Nuvalence

WHITEPAPER

A Proposal for an Infection Risk Management Platform

WWW.NUVALENCE.IO

Introduction

To aid organizations in their COVID-19 recovery and post-COVID reinvention, Nuvalence will be releasing a series of cloud based tools, consulting services and a reference architecture of a digital platform. Why? The COVID-19 pandemic has drastically perverted modern life, society, and industry. Industry is the lifeblood of modern society and it's been brought to its knees. We need to get back to business safely and quickly if we intend to recover.

We now have enough information about the pandemic to have a better sense of what we are up against. The current environment requires moving from defense to offense. This document intends to:

a. outline key challenges in this reinvigoration process

b. describe an approach for safely re-engaging the organizational workforce

c. discuss general expectations for digital tooling needed for success

The challenge in delivering on these three intentions is rooted in the nature of organizations and infectious disease. Most medium-to-large organizations (companies, universities, not-for-profit, etc.) are composed of a significant number of people spread across many locations and buildings. The collection of people, work-types (e.g. factory, office), locations, buildings, floor plans, and physical links between these entities are collectively defined as an **Organizational Entity (OE)**. An OE is an abstract geometry of sorts that describes the "shape" of an organization. Keeping in mind the definition of an OE and this concept of "shape" is important for properly interpreting the concepts in this paper.

Infectious disease does not respect the physical boundaries of an organization, so any technology solution must be able to reason through the challenges associated with the boundless propagation of infectious disease.

Being able to aggregate information about the details of an OE, along with composing a data-driven picture of "infection signals" to properly manage infection risk is a non-trivial endeavor. To date, technology vendors have made excellent, much needed progress on foundational solutions for proximity tracing (led by Apple and Google's recent partnership), contact tracing, on-premises diagnostics support such as thermal temperature checks, and other point-solutions that provide immediate, tactical value against targeted infection related issues. An open issue, however, is the lack of a "connective tissue" that pulls together these various point solutions into a comprehensive, organizationally focused system to manage infection risk. This issue is best addressed by a well-architected, infection management specific, digital platform - referred to as an **Infection Risk Management Platform** (or **IRM Platform**) for the remainder of this paper.

This document is targeted at senior leaders who have a strong desire to lead recovery at their organizations. An executive presentation of the content in this document is also available. The remainder of the document will provide details to support the summary provided in this section.

Understand the Context

The COVID-19 pandemic has disrupted life worldwide. Families of COVID-19 victims have experienced tremendous pain. Social distancing has children staying home from school, people staying away from their friends and family, and for many, staying out of the workplace. Businesses, universities, and places of worship are shut down. No organization has been spared and supply chains have ground to a halt. The ripple effect of this pandemic has yet to be fully understood - but with comparisons to the effects of the Great Depression and World War II, it's clear that the impact is unprecedented in this generation. COVID-19 will leave a forever, irreversible imprint on how we work and live - a "new normal" as many have described it.

A March 25th, 2020 McKinsey & Company presentation entitled "*COVID-19: Briefing note*" outlined five "horizons," or phases, that business leaders need to execute against if they're to successfully navigate their companies into a position of strength in the "new normal." These five phases - R*esolve, Resilience, Return, Reimagination, and Reform* - require people, plans, and tools to succeed. Two key stages, Return and Reimagination, are the stages our clients are targeting with their near term plans. The primary focus of this paper is the Return stage given that it's the most pressing, along with a digital implementation supporting the execution model outlined in the McKinsey & Company briefing note.

Return and Reimagination stand for the **reopening** of industry and a period of **reinvention**, respectively. For each organization, reopening requires a return to the capacity that it had in the pre-COVID era. But they need to do so via an **Infection Risk Ready** approach. A successful reopening ensures a stable operating foundation that will allow each organization to then *reinvent* its approaches, products, and services to fit a post-COVID era. Without reinventing what they offer and how they offer it, organizations will not maintain the product-market fit or socially-aligned operating model that they once enjoyed. They'll need to accelerate their digital strategies and build the platforms necessary for the post-COVID era.

There are two substages to reopening: **(1)** a "bolt-on" substage that leverages point solutions and processes with an emphasis on achieving some semblance of a shared workspace as soon as possible and **(2)** a "strategic" substage that follows the "bolt-on" substage which modifies the organizational operating context to be *efficient* in a pandemic-conscious era. While important tactical deployments are solving for the immediate challenges in **(1)**, this paper and proposed platform concept focus on the strategic reopening defined in **(2)**, with an emphasis on leveraging the tactical investments made in current "bolt on" models.

