Cyturus™

Provision® by Exclamation Labs

Assessing Your Cyber Maturity:

Is Identity Management Your Achilles Heel?

How Banks & Credits Unions Must Address Cyber Risk:
Ways to Identify and Prioritize Solutions

- Explained and Exposed: The flawed notion that "cybersecurity is an IT problem"
- Prioritize business-driven IT investment decisions with the Cybersecurity Maturity Index
- Deliver foundational security & business efficiencies with Identity Access Management

August 2020

Contents

Leadership Messages

Robert Hill, Founder & CEO
Cyturus Technologies, Inc.

Understanding the business impact of cybersecurity and the associated reduction of cyber risk has become common in today's executive board rooms.

Cyturus concentrates on identifying, measuring, and prioritizing the remediation of business risks associated with cybersecurity. By focusing on the cyber risk to the business, we help organizations move from an IT controls framework to an adaptive risk model. This shift enables a more proactive security posture, which is both measurable and quantifiable.

A critical foundational element to measuring and reducing cyber risk is an effective Identity and Access Management (IAM) program. Our cross-vertical analysis indicates a consistent correlation in an organization's ability to manage IAM and the reduction of cyber risk successfully.

Post-implementation maturation analysis reveals Provision by Exclamation Labs significantly improves an organization's IAM effectiveness and provides the IAM management tools necessary to support a quantifiable reduction in the IAM associated business risk.

It is our pleasure to work closely with Exclamation Labs to provide FinTech customers with a mature identity access management solution, effectively closing the gaps in this critical domain.

Jonathan Hutcherson, Founder & CEO
Exclamation Labs

After learning about Cyturus, Exclamation Labs knew building a working relationship between our two companies would create tremendous synergies. This whitepaper is an initial step. Cyturus shares our belief that cybersecurity needs to be the focus of the entire organization, not just the IT department.

We are dedicated to digital greatness. This is a saying that we frequently use at Exclamation Labs, and it has never been truer than it is in 2020.

Many companies benefit from an automated solution to manage employee account provisioning securely in multiple systems. Financial institutions, in particular, have specific requirements for cybersecurity and regulatory compliance. However, "right-sized" identity access management systems for community banks and credit unions is a remarkably unmet need. The technology experts at Exclamation Labs created Provision to meet that need.

Provision takes the manual burden of provisioning accounts and tracking user access off the shoulders of the HR and IT teams. The business impact includes a 5-6x decrease in audit prep time and resources, an increase in operational efficiency scores, and hardened security.

I couldn't be more pleased to work together to help explain the urgency to prioritize and implement security practices to accelerate the maturity of your organization's cybersecurity.

Data is Gold

Introduction

To establish the basis for protecting something of value there are basic foundational building blocks that must be in place and fundamental questions that must be asked. This holds true in business as well. We must ask the Who, What, Why, When, and Where questions, but not necessarily in that order:

- Where is the asset?
- Why is the asset valuable?
- What are the Risks to the asset?
- Who has access to the asset?
- When is the asset being accessed?

> **Too often CEOs discover too late that cybersecurity is a business problem, not just an IT problem.**
>
> **Robert Hill, CEO**
> Cyturus Technologies

Data as an Asset

Banks and credit unions have a fiduciary responsibility for protecting assets within their organization, and data is quickly becoming the most valuable asset. In 2011, the Federal Trade Commission allowed Borders to auction personal data. Later, we witnessed the auction of the RadioShack customer data as part of their bankruptcy auction. When Caesar’s Entertainment Group went into bankruptcy in 2015, creditors did not evaluate the multiple properties and land the group owned as the most valuable asset of the business. It was Caesar’s customer loyalty program data that was instead deemed the most valuable asset at $1B, lending proof to the idea that data is gold.

Consequences

Regulatory agencies worldwide have levied millions in fines on corporations under ever-evolving compliance requirements. British Airways was hit with a $230 million penalty, followed shortly by a $124 million fine for Marriott, while Equifax agreed to pay a minimum of $575 million for its 2017 breach. In addition to the financial burden of fines and penalties, lawmakers have a growing push to enact harsher legislation to hold Executives and Board Members personally liable in the event of a data breach.

From a civil liability perspective, at least one of the Equifax case's class-actions alleges that its directors and officers are responsible for the company’s stock price drop after the breach was made public. The plaintiffs allege that “Equifax’s financial statements were materially false and misleading because Equifax failed to maintain adequate measures to protect its data systems and failed to maintain adequate security and monitoring systems to detect data breaches.” A court has recently ruled that Capital One must allow plaintiffs to review a cybersecurity firm's forensic report related to the bank's 2019 data breach despite the bank's protests that it is a protected legal document. This ruling seems to facilitate post-breach civil lawsuits and potentially allows detailed breach reports to be used as evidence of knowledgeable and compliant failure by organizational leadership to provide adequate security measures.

