplace violence** and illness prevention, mitigating legal and reputational risks associated with an ineffective response.
- **Receive positive feedback** from staff and first responders with a solution that requires minimal training and is easy to use, helping to become a model for safety and emergency preparedness in their community.

4. Critical Event (Deadline to achieve their desired Impact)

There are several factors driving Sam's need to implement a new solution:

- **Recent incidents,** including fires, active shooters, and bomb threats, coupled with slow response times and ineffective communication, drive urgency for new solutions.
- **Grant application deadlines** provide a time-sensitive opportunity to acquire necessary security technology that supports critical safety initiatives.
- **Regulatory compliance and policy updates** require organizations to have communication and safety protocols in place to avoid legal penalties and ensure employee well-being.
- **System deficiencies** create pressure to improve security and communication effectiveness before a crisis occurs.
- **Coordinating with local dispatchers** to create seamless communication that helps ensure an effective response.

5. Decision (What's required to purchase)

For Sam to make his decision, he often needs to receive buy-in from multiple internal stakeholders. This includes:

- **IT leadership** (for system implementation and integration)
- **School principals/administrators** (key stakeholders who can help with user adoption)
- **Local law enforcement** (for protocol alignment)
- **Facilities management** (for physical security and infrastructure considerations)
- **Human resources** (assess impact on employee safety and legal liabilities)

The internal approval process includes several steps:

- Incident review/gap analysis of existing safety plans and communication tools.
- Researching solutions that address specific emergency needs.
- Product demonstrations, including simulated tabletop exercises.
- Site visits or discussions with peers and local agencies.
- Internal discussions with stakeholders.
- Pursuing potential grant funding.
- Receiving formal approval for purchase.

This process can be highly variable, from a few months to over a year, depending on the urgency and funding availability. Common stalling points include:

- **Budget availability:** Dependence on grants or specific safety funding cycles.
- **Lack of consensus:** Leaders resisting standardization or adoption of new tools.
- **Integration complexity:** Requires significant IT involvement.
- **Procurement processes:** Navigating state or district-specific purchasing requirements.
- **Competing priorities:** Safety initiatives sometimes take a back seat other operational projects unless a critical incident provokes an immediate need.

In addition, while Sam is determined to find a solution to his organization's problems, there are key obstacles that would prevent him from working with certain vendors:

- The cost does not fit into his budget, or no grants are available.
- There is no clear path for wide user adoption.
- The solution does not demonstrate itself to be reliable.
- The vendor does not show the value of a comprehensive, integrated system compared to piecemeal solutions.
- The vendor does not give him a full understanding of the solution's capabilities and its integration potential.
- The vendor lacks credibility and cannot back up the effectiveness of the solution with case studies or references from similar organizations.

Frank's job titles could include:

- Director of Operations
- Director of Facilities and Maintenance
- Building Automation Engineer
- Systems Administrator

Frank, the focused facility manager

Frank is accountable for the physical environment and operational efficiency of buildings and grounds. His responsibilities include managing building systems (like HVAC, lighting, and communication systems), overseeing maintenance, ensuring physical security, and supporting the daily functional needs of the organization's facilities.

Frank's top concerns are:

1. **Replacing outdated or failing infrastructure and systems,** including phones, PA, bells systems, and physical security.
2. **Eliminating ineffective communication & notification systems** that cannot reach all staff and do not deliver messages consistently.
3. **Finding new solutions that can work with existing systems** (e.g., access control, fire alarms, current phone systems, student information systems).
4. **Managing multiple locations and user information,** including staff movement and profiles, mapping alert locations, and distribution lists.
5. **Limited financial resources for upgrades,** concerns about the ongoing cost of subscription-based solutions, and the high cost of implementing new IP-based infrastructure.

How to talk about InformaCast with Frank

1. Highlight that InformaCast is a **modern, functional replacement** for outdated or failing intercom, PA, and bell systems.
2. Emphasize that the system **delivers clear, intelligible audio to all areas.**
3. Discuss how InformaCast includes **easy-to-use tools** for managing bell schedules, including exceptions.
4. Underline the ability to **integrate with existing building systems** and to be installed in challenging physical environments.
5. Bring up the **user-friendly interface and the ability to customize zones.**

Frank’s InformaCast SPICED Insights

1. Situation (Details about the current status)

Frank had a number of tools already in place to help with daily operations, but each has its own set of problems:

- Bell systems that are outdated, lack flexibility, and aren’t compatible with newer OS.
- PA systems that lack functionality and integration.
- Paging systems that provide inadequate coverage and require managing multiple amplification systems.

Frank’s ability to keep his organization safe and operational is hindered by a number of challenges, including:

- Manual PA announcements
- Managing multiple schedules for bell systems with exceptions
- Dealing with music volume overriding notification audio
- Lack of staff movement tracking
- Challenges integrating disparate systems (access control, fire alarms, TV boards, computer screens)

And his environment can be challenging to work with, hindering his ability to do larger-scale deployments, due to:

- Old buildings with thick construction and various room setups.
- Loud environments that make communication challenging.
- Multi-story buildings that make it difficult to map alert locations.
- Unstaffed departments after hours that require single-button assistance calls.