Architecting an IRM Platform, however, requires establishing an important ground-truth: most large organizations operate as a federation of locations and clusters of people who vary wildly in their type of work and as a result, in their individual exposure to infection risk. It would be hard to disagree with the statement that a worker in a warehouse and a software developer working for the same company are exposed to infection risk in different ways. This difference in OE is what makes one OE a different "shape" than another OE.

The key to strategic reopening (and the underpinning for post-COVID operations) is being Infection Risk Ready. This means operating under the assumption that infections *will* continue to happen, and understanding how that assumption needs to be managed in the context of the entire organization.

Those of us who build cloud and distributed systems for a living purposely "design for failure". Failure is expected, so we build systems that are resilient and can recover quickly. That mentality needs to be applied in this context. Society has been battling with infectious diseases for all of recorded history. With a population larger, more densely organized, and with more human-to-human interaction than ever before, any assumption other than "failure will happen" would be negligent. Even if a vaccine for COVID-19 develops, nothing prevents a new virus or superbug from emerging, putting the world at risk again. In a recent note entitled "The First Modern Pandemic" by Bill Gates, he refers to this current outbreak as Pandemic I. The numbering scheme is not an accident; it's a foreshadowing. Infection Risk Ready strategies and tools can be used to respond to infections and mitigate the impact on an organization and its people.

Maintaining a perpetual Infection Risk Ready posture requires that an organization be able to continuously:

1. **Verify**: Verify the infection status for all members and locations of the organization
2. **Manage**: Manage interaction and communication protocols between members based on real-time changes in policy and infection context
3. **Respond**: Rapidly react to the suspected introduction of infection to their workforce or places of work, invoking policies & protocol defined in (2)

Handing your leaders a 50 page PDF on managing infection risk is not enough. These three Infection Risk Ready criteria (**VMR**) require the introduction of new processes to the employee work model as well as new digital tooling to provide the backbone to implement those new processes. No solution can achieve 100% success; perfection is not the goal, but laying a foundation that can be constantly improved through iteration is the goal.

Challenges to Reopening

One of the most important metrics calculated by epidemiologists in evaluating infection risk is the infectious agent's *Basic Reproduction Number* or **R0** (pronounced "are-nought"). **R0** is a propagation ratio that measures how many people a given infected person will go-on to infect. An **R0** larger than 1 indicates that an infection will spread across a population. Generally, the larger the **R0**, the larger the proportion of the population that will get sick.

While **R0** doesn't tell the whole story (for example, it says nothing about propagation speed), it does tell us the impact one infected individual can have. It also tells us what sort of impact taking that individual out of social contact can have (hence social distancing protocols). By identifying the individual as early as possible, as well as any individuals they may have been in contact with, we can 'prune' the propagation tree and reduce the net future infection count in a group.

This is the core concept behind *contact tracing*. Contact tracing is the process of identifying as many individuals as possible that a known or suspected infected person has come into contact with, working with those individuals to distance themselves from others, and monitoring their infection status closely. This is what 'prunes' a sub-tree of propagated infections from a group of people and dampens the net infection outcome by reducing **R0**.

Contact tracing is a strategy recommended by nearly all health organizations (including the Centers for Disease Control and the World Health Organization) as a way to manage infection risk but is mostly discussed in a general sense across the broader population. A top-down, government-mandated contact tracing system is unlikely to be implemented in the United States. A government contact tracing system is much more likely to be optional and scoped. Private entities, however, can require targeted proximity tracing (with privacy controls) within their organizations as a mechanism to accelerate reopening. It's also the **only way** to allow the safe, continued interaction of people within those organizations in this post-COVID era.

The challenge, however, is the shape of each OE. An organization works across the shape of its OE, with team members of different work-styles interacting with each other across floors, buildings and even locations. While organizations might have OEs with different compositions (take a university versus a multinational corporation, for example) the fundamental OE interactions are similar and can be mapped. A person from one location within an OE, for example, might interact with someone from another location, each of whom can inadvertently introduce infection risk to the other. This means that structurally, infection can propagate through members of the OE much like how an infection propagates through groups of individuals. In a way, this implies that a sort of **R0** propagation quantifier - or **T0** (pronounced "tee-nought") in this paper - exists for organizations. This **T0** attempts to quantify infection propagation across an OE.