While we are all familiar with the adage, “hindsight has 20/20 vision,” these reports, made available through legal discovery, could highlight management decisions to deny and defund critical cybersecurity projects and programs providing a direct link to the data.

Managing Data as an Asset

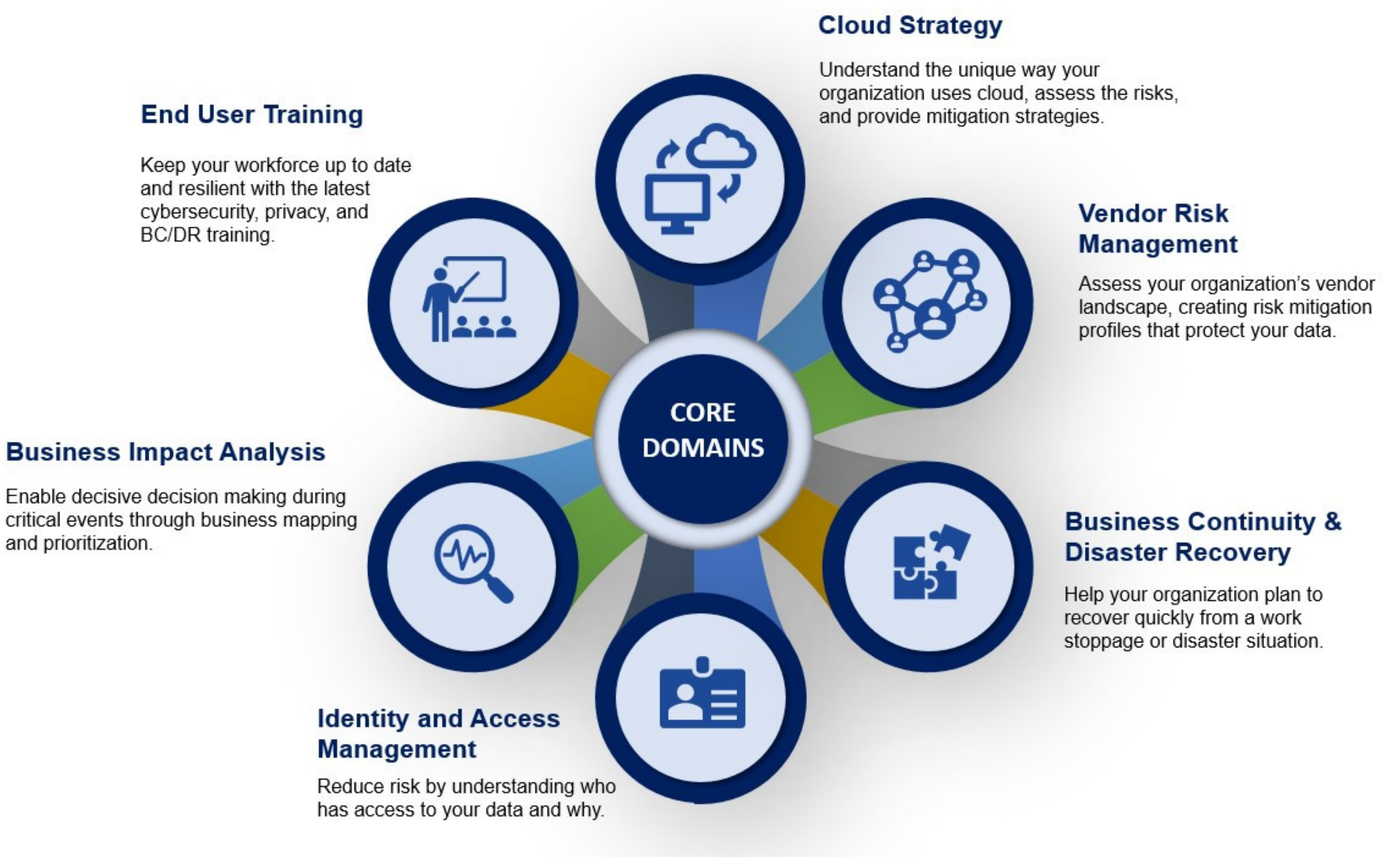
The People, the Process, and the Technology

Now that we have established data as a valuable business asset, and one when attacked can directly impact the business, we need to return to the fundamental questions of Who, What, Why, When, and Where as well as managing the answers to those questions.

