

Buck Kulkarni, CISA, CGEIT, PgMP, is the founder and president of GRCBUS Inc., a New Jersey, USA-based IT governance, risk and compliance consulting firm with a mandate to help customers “get compliant, stay compliant.” As a certified IT auditor, program manager and IT governance professional, Kulkarni (with his team) has executed many IT audit, assessment and remediation assignments over the years and helps organizations achieve compliance with the US Sarbanes-Oxley Act, the Payment Card Industry Data Security Standard (PCI DSS), and the US Health Insurance Portability and Accountability Act (HIPAA), as well as with governance frameworks such as COBIT, ISO 27001, the Software Engineering Institute (SEI)’s Capability Maturity Model (CMM) and others as appropriate to the goals and size of the organization.



Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.

Auditing Biometrics-based Authentication Systems

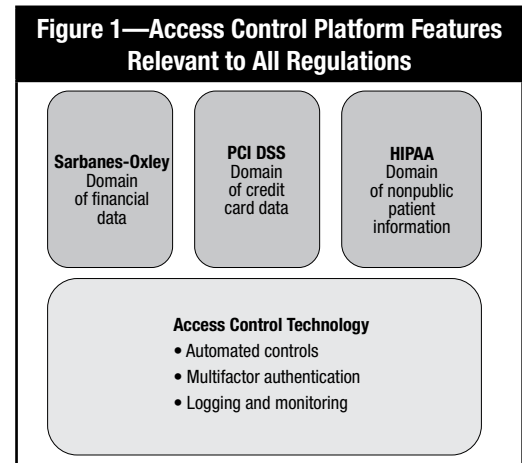
Regulations differ in the scope, focus and level of prescriptive detail they provide to enable compliance. While the US Sarbanes-Oxley Act demands integrity of financial information, the Payment Card Industry Data Security Standard (PCI DSS) demands security of payment card information and the US Health Insurance Portability and Accountability Act (HIPAA) demands confidentiality of patient information. Despite this diversity, there are a few areas of underlying commonality across regulations, e.g., the need for a demonstrated set of controls on how an organization permits or prohibits access to its sensitive data. Single-factor authentication is considered inadequate in e-banking, e-commerce, third-party processing of sensitive information, health care and other situations. This has led to many organizations using card-based, biometrics-based and other authentication methods to strengthen their data security. As these tools proliferate across businesses and governments, auditors will need to understand how they function, what their strengths and weaknesses are, and what to look for. This article aims to describe nuances of biometric authentication methods that will help the audit community.

When auditors evaluate an organization’s access control, they should look for, at a minimum, the following building blocks:

- A clearly defined data security architecture is in place, reviewed and approved by identified stakeholders. Data access is one part of data security, and it must be viewed in totality before delving deeper into the data access. For example, if the data behind the access control are strongly encrypted, the dependency on access control is different from that of a nonencrypted data store.
- Data sets are identified within the organizations that are subject to different regulatory requirements. Information life cycle management policies must specify which data need to be protected and to what degree.

- Multiple factors of authentication are planned and implemented to safeguard the identified data sets as appropriate to their sensitivity classification. Authentication can be done using what one “knows,” such as a password; what one “has,” such as a card; and what one “is,” such as a fingerprint or an iris. A combination should be chosen based on the sensitivity of what is being protected.
- A strong audit trail system that cannot be tampered with, and can be reconstructed when required, is in place to record every access attempt and its outcome. The organization must demonstrate that these trails are reviewed at fixed intervals (or in real time, as appropriate) and analyzed for incident management. Audit trails are increasingly important for both regulatory compliance and digital forensics to support legal actions.

An organization with a coherent information security policy and architecture will be able to demonstrate its access control technology as the horizontal organizational standard, as well as its implementation to individual vertical applications and data sets, as shown in **figure 1**.



Access control and authentication is of particular interest to auditors, as it is one of the common themes across all regulations, all

best practices and governance frameworks. Single-factor authentication, based on user IDs and passwords, served well for nearly 50 years, until sophisticated hacking techniques overwhelmed this simple authentication method. With increasingly valuable data (including financial information, trade secrets, production processes and designs, personal information, and many other forms of data) stored on computer systems, the use of single-factor authentication can lead to unnecessary risk of compromise when compared to the benefits of a dual-factor authentication scheme.¹ Governments, on the other hand, are struggling to balance the convenience of travelers against terrorist threats, and they

Businesses and governments are increasingly turning to biometric authentication solutions.

need increasingly sophisticated tools to achieve this.^{2,3} These are humongous tasks that make the proverbial finding of the needle in a haystack easier.

To meet these challenges, businesses and governments are increasingly turning to biometric authentication solutions. Providing fingerprints while getting a new passport,

entering another country, accessing an application or even while taking up new employment is increasingly common.

Modern biometrics-based solutions have grown in complexity, and some features an auditor can expect to find are:

1. **Enrollment processes**—How “trusted” is the enrollment process? A falsely enrolled person (fingerprint or iris of a fraudulent person associated with a legitimate user) is a potential weak link that can be exploited.
2. **Alias detection mechanism**—Can the system prohibit the same fingerprint (a complex decision in itself) being associated with more than one user?
3. **Duress/emergency mode**—How does the system detect that a user may be under duress (e.g., at gunpoint) and how does it behave to handle this situation?
4. **Number of fingerprints used for registration and matching**—Is the system scalable to meet the sensitivity levels of the asset being protected?
5. **Decision-making process and percentile setting for match**—How is a “match” or “no match” decision made by the system? Does the system administrator have control over it?
6. **False-acceptance and false-rejection rates**—How does the system perform these crucial operating parameters?