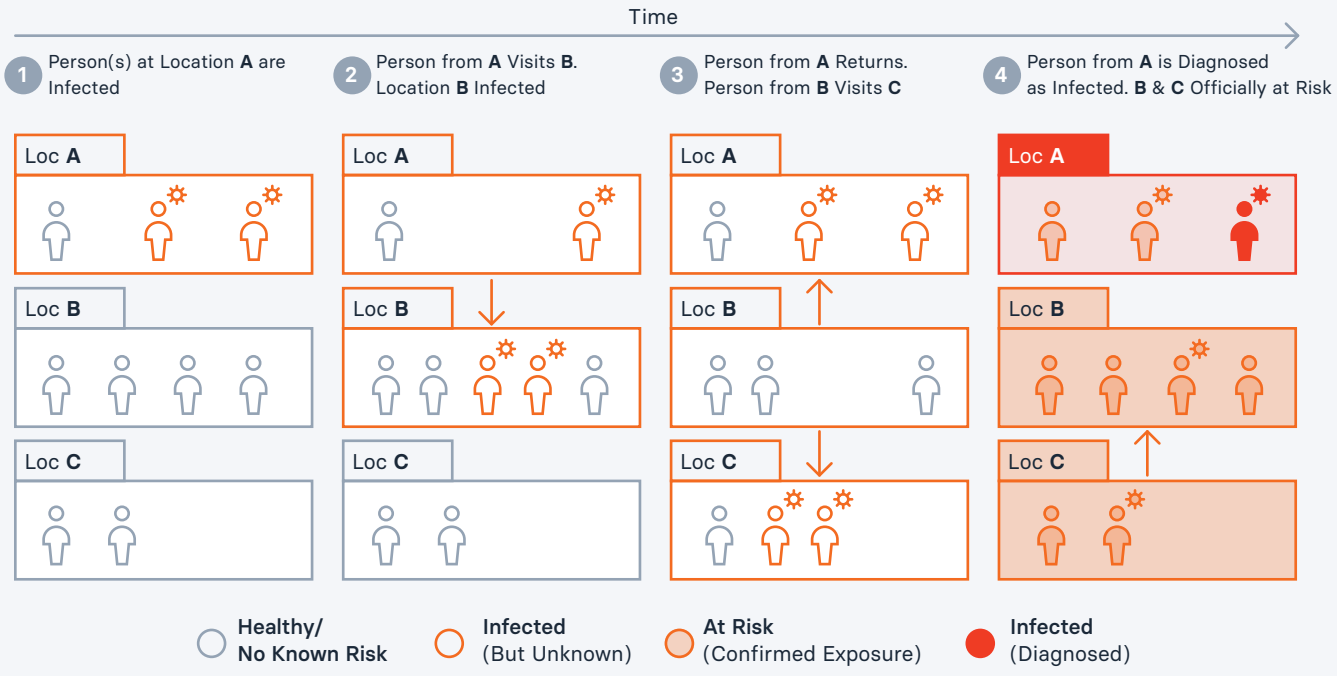

Figure 1: Transmission Risk in an Organizational Entity

T0 is a function of the infection risk posed by each individual, their work-type, the details of their location (address relative to macro-infection clusters, building location, floor, and even desk location). For clarity, an organization that is entirely remote (e.g. the OE has no physical locations, every person works from home and no one ever meets any other team member in person) has a **T0** of zero. Why? Because although individuals may become infected due to external concerns, they can never propagate that infection to people or places within the OE. Conversely, an organization with very few, densely packed locations with a physically interactive workforce will carry a high **T0** given that infection propagation risk is very difficult to reduce.

Now that we understand that the structure of an OE can pose infection risk to the rest of an OE, then a logical conclusion would be that an organization needs to minimize its **T0** through regular management of its OE and internal interactions. **Being aware of and managing T0 is the core definition of being Infection Risk Ready**. But how does an organization actually manage its **T0**? OEs suffer from a "weakest-link" structure when it comes to infection risk. Any part of the OE that is infected poses an immediate risk to any physical "links" it has to other parts of the OE. Infections do not respect physical boundaries, and by definition, solutions must follow infections across these boundaries to neutralize them. This means policies, protocols, monitoring, proximity tracing, and contact tracing *must* be OE-aware. For example, policies, protocols, monitoring, proximity tracing and contact tracing would be very different for those who work at a factory location than those who work at a software engineering center.