Identifying the entity accessing an asset is the key to managing the risk associated with an asset. The management of this information is called IAM or Identity and Access Management. We refer to the who/what as an entity because access can be granted and used by system accounts, software inquiries, and users, to name a few. Knowing who has the potential to access, who is using their access, and the location of the entity using access is all significant information in detecting potential misuse of the asset. The inherent usage data associated with providing business services is called normalized data or data normalization. When access is requested that does not match the normal usage, it is referred to as an anomaly.

One can begin to see the potential effects of an ineffective IAM program. Legacy access to critical and valuable data from banks and credit unions no longer requiring access can have disastrous consequences. External systems access can cost millions in lost revenue, enable the fraudulent transfer of funds, and facilitate the exfiltration of data. Internal access can have an even more devastating effect on the business, including insider trading, industrial espionage, and even the kidnapping and subsequent attempt to ransom the data back to the financial institution commonly referred to as ransomware.

How does a bank manage and/or mitigate such an immense and complicated risk to the business? The answer can be found in the implementation of an efficient Identity and Access Management program. The IAM program must consist of a balance between the people, the process, and the technology.



Cloud Strategy

Understand the unique way your organization uses cloud, assess the risks, and provide mitigation strategies.

End User Training

Keep your workforce up to date and resilient with the latest cybersecurity, privacy, and BC/DR training.

Vendor Risk Management

Assess your organization's vendor landscape, creating risk mitigation profiles that protect your data.

Business Impact Analysis

Enable decisive decision making during critical events through business mapping and prioritization.

Business Continuity & Disaster Recovery

Help your organization plan to recover quickly from a work stoppage or disaster situation.

Identity and Access Management

Reduce risk by understanding who has access to your data and why.

Cybersecurity is a Business Problem

Cyber Risk vs. Cyber Security

As indicated on the previous page, we see inadequate cybersecurity has a profound impact directly on the company. A fundamental mental shift is required to move from the flawed notion that "cybersecurity is an IT problem" to acknowledging cybersecurity as a business problem and that financial institutions have an existential responsibility to secure their valuable assets, including their data. Leadership teams must think in terms of Cyber Risk vs. Cyber Security.

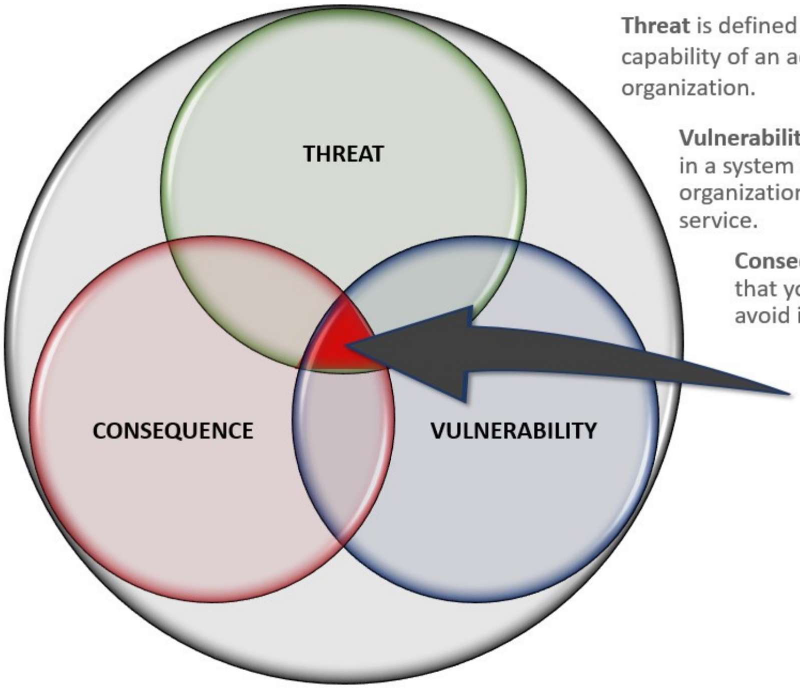
The next step is withdrawing from the widely held flawed belief that implemented IT controls alone are the answer to cybersecurity threats. While security-focused IT controls serve a valid and important function, they are not a cure-all panacea. Without measured effectiveness, IT controls provide little beyond checking a compliance box solely for the sake of checking that box. Organizations must recognize and internalize the shift toward **measurable reduction of business risk.**

> Compliance does not equate to security maturity.

Likewise, a focus on threat avoidance is necessary but, alone, does not lead to measurable maturity either.

When a bank or credit union adopts a risk-based model, the lack of compliance is seen as a business risk, and avoidance of threats is viewed as risk reduction. However, these processes alone are far from sufficient. Financial institutions must identify and **prioritize cybersecurity risks beyond compliance** and specific threat avoidance and address any risks that could impact the delivery of their business services.