2. Pain (Challenges that made them seek a solution)

Frank's current organization is dealing with a number of issues that are prompting them to seek out a new solution, including:

- **Critical failure of an existing system** or a desire to modernize outdated infrastructure.
- **Outdated bell and PA systems** are inflexible, difficult to manage, and often incompatible with newer operating systems, leading to manual workarounds.
- **Poor coverage and functionality** limit the ability to broadcast across all areas.
- **Integration challenges** with bell/PA systems to other critical facility systems hinder safety efforts.
- **Audio interference** impacts the clarity and effectiveness of announcements.

These issues also mean Franks's organization is exposing itself to potential risks, including:

- **Communication breaks down in loud environments,** which means critical announcements may not be heard, risking safety.
- **Inefficient daily operations** due to outdated systems and manual processes create bottlenecks, increasing staff workload.
- **Delayed incident response** because they can't make announcements quickly.
- **Security gaps** due to a lack of staff movement tracking and communication issues.

3. Impact (What they want to achieve with our solution)

Frank is looking for a solution that will have a significant impact on his organization's operations. He wants to:

- **Implement a functional and reliable paging and bell system** throughout buildings.
- **Increase operational efficiency** with a simple, streamlined, automated system.
- **Improve audio intelligibility** for daily announcements and emergency alerts throughout facilities, regardless of location or background noise.
- **Reduce maintenance calls and troubleshooting** with a facilities communication system that requires minimal oversight.
- **Simplify management of daily schedules and announcements** buy tailoring notification zones, setting bell schedules, overriding music with critical announcements, and single-button assistance calls.
- **Modernize infrastructure** by replacing outdated systems with flexible, integrated solutions and reducing reliance on manual processes and physical wiring challenges.
- **Successfully integrate communication systems** with building access control.
- **Receive positive feedback from staff** on the ease of making announcements or managing schedules.

4. Critical Event (Deadline to achieve their desired Impact)

There are several factors driving Frank's need to implement a new solution:

- **Systems that no longer function,** including bell and PA systems demand immediate upgrades to ensure reliable communication and minimize impact on daily operations.
- **Recent local incidents** push emergency preparedness to the top of the priority list, driving the need for better notification and evacuation tools to protect occupants.
- **The need for a phased solution** that offers a cost-effective alternative to improve capabilities without a massive upfront investment.
- **Reaching all employees** regardless of their location or device access (some can't access computers or desk phones), is paramount for safety and compliance, especially in loud or distributed environments.

5. Decision (What's required to purchase)

For Frank to make his decision, he often needs to receive buy-in from multiple internal stakeholders. This includes:

- **IT leadership** (for network connectivity and system integration)
- **Finance/procurement** (for equipment purchase and installation costs)
- **Site managers** (for multi-building campuses directly impacted by bell/PA systems)
- **Maintenance/custodial staff** (who rely on PA for announcements and may activate assistance calls)
- **IT Department** (for network infrastructure and system integration support)
- **End-users** (e.g., staff whose daily operations are impacted by paging or bell systems)

The internal approval process includes several steps:

- Assess physical infrastructure (e.g., speaker counts, wiring conditions) and identify specific operational pain points (e.g., noisy areas, complex bell schedules).
- Research vendors for replacements or upgrades.
- On-site walkthroughs or demonstrations to ensure the solution is practical for their environment.
- Discuss how the solution will connect with existing facility systems (e.g., access control, fire panels).
- Gather input from staff who directly use the systems.
- Cost estimation (including installation) and weighing the cost of new systems against the inefficiencies and risks of outdated ones.
- Budget request and approval.

This journey can range from a few months for urgent replacements to over a year for major infrastructure overhauls. Common stalling points include:

- **High upfront costs:** Especially for new IP wiring or extensive hardware installations in old buildings.
- **Installation logistics:** The complexity and disruption of replacing systems in active buildings.
- **Resistance to change:** If existing, albeit poor, systems are "working," there can be reluctance to invest in new solutions.
- **Competing capital projects:** Funds being diverted to other pressing facilities needs (e.g., HVAC, roofing).
- **Procurement requirements:** Delays in getting competitive bids or navigating specific purchasing rules.

In addition, while Sam is determined to find a solution to his organization's problems, there are key obstacles that would prevent him from working with certain vendors:

- High expense associated with running new IP wiring in old or difficult-to-access buildings ("thick, solid block construction").
- Concerns about the feasibility of installing new systems in unique environments or large, noisy production floors.
- Hesitation about replacing or integrating with existing "very old analog speaker systems" that are still "working" (even if poorly).
- Skepticism about the consistency of wireless systems given past issues with connectivity in older structures.
- Concerns about disruption during installation or the complexity of managing new bell schedules or communication workflows.

Alex's job titles could include:

- Chief Strategy Officer
- Superintendent
- Executive Assistant
- Business Unit Leader
- Owner
- Head of HR
- Assistant Superintendent for Business

Alex, the able administrator considering InformaCast

Alex is a senior leader who makes strategic decisions, manages budgets, oversees organizational efficiency, and handles external relations. Her concerns often revolve around financial viability, reputation, compliance, and fostering a productive organizational environment.

Alex's top concerns are:

1. **Maintaining business continuity** through effective crisis management to minimize significant disruptions and reputational risk.
2. **Managing costs and justifying budgets** when facing budget cuts or feeling like she's paying disproportionately high prices for licenses her organization doesn't fully utilize.
3. **Keeping employees safe** by closing gaps with solutions that reach everyone, even if they don't have access to certain channels like email or the internet.
4. **Ensuring selected vendors provide adequate support** and help reduce administrative burden by consolidating disparate systems.
5. **Assigning ownership for subscription-based solutions** to ensure critical systems do not lapse or become underutilized.