The safest OEs are those with complete participation in Infection Risk Readiness. For example, proximity tracing within a single location may not be enough if there is a direct or indirect physical link to another location. Implementing a solution at one location does not account for members of the OE crossing boundaries - whether its team members visiting offices or university professors lecturing in a building that isn't their normal campus location. This is not a surprise given that we have seen this at a global-scale; countries that brought COVID-19 somewhat under control through aggressive policy experienced a spike in cases when travelers from locations with more lax controls visited. Infection Risk Readiness requires a unified, co-operative approach across an OE, which in turn poses a number of questions that need to be answered:

1. How does an organization solicit participation from its own people to achieve Infection Risk Readiness?
2. How do members of an OE determine who within their OE have practices that are more or less healthy than another?
3. What are organizations supposed to do in cases where a suspected infected person crosses a physical link to another part of the OE? What if that infected person had no symptoms until the day after they visited, at which point they reported infection risk? How would the organization know and what should it do?
4. How would the organization map impact within its OE across more than one degree of physical separation? Can that organization determine what *indirect* interactions (if any) may have occurred between two locations through a common location?

5. How does an organization map real-time infection risk data (building access, temperature checks, self-reported health assessments) to the shape of its OE and perform necessary analytics?
6. How do organizations model cross-location potential impact to maximize the safety of their people and locations?
7. How is communication to people across physical boundaries coordinated and rapidly disseminated?

There are hundreds of questions like this. The intent of VMR is to outline cross-OE workflows and expectations necessary for successful Infection Risk Management and response, with the intent of regularly keeping **T0** to a minimum. Specific challenges are best broken down along VMR boundaries.

VERIFICATION CHALLENGES

The first challenge in verification is a strategic one and impacts the entire OE. In order to be able to coordinate Infection Risk Management across an OE, a lingua franca must exist to describe and measure **infection status**. Each person, location, and sub-location (e.g. building, floor) needs to carry with it an Infection Status - *No Known Infection, Exposed to Infection, Suspected Infection,* and *Confirmed Infection*. Additionally, a **Risk Scoring** model is needed. A single **Risk Score** should be assigned to each person, location, and sub-location. A low Risk Score is good, a high Risk Score is bad. A Risk Score is derived from tracking metrics and events in two categories:

1. **Basis Category:** A component tracking irregular events or that have systematic implications. This category captures components that make up an OE component's "base" risk status. Known location-specific policies, provable behavior, and event history all contribute to the Basis Category. The impact on Risk Score from items in the Basis Category is large but change is infrequent. For example, if a site manager has lied about an infection, a truthfulness component in the Basis Category for the Risk Scores of *both* the site manager (assuming they still have a job) and the location would carry a long term, negative implication in computing Risk Score.
2. **Active Category:** A category of metrics and events that are regularly changing and monitored. Components in this category are based on real-time information regarding known Infection Status, changes in status, measurable evidence of the use of personal or location protection, and recent interactions that may indicate exposure. The Active Category is layered on the computations coming from components in the Basis Category. That is, one person, place, or location with significant negative impact from components in their Basis Category will have a worse Risk Score even if their Active Categories are roughly the same.

A person's role in an organization and their associated duties impact their Risk Score. For example, an individual working in a warehouse has a very different inherent Risk Score than a person who works remotely for an organization from their home office. A professor who travels regularly to give talks may carry a different risk score than a professor who prefers to lecture in the classroom. The formula for calculating risk scores may be different across organizations and will change over time as we learn more about infection in the workplace. New inputs to this formula, some unique to a specific organization, will emerge. Any digital solution needs to be highly dynamic, extensible and customizable to the shape of a given OE. Although the composition of the formula will change overtime, certain truths remain with respect to infection. If any person or location is suspected or confirmed as being infected, certain rules apply:

1. The Risk Score for the organization is derived from individual Risk Scores in a composite way
2. The introduction of risk and changes in Infection Status and/or Risk Score may result from changes in the same *anywhere* within an OE
3. A direct relationship between members of an OE poses a higher risk implication than if members of an OE are 2+ degrees apart

Other verification challenges are more tactical. Verification requires individuals in an OE to either self-report or report on what they observe in their environment. This is the least invasive case of Infection Status verification and Risk Scoring. The strictest case requires that organizations either request each employee to authorize regular employer-administered testing or to submit to testing by a registered health professional. Each of these approaches presents their own challenges:

