6 Vital IT Operations Capabilities for Emerging Companies

All too often, emerging companies face sudden, costly IT challenges, especially during periods of growth. Rapid growth is the exact wrong time to establish scalable IT operations. Broken processes, missing skills, unorganized data, compliance issues, and cyberattacks aren't just operational problems, they're hindrances to future growth. Fixing these problems after the fact is costlier and more time-consuming than establishing effective IT operations in the first place.

But what does "effective IT operations" look like for your organization?

Here are our 6 recommended capabilities that emerging companies need to build a more robust IT structure.

1 Data and Document Structures Organization, Accessibility, and Permissions

In most emerging or growing organizations, documents and data are scattered across countless employee laptops and cloud storage apps, making security, control, and accessibility a significant challenge. Setting clear standards for data storage and access early is critical to ensuring all your data and files are manageable.

Key Practices

- Set clear standards as early as possible
  - The longer you wait, the less manageable and more expensive getting everything under control will be
- Facilitate complete, secure data backups with well-organized data
  - Backups are your first line of defense against increasingly-common Ransomware attacks

2 Scalable Onboarding Process

As your company scales, you'll need to hire new staff to keep up with the growth. Whether you're hiring onsite workers or remote workers, (but especially if you're hiring remote workers!) establishing a scalable onboarding process will help you save hours of setup now and even more down the road.

Key Practices

- Document new hire, procurement, and termination processes
- Standardize hardware/software configurations
- Implement Single Sign-On with automated provisioning for enterprise apps as well as Multi-Factor Authentication
  - Eliminate the headache of managing numerous logins
  - Protect employee credentials from being compromised
- Gain an audit trail of system permissions for compliance and security

3

Unified Endpoint Management

With remote work becoming a reality for nearly every emerging company, control and visibility of company devices are paramount to ensuring security and maintaining data organization. As you hire new employees, unified endpoint management allows you to better support them while protecting critical enterprise assets.

Key Features

- Real-time inventory of all hardware and software assets, both remote and local
- Monitor and enforce patching, encryption, backup, and required security setup
- Remotely install new applications with ease
- Remote lock and wipe when equipment is lost or stolen
- Granular, device-level permissions to systems and data
- Enables Data Loss Protection strategy to prevent important IP from escaping

4

Endpoint Detection and Response (the new anti-virus)

Last decade's antivirus solutions for individual devices provide nowhere near enough protection to combat the complex cyberattacks of today. Integrated real-time intelligence from endpoint, network, and applications allows endpoint detection and response solutions to identify and respond to complex threat behaviors instead of just individual events. Analytics help identify root causes and understand the actions needed to remediate them.

Key Features

- Real-time protection from Viruses, Malware, Ransomware and Phishing attacks
- Recognizes patterns of attack across multiple devices
- Provides remote and on-premise workers with a single integrated layer of protection
- Backed by 24x7 security operations center (SOC) to rapidly counter emerging threats

Endpoint detection and response technology is still new, but the right provider will put you on the path to countering evolving threats for years to come.

5

Security and Compliance Thinking Everywhere

When it comes to security and compliance, even a simple mindset change can go a long way in shaping best practices for your company as it grows. What might just seem like boilerplate exercises will actually have a real impact on your company's security and compliance and require careful planning to avoid much bigger problems down the road.

Key Practices

- Every system design should include details on security policy and compliance support
- All IT reports and plans should monitor security metrics and compliance issues routinely
  - They must be completely inseparable from all IT operations
- Policies for security and incident management should be in place before they become necessary

(408) 550-8007 • sales@kaliotek.com

kaliotek.com • 19200 Stevens Creek Blvd., #110 • Cupertino, CA 95014

KalioTek™

6 Durable IT Staffing Strategy

Your IT is only as capable and as stable as your IT team. IT is PEOPLE, processes, and tools. Often, too much emphasis is placed on the tools and processes. It becomes easy to overlook the value of committed, knowledge-able people to run them in the midst of rapid change. Industry wide, IT employees typically change jobs every 18-24 months. Even with adequate documentation, which isn't common at all, a lot of knowledge walks out the door when an IT employee leaves. This translates into unforeseen costs for the organization in the form of recruiting, training, and lost productivity during ramp-up of new IT employees. Investing in quality IT team management always pays dividends.

Key Practices

- Make sure your team has the tools they need to do the job
- Set detailed documentation processes in place in preparation for staff turnover
- Consider bringing in an IT services provider as a backup team to provide fractional roles and augment staff as needed.
    - Outside teams can hold institutional knowledge of your IT and security capabilities and fill missing roles temporarily, smoothing inevitable transitions.

If you're interested in learning more about these capabilities or how to enact them within your own organization, please feel free to contact KalioTek today.

About KalioTek

KalioTek's mission is to partner with growing life sciences organizations to provide access to a wide range of IT and security expertise in a flexible, as-needed, and affordable model. Since 2002, our team has served hundreds of emerging and midsize companies. Our client base requires that we stay on top of IT and security technologies as they evolve and understand the solutions that are appropriate for this specific market.

For more information or to inquire about how KalioTek can help your company with some of the solutions described above, contact us at 408.550.8007 or sales@kaliotek.com.

(408) 550-8007 • sales@kaliotek.com

kaliotek.com • 19200 Stevens Creek Blvd., #110 • Cupertino, CA 95014

KalioTek™