How to talk about InformaCast with Alex

1. Highlight a clear value proposition showing how the investment will **lead to cost savings, increased efficiency, or avoided risks.**
2. Emphasize how InformCast can **enhance public perception** and fosters confidence.
3. Discuss how InformaCast can **streamline workflows and reduce manual tasks.**
4. Underline ease of adoption, scalability, and the ability to **build a holistic solution.**
5. Bring up Singlewire's track record for **excellent customer service, clear communication, and reliable ongoing support.**

Alex’s InformaCast SPICED Insights

1. Situation (Details about the current status)

Alex’s existing toolset is limited, and often only includes:

- Limited or no existing emergency/mass communication systems.
- Basic email and text communication.

Alex’s ability to keep her organization safe and operational is hindered by a number of challenges, including:

- Manual processes for reaching employees.
- Relying on personal phones for communication.
- Dealing with budget cuts and funding limitations.
- Difficulty with communication during social media threats.
- Lack of consolidated vendor relationships.
- Managing multiple password logins.
- No clear ownership of subscription-based solutions.
- Challenges finding certified installers for security systems.

And she faces several challenges that she needs to address in her environment, including:

- The need for scalable solutions.
- Meeting regulatory requirements from workplace violence and illness prevention.
- Ensuring she can reach full-time and part-time/event-specific employees.
- Reaching employees that are constantly on the move.
- Working with limited tax revenue that leads to relying on the sheriff’s department for emergency response.

2. Pain (Challenges that made them seek a solution)

Alex’s current organization is dealing with a number of issues that are prompting them to seek out a new solution, including:

- **Limited or non-existent communication infrastructure** (e.g., basic email/text or personal phones) for critical communication, which is unreliable and inefficient.
- **Tight budgets** make it difficult to find scalable, cost-effective solutions for emergency communication.
- **Lack of automated systems** for reaching all employees, especially those without email or internet access, or across distributed sites.

- **Desire not to manage multiple vendors and disparate systems** to reduce administrative burden and consolidate support.
- **Lack of clear ownership** for subscription-based solutions, leads to confusion and potential oversight.
- **Meeting requirements for workplace violence** or illness prevention with robust communication tools.

These issues also mean Alex's organization is exposing itself to potential risks, including:

- **Reputational damage** due to the inability to effectively communicate during crises.
- **Compromised employee safety** and morale due to inadequate systems.
- **Operational disruptions** from poor communication can impact productivity and revenue.
- **Legal and financial penalties** from non-compliance with safety regulations.
- **High employee turnover** because staff feel unsafe or that their well-being is not prioritized.

3. Impact (What they want to achieve with our solution)

Alex is looking for a solution that will have a significant impact on her organization's operations. She wants to:

- **Achieve cost savings or greater value** with demonstrable ROI from communication and safety investments.
- **Improve the organization's reputation** and public image through effective and transparent communication, especially during crises.
- **Enhance organizational efficiency** by reducing administrative burdens and streamlining processes.
- **Implement an easy to use solution** that employees will adopt with minimal training.
- **Standardize communication and safety protocols** across multiple sites or departments.
- **Ensure the organization meets its duty of care** and avoids potential liability related to safety failures.
- **Receive positive feedback** from the community or employees regarding crisis communication situations.

4. Critical Event (Deadline to achieve their desired Impact)

There are several factors driving Alex's need to implement a new solution:

- **Inability to communicate effectively during crises** (weather, active threats, power outages) leading to significant business disruption, reputational damage, and potential safety liabilities.
- **Budget cycle creates limited windows for approval and expenditure,** which means Alex must secure necessary funding, or risk delaying crucial safety initiatives.
- **Regulatory mandates and internal safety policies** are driving the need for immediate action to avoid legal exposure, maintaining a safe environment, and protecting vulnerable populations.
- **Current vendor relationship has deteriorated** and the contract will not be renewed, and Alex wants to find a single, reliable provider to streamline operations and ensure better service.
- **Employees feel unsafe** due to lack of communication during incidents, and Alex needs an effective system to maintain a positive work environment.

5. Decision (What's required to purchase)

Alex typically initiates or gives final approval for strategic investments like this, but she still needs buy-in from multiple internal stakeholders. This includes:

- **IT leadership** (for technical feasibility)
- **Safety/security teams** (for operational viability)
- **Facilities/operations teams** (for operational viability)
- **Legal counsel** (for compliance and liability considerations)
- **HR** (for employee morale considerations)

The internal approval process includes several steps:

- Review strategic goals and seek proposals that articulate ROI, organizational impact, and risk mitigation.
- Evaluate vendor stability, track record, and ability to provide comprehensive support.
- Facilitate cross-departmental collaboration to build consensus.
- Present to board or executive committees for formal approval (providing details financial justifications).
- Conduct a legal review for contracts and data privacy concerns.