1. Organizations will have to solicit honest self-reporting from staff. Many may be reluctant or nervous to self-report accurately, either because they're nervous about privacy, social stigma, or they're nervous that self-reporting may reduce their work hours (and their paycheck)
2. Self-reporting may result in false-positives for those who are over-assessing the gravity of their symptoms
3. Employees may not know that they're sick with an infection. They may be asymptomatic or may be under-assessing the seriousness of their symptoms
4. Employees may refuse to allow their employer to test them
5. Employees may not have the time or willingness to visit a health professional for testing, or organizations may not be accommodating
6. Parts of an OE (e.g. a specific office or warehouse) feign verification compliance, leading to a lack of compliance provability for certain parts of an OE

If all of these challenges are solved, an organization is capable of high fidelity Verification. For each challenge that goes unsolved, said fidelity is degraded. Given that each organization will have varied success in solving each challenge, verification fidelity will lie on a spectrum. In the near term, however, certain compromises in fidelity will be purposefully made. Many organizations will likely error on the side of caution and accept a high false-positive rate. Over time, reducing false-positives will prove to be an optimization that a digital solution can help power. Negotiating protocol and action within an OE is a non-trivial task. This all impacts how an organization can Manage and Respond, thereby impacting Infection Risk Readiness.

MANAGEMENT CHALLENGES

What should an organization do when one part of their OE with a low Risk Score has a physical interaction with a part of their OE that has a naturally higher Risk Score? What if the former finds out after a visit from the latter that one of the visiting employees tested positive *after* a visit? This is partly influenced by policy and the safety rules each organization follows. This is a question of Management. Challenges in implementing good Management include:

1. Having to decide what is "too risky" when signals are ambiguous. For example, in credit scores, credit inquiries, account age, and credit utilization all impact credit score.
2. Knowing what is verifiably safe versus not, and defining what to do if verifiability is not possible
3. Communicating why a decision was made to change plans
4. Documenting decisions (along with supporting data) in a formal way to ensure alignment
5. Understanding how to shape policy based on the policies of directly connected organizations in a given OE, or even based on those more than 1-degree of separation

Being able to receive and interpret information related to infection risk is critical for making effective management decisions. The core issue is that the information for making good Management decisions is often 2+ degrees away. No solution can ensure perfect decision making in these situations. Currently however, most organizations are flying blind and need a starting point that makes the overwhelming nature of the problem manageable.

RESPONSE CHALLENGES

Spending time on "if and when" an infection might happen or on infection avoidance within an OE is not a sufficient approach. We've established a "design for failure" mindset earlier in this paper, which means the focus should be on responding to assumed infections. Every part of an OE needs to be prepared to respond whenever any part of an OE suspects or confirms infection. This is a non-trivial task. It requires overcoming the challenges of:

1. Root cause identification of the infection risk
2. Proximity tracing, contact tracing and evaluating net exposure
3. Notification of potentially at-risk parties (e.g. employees, suppliers, customers, family and friends)
4. Remediation of contaminated locations using prioritized scope. For example, while one-thousand employees might work in the same multi-floor building, on average, inter-floor traversal happens much less frequently than intra-floor traversal.

Response coordination within an organization and all of its OE parts needs to be data-driven. Making a mistake during the response phase can be costly, delay recovery, and dilute the impact of remediation. In fact, an "early release" peer-reviewed study from South Korea showed the positive effects of a rapid, albeit manual, response to infection risk in a call center in one of Seoul's busiest office buildings:

Figure 2: (Blue seats were confirmed infections)

In this case in the Seoul call center, the first infection was reported on March 8th, 2020, with a shutdown of the building on March 9th, 2020, followed by an intensive, human-driven cataloging of people within and around the building. This cataloging led to manual contact tracing, which resulted in sending 16,628 text messages to inform people of quarantine expectations. The result of this rapid response is best described visually through the floorplan in **Figure 2**: the effect of rapid response was containment precision that isolated the infection to just a part of a floor in the building. *The only "failure" in this response was that it was predominantly a manual, non-technology oriented response since no tooling exists to support a response of this type. Without proper tooling, it would be impossible to scale this sort of effective response tactic across buildings and people within an organization (at least not without an army of infection response personnel).* **The core intent of an Infection Risk Management platform would be to provide a digital backbone to planning for and solving against this case study efficiently, effectively, and safely.**

If an organization is not equipped to overcome VMR-related challenges, it will fail because *reopening* will fail. It will never earn the opportunity to reinvent itself for a post-COVID era. Right now, most organizations are tackling response with their best effort. This has resulted in total shutdown. Incremental improvements to response readiness helps get society out of total shutdown. These incremental improvements can start with organizational processes supported by technology investments that simplify those processes.