Understanding and defining risk is critical to the shift in thinking from reactive cybersecurity incident response to proactive cyber risk reduction.



Threat is defined by the motivation and capability of an adversary to attack your organization.

Vulnerability is the level of weakness in a system or process used by your organization to perform a business service.

Consequence is the negative impact that your organization wants to avoid if attacked.

Risk is the convergence of a Threat against a Vulnerability associated with a Consequence to the organization.

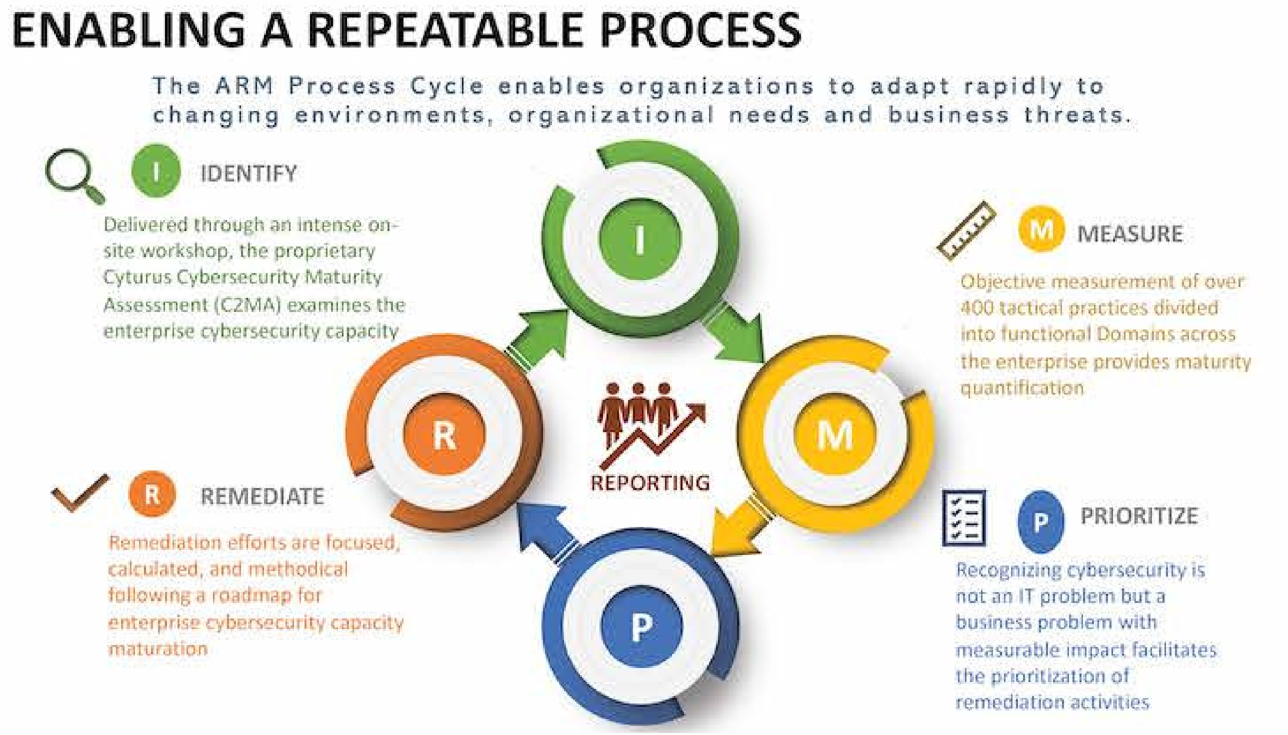
These Risks can be accepted, transferred, or mitigated based on the organizational *Risk Management Strategy*.

Adaptive Risk Model

Measurable Reduction of Business Risk

Cyturus's proprietary **Adaptive Risk Model (ARM)** enables the achievement of the proactive cyber risk reduction objective. By adopting a proven maturity model that enables rapid adaptation to constantly changing technical environments, fluctuating organizational needs, and aggregating business threats, Cyturus helps financial institutions succeed despite resource limitations and an ever-growing list of highly motivated and increasingly sophisticated malicious actors.

One of the Adaptive Risk Model functions helps businesses discover and maintain the balance of people, process, and technology with their organizational IAM program. It is imperative to have the process and governance to guide the program, the tools to provide the details and store the information, and the people to use the tools guided by the governance.



ENABLING A REPEATABLE PROCESS

The ARM Process Cycle enables organizations to adapt rapidly to changing environments, organizational needs and business threats.