Decisions at this level are often the longest, ranging from six months to multiple years, as they involve significant financial and strategic implications. Common stalling points include:

- **Budget approval:** The most significant hurdle, especially when budgets are tight.
- **Lack of consensus:** Can't get all stakeholders to agree on a unified approach.
- **Risk aversion:** Hesitation to commit to a new vendor or technology due to past negative experiences or fear of the unknown.
- **"Kicking the can down the road":** Delaying decisions until a critical incident forces action or new funding becomes available.
- **Complex procurement:** Navigating multi-year contracts, competitive bidding, and legal reviews.
- **Leadership transitions:** Changes in key members can restart or delay initiatives.

In addition, while Alex is determined to find a solution to her organization's problems, there are key obstacles that would prevent herv from working with certain vendors:

- High price points are often a significant barrier especially when ROI is not evident.
- Vendor support seems poor, communication is inconsistent, or the solution does not seem to be able to address critical needs.
- Vendor is unable to demonstrate that the solution is not too complex or piecemeal.
- They underestimate the financial and reputational cost of not having an effective emergency communication system.
- They believe a perceived cheaper alternative (e.g., Microsoft Teams for communication) will fully address all their complex safety and operational needs.

VISITOR AWARE PERSONAS

Ian's job titles could include:

- Director of Technology/IT Director
- Tech Coordinator
- Network & Phone Engineer
- Network Technician
- Telecommunications Analyst
- IT Manager
- Systems Network Analyst or Specialist
- Chief Information Officer
- IT Admin or Specialist

Ian, the industrious IT leader

As an IT leader, Ian is responsible for the overall technology infrastructure, network systems, data management, and the implementation and maintenance of software and hardware solutions within his organization. He ensures the reliability, security, and efficiency of all technological resources.

Ian's top concerns are:

1. **Replacing clunky, outdated systems** that are often Windows-based.
2. **Overcoming integration challenges** with SIS, mass notification, and other existing systems.
3. **Difficulty with hardware,** including scanner issues and printer compatibility.
4. **Budget constraints and unexpected costs** for features or upgrades.
5. **Manual data processes** that are time-consuming and prone to errors.

How to talk about Visitor Aware with Ian

1. Highlight Visitor Aware's ability to **integrate with other systems.**
2. Emphasize that the system is reliable and has a **strong track record for uptime.**
3. Discuss how Visitor Aware is **built with scalability and flexibility in mind.**
4. Underline the strong **security and data privacy policies in place.**
5. Bring up the systems **reporting and analytic capabilities (real-time visitor insights).**

singlewire software

Ian’s Visitor Aware SPICED Insights

1. Situation (Details about the current status)

Ian has visitor management tools already in place, but they have a number of problems:

- Often described as “junky,” “lackluster,” “underwhelming,” “clunky,” or “very kludgy”.
- Windows-based, but Ian’s working in a Mac/iPad environment.
- Older hardware, like scanners and printers, is incompatible with desired new systems.
- Existing systems may be disparate or lack integration capabilities.

The visitor check-in process is often time-consuming and inefficient due to:

- Paper-based systems like log books and sign-in sheets.
- Systems that frequently fail, crash, or experience connectivity problems.
- Inconsistent functionality.

And his environment can be challenging to work with, due to:

- High levels of frustration with existing tech from staff.
- Budget constraints and unexpected “nickel and diming” from current vendors.
- The need for a holistic, single-vendor solution and modern features like tablet kiosks and self-service that can be difficult to find.

2. Pain (Challenges that made them seek a solution)

Ian’s current organization is dealing with a number of issues that is prompting them to seek out a new solution, including:

- **Existing systems are “junky” or “clunky” systems** leading to a desire for modern, integrated solutions.
- **Time-consuming manual processes and system failures** that waste time and create inefficiencies, leading to a demand for automated and dependable systems.
- **Budget surprises and lack of holistic solutions** that create financial strain and operational headaches.
- **Upcoming contract expirations** create a need to implement a new system.

These issues also mean Ian’s organization is exposing itself to potential risks, including:

- **Incidents of unauthorized access** due to lacking the ability to screen visitors.
- **Unchecked, increased foot traffic** leads to systems struggling to handle high volumes of visitors during busy periods.

3. Impact (What they want to achieve with our solution)

Ian is looking for a solution that will have a significant impact on his organization's operations. He wants to:

- **Achieve a stable, consistently functional system** that "just works" and minimizes downtime.
- **Automate manual processes** (e.g., visitor sign-in, background checks, badge printing) to reduce staff workload and human error.
- **Integrate new solutions with existing IT infrastructure** (SIS, HR systems, access control) for unified data management and reporting.
- **Reduce operational costs** associated with inefficient systems, maintenance, and potentially avoid "nickel and diming" from current vendors.
- **Demonstrate ROI** through cost savings or efficiency gains justifying the investment.
- **Implement modern, user-friendly technology** that aligns with current IT best practices and provides desired features (e.g., tablet kiosks, self-service).
- **Future-proof** with a scalable solution that can adapt to future technological advancements and organizational growth.
- **Be seen as a proactive** and effective department head that delivers reliable and innovative solutions and receive positive staff feedback.

4. Critical Event (Deadline to achieve their desired Impact)

There are several factors driving Ian's need to implement a new solution:

- **Specific budget windows** (e.g., fiscal year-end, new budget allocation) that create a deadline for securing funds and implementing new systems.
- **Aging infrastructure/end-of-life systems** creates an immediate need to replace them to avoid operational disruptions and maintain business continuity.
- **High staff frustration/low adoption of current tech** that create internal pressure for IT leadership to find a solution to improve morale and productivity quickly.
- **Desire to keep pace with industry trends** or improve user experience, creating urgency to adopt new tech sooner.