A Digital Platform as the Path Forward

If the current context arose in the 1800s and the aforementioned challenges were outlined, it would be impossible to implement a solution. Why? The tooling for even partially automated approaches didn't exist. In fact, the ability to create a holistic solution would have been challenging even a few months ago. We can see evidence of this in the South Korea call center case study described as part of **Figure 2**, where a positive outcome was achieved through significant manual intervention with little support from purpose-built solutions. The outcome in the South Korea call center case study should serve as the canonical problem model for any solution to tackle if it intends to be effective. Success for a solution should produce equal or better results to that case study, but with a massive reduction in effort and cost.

Technology point solutions are emerging to help. In response to COVID-19, Google and Apple embarked on an unprecedented joint partnership by deploying capabilities in each of their phone OS' allowing for cross-platform contact tracing. Also in response to COVID-19, protocols for phone-based contact tracing such as OpenTrace have emerged. But these are *not* solutions; instead, they are foundational elements to solutions. They are not holistic, integrated or focused end-to-end efforts for dealing with Infection Risk Readiness.

For organizations to succeed in reopening and to be able to reinvent post-COVID, they need a platform to track and analyze data in realtime and execute VMR.

A sampling of expectations to execute a continuous VMR model is to allow for (at a minimum):

1. Infection-risk reporting (through self-reporting as well as allowing for proxy reporting when symptoms are observed in 3rd parties)
2. Proximity tracing, if possible, to allow for a rapid inventorying needed for effective contact tracing
3. Technology supported contact tracing of infected parties across OE boundaries
4. Rapid response to remediation needs to aid corporate infection containment attempts

But why is a digital platform required? Why not just build an app and call it a day - what's wrong with that? Apps tend to solve problems in a fixed way for a fixed set of problems. Apps are not built to be extended, let alone by a set of globally distributed organizations and developers. Apps are not designed with a reusable set of APIs and primitives needed to assemble complex solutions from those primitives.

Viruses and bacteria mutate, evolve, and change. They jump from one species to ours, suddenly introducing themselves into our lives and quickly changing our reality in extreme ways. A digital response platform needs to adapt and iterate at least as fast as the virus it's trying to contain, otherwise the solution is guaranteed to become wholly ineffective overtime.

To solve for the constantly changing environment related to infections, we need a solution that can be quickly extended and that supports a decentralized value creation and distribution model. That solution needs to allow for taking new knowledge and equipping the ecosystem that is using it to extend itself in ways that solve emerging problems. All organizations are different. There is no "one size fits all". Policies will vary by vertical, country, climate, workforce demographics, etc. Solutions need to be highly customizable and evolvable, which is what platforms uniquely enable. With so much uncertainty in the months and years ahead, platforms are not only sufficient, but necessary since they are designed to be used in ways that we cannot fully predict in advance.

At Nuvalence, we've applied significant rigor to defining application/software reuse taxonomies and building global-scale digital platforms. We can, with certainty, state that only a digital platform can solve the challenges defined in this document. Applications, frameworks, libraries, or APIs simply won't suffice.

For the specific challenge within the infection risk management domain, only an Infection Risk Management Platform would solve the challenges outlined in this document at global scale. This platform would provide a base set of reusable primitives that would equip the ecosystem to quickly write new code to extend and enhance the platform as reality changes and new types of threats emerge. Only through this model can the world have a solution that evolves as quickly as a virus spreads. Any other technical model is either a point solution or wholly ineffective; a holistic, extensible platform capable of cross-organization infection risk management is the only approach.