I IDENTIFY

Delivered through an intense on-site workshop, the proprietary Cyturus Cybersecurity Maturity Assessment (C2MA) examines the enterprise cybersecurity capacity

M MEASURE

Objective measurement of over 400 tactical practices divided into functional Domains across the enterprise provides maturity quantification

R REMEDIATE

Remediation efforts are focused, calculated, and methodical following a roadmap for enterprise cybersecurity capacity maturation

P PRIORITIZE

Recognizing cybersecurity is not an IT problem but a business problem with measurable impact facilitates the prioritization of remediation activities

All of these actions are a critical part of an overall maturity risk game plan. Any of these services can be ingested into the Cyturus ARM Framework for deeper examination of lateral impact.

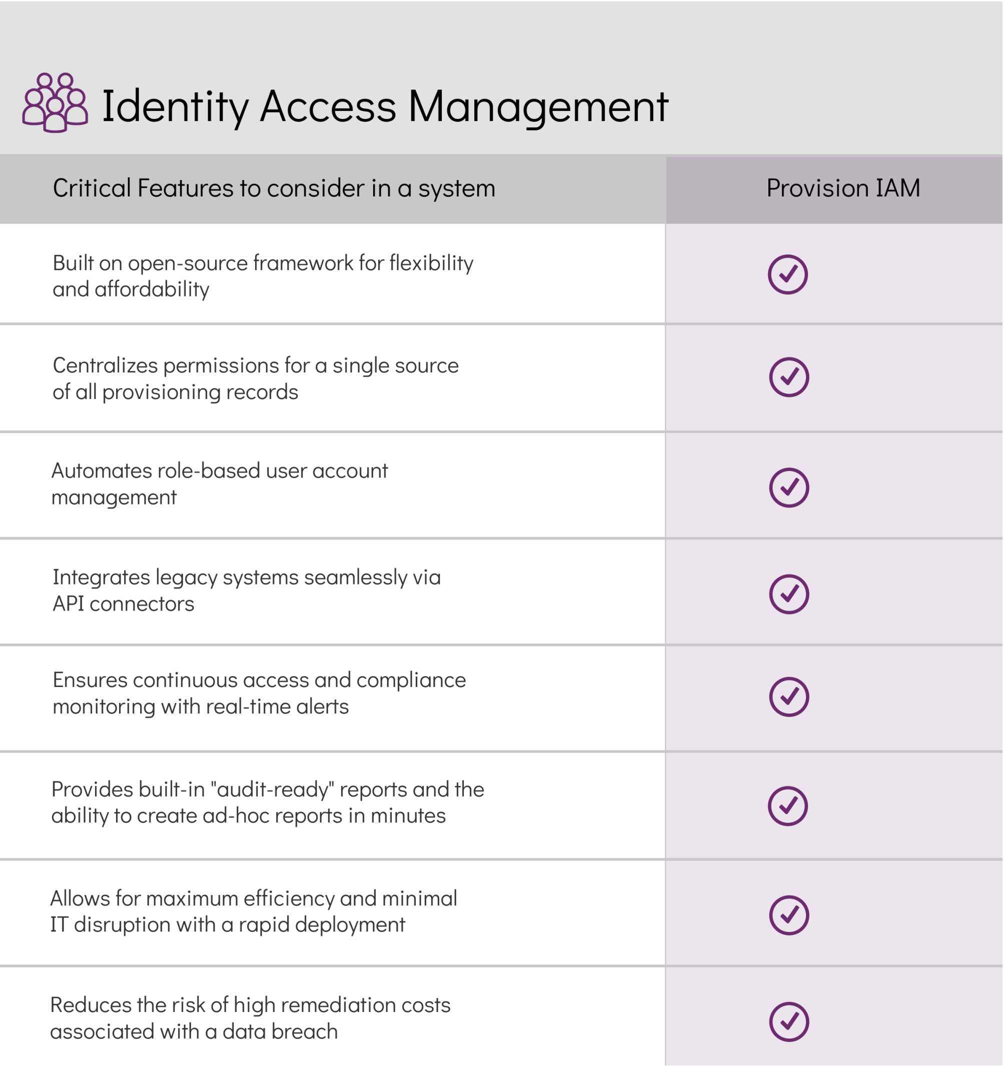
High Maturity IAM

Taking Your IAM to the Next Level

When you think of the word, "mature," you think of something that is full-grown or complete. So it's understandable that the end-goal in implementing an identity access system is that it would be mature. Your IAM solution gives employees access to the systems that they need to perform their jobs. Furthermore, businesses need to know who has access to what data, and when they access it. An effective Identity Access Management system is one of the key components of the IT infrastructure.

Your assessment from Cyturus will pinpoint which areas of your IAM system need improvement. An IAM system should be a **centralized and automated tool** to integrate user identity across systems, and enforce corporate policies. Secondly, the ability to quickly provision a user account is essential to organizational productivity. Automatic de-provisioning is just as important.