5. Decision (What's required to purchase)

For Ian to make his decision, he often needs to receive buy-in from multiple internal stakeholders. This includes:

- **Administration** (Superintendent, Business Manager) will be involved for budget approval and strategic alignment.
- **Safety & Security Leadership** who provide input on features and compliance.
- **Operations & Facilities** may weigh in on hardware needs and physical deployment.
- **School Board** (or similar governing body) might need to give final approval for significant technology investments.
- **End-users,** such as front desk staff, will also provide crucial feedback during trials.

The internal approval process includes several steps:

- Initial problem identification
- Technical requirements gathering
- Vendor vetting
- Internal feasibility study
- Cost-benefit analysis
- Pilot program
- Budget allocation
- Security and privacy review
- Procurement and implementation planning

This process can take 6-18 months, and can stall out for multiple reasons:

- **Complex Integrations:** If the solution struggles to integrate seamlessly with critical legacy systems, or if custom development is required, the project can hit significant roadblocks.
- **Resource Availability:** Lack of IT staff or budget for new hardware can cause delays.
- **Security/Privacy Concerns:** Strict internal security policies or unresolved data privacy questions can lead to lengthy reviews.
- **Pilot Program Issues:** Any technical glitches, performance issues, or significant negative feedback during a pilot can halt progress.
- **Vendor Support Confidence:** If IT leadership is not fully confident in the vendor's long-term technical support and roadmap, they may hesitate.

In addition, while Ian is determined to find a solution to his organization's problems, there are key obstacles that would prevent him from working with certain vendors:

- Fear that a new system will be difficult to integrate.
- Hesitation regarding data privacy, network security, and potential new attack vectors.
- A solution that might limit future flexibility or create dependence on a single vendor.
- Doubt about whether the solution can effectively scale with growth or handle future changes in their environment.

Sam's job titles could include:

- Director of Safety and Security/Safety Director
- Safety Specialist or Coordinator
- Manager Security Systems
- Director of Public Safety,
- Environmental Health Safety Supervisor

Sam, the strategic safety leader

As a safety leader, Sam is dedicated to developing, implementing, and overseeing safety protocols, emergency response plans, and security measures at their organization. Sam's primary focus is on ensuring the well-being of people and assets, managing crisis communications, and maintaining compliance with safety regulations.

Sam's top visitor management concerns are:

1. **Ineffective visitor screening** and background checks, especially for sex offenders.
2. **Lack of a unified system** for tracking all individuals on campus during emergencies.
3. **Reunification processes** that are manual, chaotic, and lack real-time accountability.
4. **Insufficient or unreliable emergency notification** and communication systems.
5. **Challenges with unauthorized access** and ensuring staff enforce check-in procedures.

How to talk about Visitor Aware with Sam

1. Highlight real-time threat screening and identification that helps **enhance security.**
2. Emphasize that the system can tie into InformaCast to **leverage critical incident management features.**
3. Discuss how it can **provide a centralized view** for multiple sites.
4. Underline how it can **create automated records** to serve as audit trails to meet compliance.
5. Bring up the ability to customize set ups and screening protocols to **meet the needs of unique environments.**

Sam’s Visitor Aware SPICED Insights

1. Situation (Details about the current status)

Sam has visitor management tools already in place, but they have a number of problems:

- Rely on manual sign-in, or operating an “open campus”.
- Only perform basic sex offender registry checks.
- Often “antiquated” or “underwhelming”.

The visitor check-in process is often labor-intensive, slow, and unreliable due to:

- Manual processes for screening, tracking, or emergency reunification.
- No automated way to comply with audit requirements and tracking visitor logs.

And his environment can be challenging to work with, due to:

- Increasing concern for physical security.
- Lack of uniformity across multiple sites or campuses.
- Concerns about unauthorized access or security vulnerabilities.

2. Pain (Challenges that made them seek a solution)

Sam’s current organization is dealing with a number of issues that is prompting them to seek out a new solution, including:

- **No current system for screening guests,** relying on manual sign-in, or having an “open campus” where anyone can walk in.
- **Need to track visitor logs, comply with regulations** (e.g., sex offender registry checks), and ensure system integration with safety centers for reporting.
- **Current systems only check sex offender databases,** and there’s a need for more comprehensive background checks.
- **Lack of uniformity across multiple sites/campuses** regarding visitor management.
- **Unreliable or “underwhelming”** previous visitor management systems.
- **Public or internal concerns** about security and visitor vetting processes.

These issues also mean Ian’s organization is exposing itself to potential risks, including:

- **Unauthorized individuals gaining access** or security vulnerabilities were exposed.
- **Not “meeting the moment,”** by addressing the growing focus on physical security.
- **Rely on antiquated systems** that are “not appropriate for their situation”.

3. Impact (What they want to achieve with our solution)

Sam is looking for a solution that will have a significant impact on his organization's operations. He wants to:

- **Enhance safety and reduce security incidents** through robust visitor screening and tracking to prevent unauthorized access and protect students and staff.
- **Improve capabilities and response times** for efficient emergency reunification and accurate accountability during critical incidents.
- **Meet or exceed compliance requirements** related to visitor logs, background checks (e.g., sex offender registry), and reporting.
- **Achieve a unified and consistent security approach** across all facilities, providing centralized visibility and control.
- **Identify potential threats** (e.g., barred individuals) before they enter the premises.
- **Be recognized as a leader in safety** and security best practices.
- **Create peace of mind** by developing an environment where staff, students, and visitors feel secure and protected.