7. **Fingerprint data store, encryption and transmission**—Can the fingerprint data be stolen, copied or used while in transit or at rest?
8. **Centralized, decentralized or localized data store**—How and where are the data stored? What are the security, cost-benefit and ease-of-use implications of the employed method?
9. **Integration with other access control repositories and applications**—Does the system integrate with other access control assets of the organization or does it function as a stand-alone system, necessitating duplication of effort and data, leading to further risks?
10. **Audit logs maintenance**—How exhaustive is the log creation system? Does it capture every administrative action and every transaction action? How safe and tamper-proof are the logs? Can they be used following events?

ISACA IT Audit and Assurance Guideline G36 Biometric Controls⁴ provides a conceptual and practical framework for auditing biometric systems. It describes the basic functions, types, risks and countermeasures to empower the auditor to plan and execute the audit. **Figure 2** shows the functions described by G36 and some specific information the auditor should seek to audit each functionality.

CONCLUSION

From simple time-and-attendance clocking on a stand-alone machine to safeguarding sensitive information worth billions to protecting a country’s borders, biometric systems have come of age and their deployment is exploding globally. Biometric systems operate on different body parts that offer unique characteristics, such as fingerprints, irises, noses and veins in the palms (or other body areas), and this technology will expand rapidly as national security and commercial considerations demand more and stronger tools. These tools can add a lot to security, but every tool brings forth new vulnerabilities in its wake.

IT auditors will be increasingly challenged to understand these technologies, vulnerabilities, applications and implications for the business process so that they can provide the required level of assurance to their customers. Auditors need to invest their time in learning the nuances of this technology to meet this challenge successfully.

Figure 2—G36 and the Auditor

ISACA G36 Function Description	Auditor Information
<p>Enrollment The enrollment process requires the intended user to provide the system with a biometric sample that will be digitally converted and stored in a repository as a reference template. Many biometric systems use multiple samples, and the average of all the templates is used in the creation of a reference template.</p>	<ul style="list-style-type: none"> • A fraudulent registration will be the fatally weak spot of a biometric system. • The system should provide for a tightly controlled enrollment process with a supervised mode, logs and records that can be reviewed and audited. • The system should not permit one too many fingerprint-to-user IDs or <i>vice versa</i>.
<p>Data Storage Individual reference templates are stored in an accessible repository for verification of the user's biometrics during real-time access. Storage can be local in the biometric device, remote in a central repository, portable in tokens such as smart cards or a combination of these methods.</p>	<ul style="list-style-type: none"> • The images must be stored at a known destination, ideally at a central, secure and monitored location. • The storage is encrypted with a strong encryption method. • A derived value is stored, not the image itself, so if it is stolen, it cannot be used by a hacker.
<p>Data Acquisition Data are acquired for identification and authentication of valid users to gain access. Data are acquired every time the user wishes to gain access.</p>	<ul style="list-style-type: none"> • The system must be capable of asking for authentication multiple times and at different logical points of the operation. • The system compares the data with a central, secure database. • This process cannot be circumvented by any means. • This process must be seamlessly integrated into the business process. If these are two disparate processes, hackers may insert themselves in between while the decision is being transmitted to the end-user application.
<p>Data Transmission A transmission channel is used by the system to transmit the data acquired for the purpose of identification and authentication. This channel may be internal to the biometric system or external, such as a local area network (LAN).</p>	<ul style="list-style-type: none"> • Transmission should take place over a secure channel. • Transmission replay should not be possible. • Transmission protocol should follow established, secure principles. • Data should be encrypted to a strong standard. Encryption should be performed and checked prior to entering the transmission channel.
<p>Signal Processing Signal processing or image processing involves the matching and validating of the data acquired with the data stored. The reference template stored in the repository is matched with the data acquired.</p>	<ul style="list-style-type: none"> • The data sent should be supported/encapsulated with some metadata to track until the result is reached. • The system should have complete control over every decision as an individual process, even if the system is processing thousands of decisions in parallel.
<p>Decision Making A "match" or "no match" decision is made for allowing or denying access to the user.</p>	<ul style="list-style-type: none"> • Matching algorithms must provide a very high degree of discrimination and accuracy to meet different operating and strategic objectives. • The system must have special modes to process exceptional situations (e.g., a user is forced to authenticate in a physically risky situation). • The system must maintain and provide a detailed log for each decision request received and processed.

ENDNOTES

¹ "Vulnerability, Using Single-factor Authentication," Open Web Application Security Project (OWASP), *OWASP.org*, April 2010

² US Homeland Security, Visitor & Immigrant Status Indicator Technology (VISIT), US 2004, *www.dhs.gov/files/programs/usv.shtm*

³ Dubai Naturalization & Residency Department, Dubai Government, 2007

⁴ ISACA, IT Audit and Assurance Guideline G36, Biometric Controls, *www.isaca.org/standards*

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *ISACA Journal* does not attest to the originality of authors' content.

© 2011 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org