Take a look at the list below to see the other critical features that the **Provision IAM** by Exclamation Labs offers to **improve operational efficiency** and **strengthen cybersecurity.**



Identity Access Management

Critical Features to consider in a system	Provision IAM
Built on open-source framework for flexibility and affordability	✓
Centralizes permissions for a single source of all provisioning records	✓
Automates role-based user account management	✓
Integrates legacy systems seamlessly via API connectors	✓
Ensures continuous access and compliance monitoring with real-time alerts	✓
Provides built-in "audit-ready" reports and the ability to create ad-hoc reports in minutes	✓
Allows for maximum efficiency and minimal IT disruption with a rapid deployment	✓
Reduces the risk of high remediation costs associated with a data breach	✓

From the Technical Experts

Brandon Powers
Lead Developer, Provision

“In every bank we’ve worked with, teams were very focused on security. They instantly saw the need to uniformly govern system access of bank personnel and automate the rules for the processing and propagation of data. These banks saw Identity Governance as the foundation of IT security.”

David Malicoat, CISSP
Cyturus Technologies

“IAM is a lynchpin of a mature cybersecurity program. With new advancements in cybersecurity such as The Secure Access Service Edge (SASE), in addition to the challenges that banks and credit unions face with remote work, IAM will only become more critical in how technology is securely consumed.”

Jonathan Hill
Provision Installation Expert, Developer

“Banks must have granular controls on both their systems and personnel. Identity management was the foundation, allowing them to know who’s assessing which systems and what they’re doing with the data they can access.”

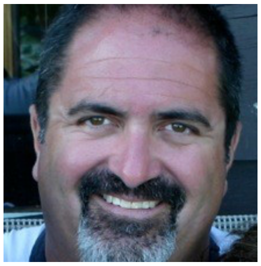
Brad Berline
Senior Product Manager, Provision

“Getting Provision ‘right’, isn’t just about security and automation— it has to make the job of the CISO or CTO easier, it has to make their daily routine less complicated. Additionally, Provision has to stand out as the defacto IAM solution for financial institutions.”

Thomas Torgerson, CISSP, CCSK
Cyturus Technologies

"Certainly, IAM will stay as one of the primary expenditures for top security executives. Everywhere I’m seeing a movement towards ‘Zero Trust’ – and IAM is the key enabler for them to manage access to applications."

IAM Thought Leadership



Lou Carli, Chief Revenue Officer
Cyturus Technologies

"With the shift to 'Zero Trust' architectures, Identity Access Management (IAM) will become more critical to managing access to applications. IAM will continue to be the number one spend priority for CISOs in 2020 and beyond."

Lou Carli's proven track record for rapidly increasing revenue and profitability for several national consultant/integrator organizations is one of the significant values that he brings to Cyturus.

Lou is a veteran cybersecurity executive with over 20 years of experience building nationally recognized sales and engineering teams. He has developed multiple large-scale channel programs and is an established expert at implementing successful channel partner relationships.

Jeff Ellis, Founder
Jellis Enterprises, LLC

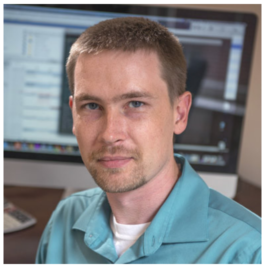
"IAM is a foundational domain of any enterprise level cybersecurity assessment program. As financial institutions evolve digitally to increase efficiency and enhance customer experience the need for robust IAM programs also grows."

Jeff Ellis is the Founder of Jellis Enterprises, LLC. He shares a passion for cybersecurity with Cyturus to help others understand that security is not just an IT issue, but rather a business problem that can be mitigated through a proactive approach.

After spending 25 years in the big data industry and witnessing the pain points related to data breaches first-hand, Jeff determined that there was a need to shift focus.

Exposure to risk is a critical factor to consider when conducting business in any industry, and thoughts on how to quantify and mitigate this threat should be top of mind for any executive. Jellis Enterprises works with Cyturus Technologies to help organizations of all sizes assess cyber maturity across their entire operation.

IAM Thought Leadership



Andrew Cope, CTO
Exclamation Labs/Provision

"Working with IT departments in Banks and Credit Unions has opened my eyes to how incredibly complex their jobs are. It's gratifying to see the astounding impact Provision can have in a short time in simplifying their jobs."

Andrew has 20 years designing and developing advanced enterprise-level web and software applications—over 10 years have been with Exclamation Labs. He holds detailed knowledge of the entire infrastructure for multiple large-scale web applications and excels in building the tooling, process, and infrastructure to support multiple development teams working together in a large production environment. Andrew is the visionary and architect behind the current Provision Identity Access Management application as well as the future subscription model version.