4. Critical Event (Deadline to achieve their desired Impact)

There are several factors driving Sam's need to implement a new solution:

- **Recent security incidents (internal or external)** or heightened public awareness of safety issues can create immediate pressure to implement more robust visitor management and emergency response systems.
- **Compliance with specific security audits,** regulations, or local/state mandates creates a deadline for having auditable visitor logs and security protocols in place.
- **Upcoming initiative to standardize operations or security across multiple campuses** creates a window of opportunity and urgency to implement a unified visitor management system.

5. Decision (What's required to purchase)

For Sam to make his decision, he often needs to receive buy-in from multiple internal stakeholders. This includes:

- **School Administration (Superintendents, building principals, Deans of Students)** is critically involved for operational impact and school-level buy-in.
- **IT Leadership** is essential for technical feasibility, integration with existing systems, and network considerations.
- **Finance/Business Office** plays a gatekeeping role for budget approval.
- **School Board** (or similar governing body) will likely need to approve significant security investments, especially those impacting policy or requiring public funds.
- **Parents and community groups** can also be informal influencers, especially after a security incident.

The internal approval process includes several steps:

- Initial problem identification (sometimes brought on by an incident)
- Research and solution exploration
- Cross departmental collaboration
- Policy and protocol review
- Pilot program
- Compliance justification
- Budget and grant application
- Board presentation and approval
- Implementation and training

This process can take 6-18 months, and can stall out for multiple reasons:

- **Budget Availability:** Security solutions can be perceived as high-cost, and securing funds can be difficult without a clear budget allocation or successful grant application.
- **Lack of Urgent Catalyst:** If there hasn't been a recent security incident or a new compliance mandate, the initiative might be deprioritized.
- **Inter-Departmental Friction:** Resistance from IT due to integration concerns, or from Administration due to perceived operational disruption, can slow progress.
- **Pilot Program Feedback:** Negative feedback during a pilot regarding system reliability, false positives, or user difficulty can halt the process.
- **Community Pushback:** Concerns from parents about privacy or ID scanning can lead to delays or require extensive public relations efforts.
- **Legal/Compliance Review:** Lengthy internal legal reviews regarding data privacy or screening protocols.

In addition, while Sam is determined to find a solution to his organization's problems, there are key obstacles that would prevent him from working with certain vendors:

- Doubts about the comprehensiveness and reliability of background checks (beyond sex offender registry) and real-time alerts.
- Concern that a new system might not truly enhance or seamlessly integrate with existing emergency protocols (e.g., lockdown systems, reunification plans).
- Worry about the system generating too many false positives or slowing down daily operations (e.g., long check-in lines during peak times).
- Concerns about data collection, privacy, and the legal ramifications of visitor screening data.
- Hesitation about the time and effort required to train staff on a new security system, especially for frontline personnel.

Frank's job titles could include:

- Director of Facilities & Operations
- Director of Transportation
- Director of Operations
- Director of Facilities and Maintenance

Frank, the focused facility manager

Frank is accountable for the physical environment and operational efficiency of buildings and grounds. His responsibilities include managing building systems (like HVAC, lighting, and communication systems), overseeing maintenance, ensuring physical security, and supporting the daily functional needs of the organization's facilities.

Frank's top visitor management concerns are:

1. **Current systems that are not user-friendly,** leading to staff frustration and training needs.
2. **Manual processes** for check-in and check-out that are inefficient and labor-intensive.
3. **Lack of centralized control** and uniformity across multiple school buildings or facilities.
4. **Difficulties with tracking employee time** and attendance.
5. **Challenges with physical security infrastructure** like door access and camera systems.

How to talk about Visitor Aware with Frank

1. Highlight user friendliness and **self-service options.**
2. Emphasize its hardware flexibility to **meet organization needs.**
3. Discuss ability to customize set ups and processes for **unique facility workflows.**
4. Underline ability to provide comprehensive, **real-time insights** about who is within a building.
5. Bring up the system's proven track record for **reliable performance,** even in high traffic areas.

Frank’s Visitor Aware SPICED Insights

1. Situation (Details about the current status)

Frank has visitor management tools already in place, but they have a number of problems:

- Hardware maintenance is an ongoing struggle.
- And different campuses may use disparate visitor management solutions.

The visitor check-in process is often less the optimal due to:

- Difficulty managing unique visitor flows within a facility (e.g., manufacturing to warehouse).
- No “single console” for management resulting in a lack of streamlined processes.

And his environment can be challenging to work with, due to:

- Aging infrastructure and current systems starting to fail or nearing end-of-life.
- Lack of centralized visibility across all sites.
- Struggling to allocate budget for new technology, especially when moving to the cloud.
- Concerns about hardware compatibility with new systems.

2. Pain (Challenges that made them seek a solution)

Franks’s current organization is dealing with a number of issues that is prompting them to seek out a new solution, including:

- **Lack of uniformity across campuses:** Different campuses using disparate visitor management solutions, hindering centralized control.
- **Inefficient internal processes:** Challenges with managing unique visitor flows within a facility (e.g., manufacturing to warehouse).
- **Budget allocation:** Planning for future budget cycles to move to cloud systems or invest in new security technology.
- **Hardware compatibility:** Concerns about new systems integrating with existing hardware (e.g., old badge printers, intercom systems).
- **Desire for “single console” management:** Overwhelmed by too many disparate security systems and seeking consolidation.
- **Aging infrastructure:** Current systems “starting to fail” or being at end-of-life.