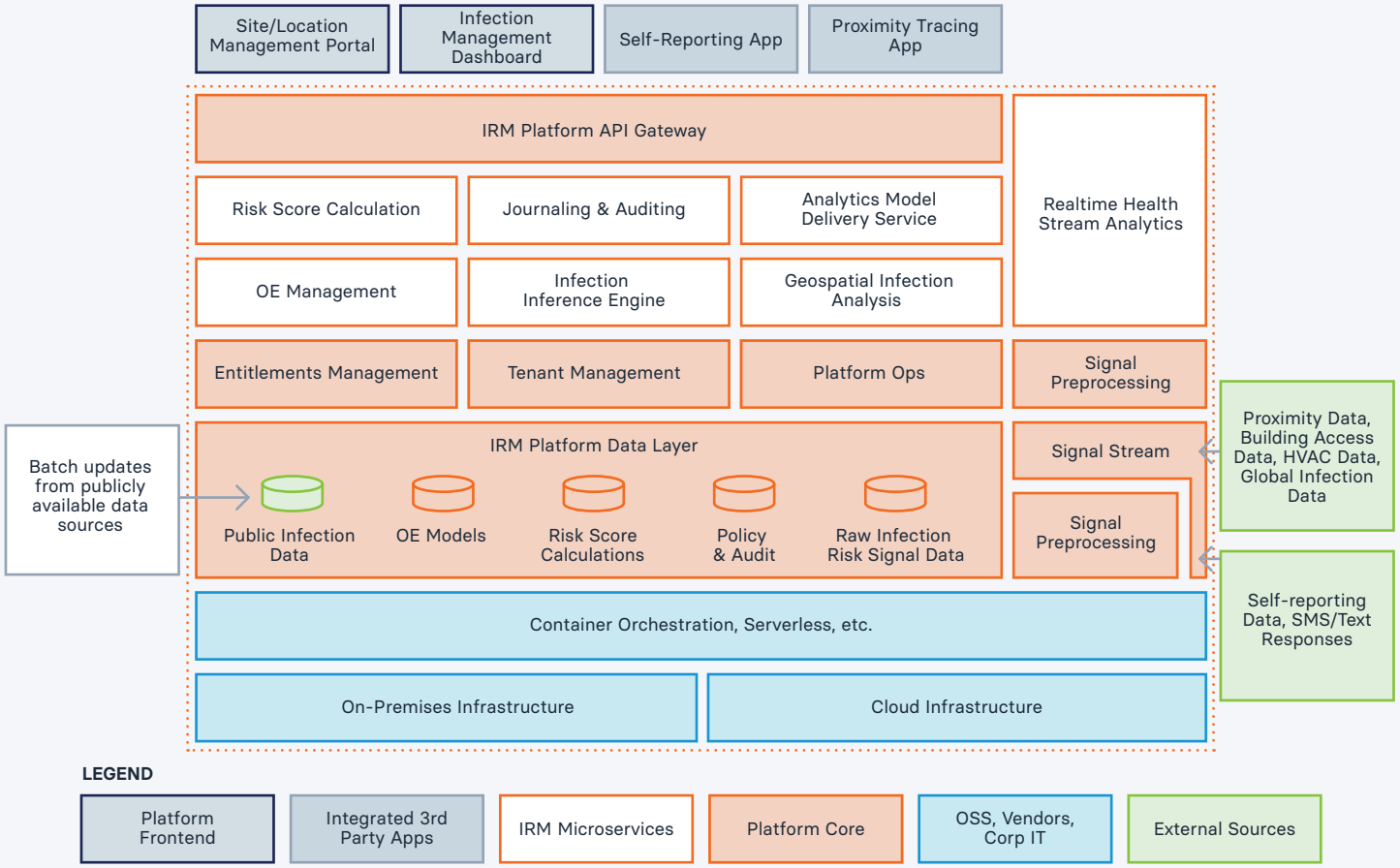

Figure 3 IRM Platform Reference Architecture

Parties within an OE share the same IRM Platform, allowing them to develop the communal defense discussed in this paper. This will not only aid in recovery, but will be the basis for competitive advantage in the future. Many organizational leaders will wonder whether they should wait for an "off the shelf" solution. Unfortunately, waiting is not a luxury anyone can currently afford when dealing with an urgent, safety related context. What organizational leaders can and should do is align with an IRM Platform model approach that can provide a re-usable core to an eventual "off the shelf" solution.