John Jacobs, Sales & Partnerships
Exclamation Labs/Provision

"IAM is a critical tool in safeguarding client data and maintaining the security and soundness of financial institutions. I'm excited to help our banking partners leverage Provision to reduce the risks associated with outdated and disparate identity management procedures."

John has over 15 years of experience in driving B2B growth initiatives with enterprise to mid-market clients in the financial industry. He was most recently the Director of FinTech Strategies for eOriginal. Inc., specializing in electronic signatures and digital transaction management. John guided managing trusted transactions of digital financial assets for all parties, from the borrower to the secondary market. He is a highly sought-after conference speaker invited to speak about how digital transformation improves processes, creates operational efficiencies, and can connect to a trusted ecosystem of financial industry leaders. John delivers high-caliber presentations, which result in his sessions ranking among some of the most well-attended at financial conferences across the country.

"We were looking for a solution to manage provisioning and considered six possible providers. Of the vendors we considered, Exclamation Labs distinguished themselves with their technical knowledge and advanced digital capabilities, coupled with their affordability."

Matthew Growden, CISSP, CCBSO
Vice President & CIO
First United Bank & Trust

Summary

Achieving A Mature IAM Solution

Financial institutions have an ethical and fiduciary responsibility to protect assets within their business, and data is quickly becoming the most valuable asset. Financial information is among the most coveted, and unfortunately, some of the most frequently stolen data. Banks must shift from reactive cybersecurity incident response to proactive cyber risk reduction. Failing to do so has enormous reputational costs and astronomical remediation fees, penalties, and loss of customers.

The Cyturus proprietary Adaptive Risk Model (ARM) identifies deficiencies, measures potential business impact, and recommends prioritized remediation actions across the entire enterprise.

For example, Cyturus helps banks and credit unions gain insight into the potential risks and challenges associated with their current IAM program and infrastructure by assessing business needs and requirements against core fundamentals.

Cyturus conducts this service through a tailored assessment and provides the business justification and associated plan for transforming your IAM program into a mature solution that meets its business goals.

85% of Bank IT decision-makers say they would buy an IAM system if it were easy, affordable, and tied into their financial systems.

The IT departments at financial institutions are overwhelmed with securing the dozens of new systems added annually containing confidential data, unique user access, and complicated IT integration. Attempting to manage user access manually is a losing and risky proposition that puts a stranglehold on productivity.

Provision was developed by Exclamation Labs specifically for financial institutions to deliver increased security, value, and efficiency. Provision provides a single, automated solution for unprecedented breach protection, audit-ready documentation, and a rapid timeline for implementation. Furthermore, through state-of-the-art API connectors, Provision can integrate with the financial systems that banks rely on for daily business operations.

You can’t fix what you don’t know is broken. The Cybersecurity Capacity and Maturity Assessment (C2MA) from Cyturus provides visibility into areas offering the greatest potential reduction in business risk. Exclamation Labs mitigates the risk of managing internal access to banking systems with the implementation of Provision.

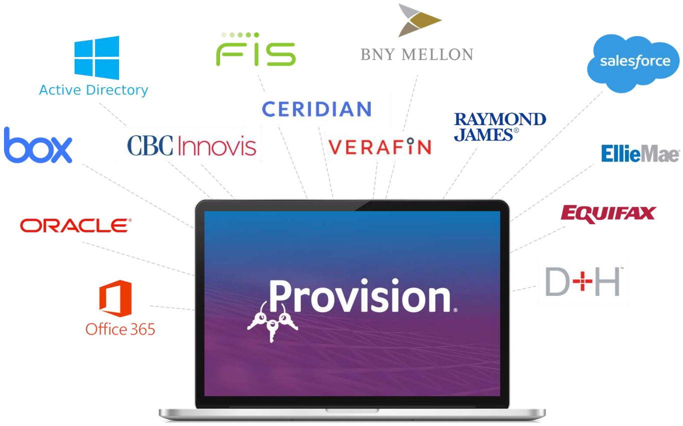
EXCLAMATION LABS

Two Decades of FinTech Innovation

About Exclamation Labs

Providing the functionality financial institutions need to do business in a new digital ecosystem.

Transforming your business operations is no easy task. We know that. Exclamation Labs is an innovative technology partner that understands the needs of financial service providers. Our team offers diverse capabilities in new product solutions, operations, and regulatory compliance. Exclamation Labs designed the Provision Identity Access Management (IAM) platform to address an unmet need in community banking for a single source of provisioning records. Financial institutions nationwide can achieve superior compliance by operationalizing and instantly documenting internal system-wide permissions via connectors across their entire suite of systems.