These issues also mean Frank's organization is exposing itself to potential risks, including:

- **Unauthorized individuals gaining access** or security vulnerabilities were exposed.
- **Lack of insight around critical situations**, due to failing systems and lack of centralized visibility.
- **Reputational issues** due to inefficient check-in processes.

3. Impact (What they want to achieve with our solution)

Frank is looking for a solution that will have a significant impact on his organization's operations. He wants to:

- **Achieve centralized security control** with uniform visitor management and security protocols across all facilities.
- **Create efficient internal processes** by streamlining workflows, such as managing specific access requirements within different zones.
- **Optimize resource allocation** through informed decision making about facility upgrades and technology investments based on clear data and needs.
- **Improve hardware performance** with new systems that integrate seamlessly with existing or upgraded physical security hardware (door access, cameras, intercoms).
- **Accurately track the presence and movement of individuals,** including employees, contractors, and visitors, within various facility zones.
- **Reduce facility access incidents** with fewer unauthorized entries or security breaches in specific facility areas.
- **Reduce costs** related to manual processes or inefficient security systems.
- **Streamline compliance reporting** by generating reports for audits or external regulations.
- **Receive positive feedback** from teams regarding improved efficiency and ease of use.

4. Critical Event (Deadline to achieve their desired Impact)

There are several factors driving Frank's need to implement a new solution:

- **Aging infrastructure reaching end-of-life** creating a critical and immediate need for replacement to avoid operational downtime and security gaps.
- **Upcoming budget cycles/capital expenditure planning** drive the need to allocate budget for new technology, especially cloud systems, creating a time-sensitive window to secure funding and make purchasing decisions.
- **Facility expansion or new site openings** creates an opportunity and urgency to implement new, standardized security and operational systems from the outset.
- **Desire for operational efficiency and consolidation** creates an urgency to adopt integrated solutions that deliver these benefits.

5. Decision (What's required to purchase)

For Frank to make his decision, he often needs to receive buy-in from multiple internal stakeholders. This includes:

- **IT Leadership** is a crucial partner for technical integration and system compatibility.
- **Safety & Security Leadership** will be involved for broader security policy alignment and emergency response integration.
- **Finance/Business Office** provides budget oversight.
- **Administration/Leadership** might be involved in standardizing solutions for larger organizations with multiple sites.

The internal approval process includes several steps:

- Infrastructure assessment/problem identification
- Research solutions
- Technical and integration vetting
- Operational impact analysis
- Building a business case to justify the cost
- Pilot program
- Budget approval
- Vendor selection and procurement
- Implementation and training

This process can take 8-24 months, and can stall out for multiple reasons:

- **Budget approval for capital expenditures:** Significant hardware investments or large-scale rollouts often require longer budget cycles and multiple levels of approval.
- **Complex integration challenges:** Difficulties in seamlessly integrating with diverse, often proprietary, physical security systems can lead to delays.
- **Operational disruption concerns:** Fear of downtime during implementation or potential negative impacts on daily facility operations can cause hesitation.
- **Unique workflow accommodation:** If the solution cannot address specific or complex operational workflows, it may be rejected.
- **Prioritization of other facility projects:** Competing demands (e.g., HVAC, structural repairs) can push visitor management projects to the back burner.
- **Lack of an urgent catalyst:** If there isn't a pressing security incident or compliance mandate, the initiative might be deprioritized.

In addition, while Frank is determined to find a solution to his organization's problems, there are key obstacles that would prevent him from working with certain vendors:

- Skepticism about seamless integration with existing access control, door locks, cameras, and intercom systems, especially if they are older.
- Concern about the need for significant hardware upgrades or replacement (e.g., badge printers, kiosks) to support a new system, adding unforeseen costs.
- Fear that implementing a new system will cause downtime or significantly impact daily facility operations.
- Concern that a standard solution won't accommodate specific operational nuances like tracking movement between buildings or managing specific visitor types, like contractors.
- Worry that vendor support will not be adequate to maintain the new system.
- Believing that the system is only meant for K-12 or office environments.
- Not seeing the justification to move on from current ad-hoc methods are deemed "sufficient" for safety and compliance.

Alex, the able administrator considering InformaCast

Alex is a senior leader who makes strategic decisions, manages budgets, oversees organizational efficiency, and handles external relations. Her concerns often revolve around financial viability, reputation, compliance, and fostering a productive organizational environment.

Alex's job titles could include:

- Dean of Students
- Superintendent,
- Project Manager,
- Assistant Director
- Director of Operations
- Executive Director
- HR Director

Alex's top visitor management concerns are:

1. **Cost** of current or potential new systems is a significant.
2. **Inefficient processes** that lead to wasted staff time and operational bottlenecks.
3. **How visitor data is collected and stored** and how background checks are conducted.
4. **Lack of reporting capabilities** for attendance, audit records, and other metrics.
5. **Difficulty getting buy-in and feedback** from end-users for new system adoption.