Priming an IRM Platform

An IRM Platform needs to be primed with critical data from the onset. Success in reopening and stabilizing the go-forward operating model requires two things: to be able to track Infection Status across components of an OE and to integrate Infection Status signals from the OE into the decision-making process. Each organization must be confident that all parties in their OE are also managing infection risk with the same level of rigor. The only way to ensure this is to inventory the appropriate data and recruit all parts of the organization into the OE Infection Risk Management model. This information enables the creation of an appropriate Risk Score model for the OE. Some examples of necessary data gathering exercises include:

1. Categorizing all people within the organization by worktype/physical interaction frequency. For example, someone who interacts regularly with individuals external to the organization (such as a delivery person) has an implied risk category that is higher than someone who works in a warehouse but interacts primarily with people within the warehouse, who may be higher than someone who works in an office with infrequent interaction, who is likely higher risk than a remote employee who rarely never comes to the office. An expansion of this framework would propose a set of default categorizations, which could then be tailored for each organization.

   People without modern devices (e.g. smartphones) should be documented as well, since they may need supplemental support to properly participate in an IRM Platform.

2. Inventorying the Infection Status of all people within the organization at the highest fidelity possible through an app that is integrated with the IRM Platform. Direct testing or healthcare verified testing is preferred over self-reported symptoms and status. The latter is still better than nothing (given a "Good Samaritan" assumption).

3. Fine-grained inventorying of location information down to the floor plan level (if possible)

4. Cataloging of all systems pertinent to managing infection risk at a location, including but not limited to: building access systems such as keycard systems, visitor check-in systems, HVAC systems, elevator systems. Where possible, systems that are accessible by API should be noted so that real time signals from each can be incorporated into the IRM Platform's scoring and management system. For example, the IRM Platform should know if fresh air circulation through HVAC has failed, which in turn may initiate communications to individuals who work from that office or warehouse to either leave the building or not come to the building if the failure happened over night.

5. Modeling the relationships of the OE structure, particularly who works from what locations (down to the floor plan level), and the physical relationships between locations (e.g documenting common traversals between locations)

   In order for an organization to ensure the safety of its own workforce, it must ensure that all parts of its OE take Infection Risk Readiness seriously. Any part of the OE that is not capable of meeting the policy needs established by the IRM Platform, needs to be documented and considered at a different infection risk level than the rest of the OE.

   These modeled relationships will be registered with the IRM Platform and used to enable organization proximity and contact tracing, allowing for Infection Status and Risk Score management across the entire OE.

6. Capturing information regarding the "refresh cadence" of critical Infection Risk signals. For example, detailing how often buildings will be cleaned or how often temperature checks will occur. This sort of information will help determine the regularity of Risk Score updates.

7. Protocols and response plans between parts of the OE should be defined, and each OE member should craft their own protocols and response plans tailored to their unique needs.

8. Partners, suppliers, and 3rd parties from the organizations ecosystem who **regularly visit** should be inventoried as well. Initially, this information would be used to manage infection risk introduced by visitors, and can be dynamically updated through integrations with visitor check-in systems. Overtime, the IRM Platform could solicit direct participation of an organization's ecosystem for a stronger, cross ecosystem infection risk management model.

Assessment and assessment-informed processes are required for each organization to define a tailor-fit organizational framework. The aforementioned are for guidance; they simply scratch the surface and require consultative support to define in depth. Fundamentally, you're going to take in highly dynamic signals that impact infection risk for individuals and organizations. You'll need to process those signals through an extensible policy framework and decide what actions to take next.

Conclusion & Next Steps

This document has outlined just the beginnings of a transformative journey. Despite covering a significant amount of content, this is still the tip of the iceberg. Building a comprehensive solution would take years.

Our job is to help organizations get started with practical tools needed to achieve early success, setting the foundation for thriving in the long term.

We're not going to release something that solves all of this, nobody is. But we can make meaningful headway. **We need to get started now**.

There is one truth that needs to be acknowledged: every organization must invest time, energy, and money in preparing for this "new normal." Any approach to recovery and long term reinvention that does not include a communal defense model via a IRM Platform will have a much lower chance of succeeding. The right processes provide the execution framework, a digital platform provides the continuous monitoring and adaptation needed to evolve alongside infection risk, and having a community of organizations that coordinate their approaches creates the most gap-free model possible.

Nuvalence plans to release a IRM Platform and associated consulting offerings to tackle the challenges outlined in this document and to support an expanded version of the proposed framework. For additional information or to participate as a commercial partner, send an email to new-normal@nuvalence.io.

Even if you don't work with us, we hope that you'll be able to use our thinking as a framework and take some of the digital assets that we generate to help accelerate your own individual strategies.