One of the primary benefits for banks is the number of financial connectors we have built and will be building.

Banks and credit unions manage access permissions for their employees to multiple business systems, while at the same time complying with frequently changing requirements from federal and state regulatory agencies. Many IAM systems provide sampled data, but Provision produces a complete audit trail with full documentation and reporting, allowing internal auditors and regulatory agencies to quickly see everything that has happened across systems. This feature, combined with role-based, policy-driven permissions, empowers mid-sized financial institutions with advanced technology to manage digital identities securely, with half of the financial investment of the closest competitor.

Exclamation Labs has banking partnerships with FIS and Fiserv, core service providers that together serve over half of all US financial institutions. In fact, Provision was the first IAM product with connectors into the FIS IBS core.

Contact: John Jacobs | O: 888.545.5008 x150 | M: 443.977.0830
jjacobs@exclamationlabs.com | www.ProvisionIAM.com

Provision Case Study

First United Bank & Trust

The Problem: Since midsized banks often manage hundreds of independent systems, it is necessary to define who is allowed to access data within those systems. Successfully managing access includes identification, authentication, and authorization.

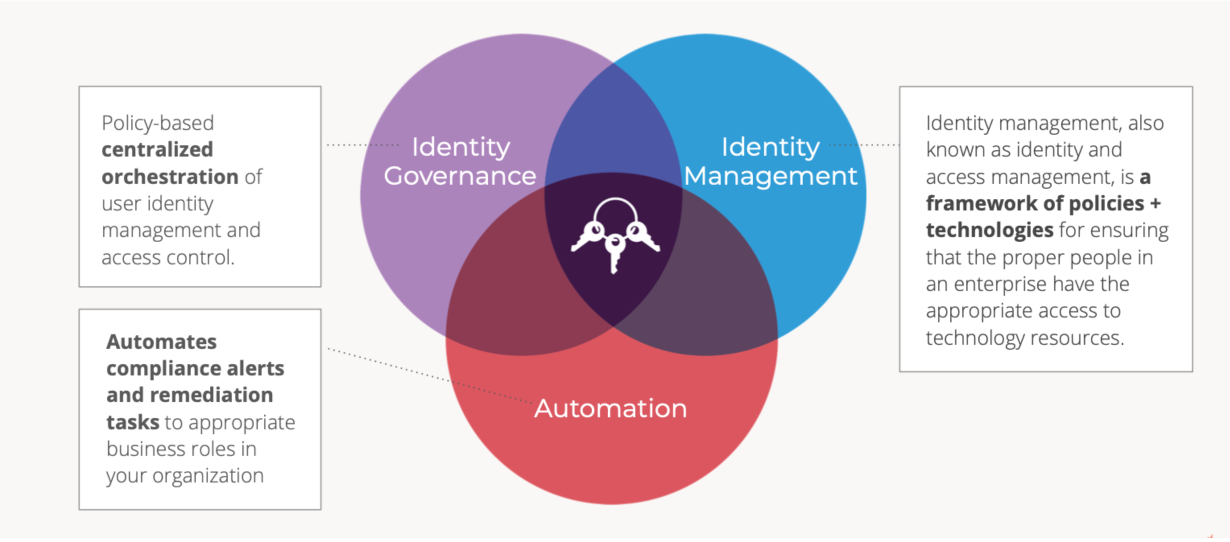
Headquartered in Oakland, MD, First United Bank & Trust has 26 branches located throughout Western Maryland and West Virginia. Historically, access protocols were managed via spreadsheets, and much of the knowledge was reliant on a small group of individuals. Exclamation Labs worked with First United to customize and implement an identity management and governance system for their use.

The Solution: Provision by Exclamation Labs provides banks with a single-source solution via connectors across their entire suite of IT systems. Provision makes it easy to automate the creation of role-based user accounts and privileges, adapted to unique branch configurations. Banks can also generate valuable real-time security auditing and reports.

Key Business Impacts:

- Enhanced productivity was achieved by reducing the time spent manually managing, reviewing, and certifying systems access by 80%
- Using Provision as the central system for managing employee identity enabled First United to better enforce bank policy through standard operating procedures, allowing real-time, and up-to-date access information 24/7
- Improved audit accuracy, reporting, and compliance
- Lowest Total Cost of Ownership among competing solutions

WHAT IS PROVISION IAM?



Policy-based **centralized orchestration** of user identity management and access control.

Automates compliance alerts and remediation tasks to appropriate business roles in your organization

Identity management, also known as identity and access management, is **a framework of policies + technologies** for ensuring that the proper people in an enterprise have the appropriate access to technology resources.