How to talk about Visitor Aware with Alex

1. Highlight Visitor Aware's **user-friendly interface** for staff and visitors.
2. Emphasize that the system can help organizations **improve efficiency and speed up check-ins.**
3. Discuss how it provides organizations with **accurate record and reports.**
4. Underline ability for visitors to do **pre-screening** ahead of large scale events.
5. Bring up Singlewire's **commitment to data security.**

Alex's Visitor Aware SPICED Insights

1. Situation (Details about the current status)

Alex has visitor management tools already in place, but they have a number of problems:

- Front desk staff are often burdened with manual check-in processes.
- Often need to manage multiple disparate systems.
- Existing kiosks are not intuitive, requiring staff intervention.

The visitor check-in process is often less the optimal due to:

- Manual sign-in.
- Slow check-in/out times.
- Difficulties with pre-registration for events.
- Inability to track who is on campus, especially during emergencies.
- Integration with SIS/attendance systems is often lacking.

And her environment can be challenging to work with, due to:

- The front desk being frequently overwhelmed, due to high volumes of visitors during specific events or peak times.
- Sensitivity around scanning IDs and collecting personal information.

2. Pain (Challenges that made them seek a solution)

Alex's current organization is dealing with a number of issues that is prompting them to seek out a new solution, including:

- **Front desk staff overwhelmed by manual check-in processes,** managing multiple systems, and constantly assisting confused visitors.
- **Poor user experience** including visitors not finding current kiosks intuitive, leading to staff intervention and defeating the purpose of self-service.
- **Struggling to cope with large influxes of visitors** during events or peak times.
- **Difficulties in syncing visitor and student attendance data** with existing student information systems.
- **Facing limited resources,** requiring strategic spending on new technology.

These issues also mean Alex's organization is exposing itself to potential risks, including:

- **The inability to accurately account for all individuals on campus** (visitors, volunteers, students) poses a significant safety risk during emergencies and complicates compliance.
- **Disconnected systems create data silos,** requiring redundant data entry and increasing the risk of errors.

3. Impact (What they want to achieve with our solution)

Alex is looking for a solution that will have a significant impact on her organization's operations. She wants to:

- **Reduce burden on administrative staff** by automating check-in processes and minimizing manual interventions to free up staff for higher-value activities.
- **Maintain precise records** of who is on campus at all times, including visitors, volunteers, and vendors.
- **Provide an intuitive and efficient check-in process** for visitors, volunteers, and parents resulting faster check-in times.
- **Facilitate better communication** between front office staff, teachers, and other departments, and ensure relevant data is accessible.
- **Create a "Well-Oiled Machine"** through a highly efficient and smoothly running administrative office.
- **Leave a positive first impression** on all visitors as a secure and professional environment.

4. Critical Event (Deadline to achieve their desired Impact)

There are several factors driving Alex's need to implement a new solution:

- **Start of a new school year/peak visitor periods:** Anticipated high volumes of visitors at the start of a school year, during events, or peak times create a strong incentive to implement an efficient check-in system to improve flow.
- **Addressing staff burnout/improving visitor experience:** Persistent "headaches" and "frustration" at the front desk due to manual processes create internal pressure to find solutions that alleviate stress and improve the experience for staff and visitors.
- **New compliance or reporting requirements:** Changes in regulations regarding visitor tracking, volunteer management, or emergency accountability can create deadlines for implementing systems that ensure accurate data and compliance.
- **Previous safety incidents/desire for improved accountability:** Even minor incidents or near-misses related to tracking individuals on campus can create immediate urgency to implement systems that ensure accurate accountability, especially during emergencies.

5. Decision (What's required to purchase)

For Alex to make her decision, she often needs to receive buy-in from multiple internal stakeholders. This includes:

- **Front Desk Staff/Secretaries** are critical influencers due to their daily interaction with the system and visitors; their pain points drive the search.
- **IT Leadership** are involved for technical feasibility, integration, and ongoing support.
- **Safety & Security Leadership** provide input on the security implications.
- **Finance/Business Office** manage the budget.
- **Superintendent or District Leadership** give final approval in larger districts.

The internal approval process includes several steps:

- Recognize the pain point
- Informal research and peer consultation
- Internal committee forms to gather requirements and evaluate options
- Vendor demos and "walk-throughs"
- Cost-benefit analysis
- Budget approval
- Pilot program
- Communication and rollout planning

This process can take 4-9 months, and can stall out for multiple reasons:

- **User adoption concerns** if initial feedback from front desk staff or visitors suggests the system is too complicated or creates new problems.
- **Budget constraints** might make the solution seem as a "nice-to-have" rather than a critical infrastructure investment.
- **Fear of disrupting established routines** or causing stress during implementation.
- **Privacy pushback** due to significant community concern about ID scanning or data collection makes administrators hesitant to proceed.
- **Lack of clear ROI on soft benefits** like improved staff morale or streamlined processes.

In addition, while Alex is determined to find a solution to her organization's problems, there are key obstacles that would prevent her from working with certain vendors:

- Fear that a new system will cause more problems that it solves, disrupting existing routines, creating more work for already overwhelmed staff, or requiring extensive retraining.
- Concern that staff, visitors, or volunteers will resist using a new system, leading to workarounds or abandonment.
- Lack of clarity of how data is protected and stored leading to pushback from parents or community members regarding data collection or ID scanning.
- Concerns about receiving adequate vendor support post-implementation.