# RBAC, BCM & SoD

What a perfect information technology headline! Three acronyms and not a single word. But they are three important concepts in information security, and I would like to take a few pages to explore their intersection.

## RBAC

Role-based access control (RBAC) has been one of the most significant goals of information security for at least 20 years. According to the US National Institute of Standards and Technology (NIST),[1] it springs from theoretical work performed by David F. Ferraiolo and D. Richard Kuhn in 1992.[2] In simple terms, the premise of RBAC is that access privileges to data, applications and software tools are granted to defined roles, rather than to individuals. Individuals are assigned to roles, and the management decision-making of who gets to access what is generalized across specified functions. The underlying assumption is that access privileges can be grouped so that no individual requires unique utilization of information resources.

> “IF ROLES ARE ALTERED IN A DISRUPTION, AS THEY ARE LIKELY TO BE, THEN THE PRIVILEGES ASSOCIATED WITH THOSE ROLES MUST ACCOMMODATE THE CHANGES.”

By itself, RBAC does not actually act as the switch that either allows or disallows a given person use of certain resources; that is performed by the access control mechanisms in the infrastructure or the applications. When successfully implemented, RBAC provides consistency and efficiency in enabling people to use all and only the information and software that they need for the functions they perform. (It is worth noting here that RBAC is among the most widely used methods in the information security tool kit.)[3]

## BCM

Business continuity management (BCM) is a process by which an organization can “continue delivery of products or services at acceptable predefined levels following [a] disruptive incident.”[4] The BCM process must be aware of the functions performed in the enterprise to determine which are critical and which can be deferred or bypassed. This is where the incongruity with RBAC occurs.

The effectiveness of RBAC depends on knowing *all* the resources a given role (i.e., function) requires. Effective BCM requires knowledge only of the *critical* resources for those same functions. Moreover, and perhaps more important, RBAC is based on the roles performed by an organization in *normal* times and BCM, by definition, addresses those roles in *abnormal* times.

## RBAC and BCM

Thus, BCM establishes one model of how information (and other) resources are to be used and RBAC forms another. If roles are altered in a disruption, as they are likely to be, then the

**Steven J. Ross,** CISA, CDPSE, AFBCI, CISSP, MBCP
Is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal's* most popular columns since 1998. He can be reached at stross@riskmastersintl.com.

“AS MORE FUNCTIONS ARE AUTOMATED, ESPECIALLY WITH THE ADVENT OF AI AND ROBOTICS, IT BECOMES INCREASINGLY DIFFICULT TO SEPARATE DUTIES BETWEEN TWO OR MORE PEOPLE.”

privileges associated with those roles must accommodate the changes. In principle, this means that an organization should maintain two RBAC models, one for normal times and another for disruptions. In principle, maybe; in practice, I am not aware of anyone doing it.

Even if an organization had an alternative RBAC model, it might not be of any value. Response to disruptions is almost always improvisational. People are given permission to take shortcuts and to bypass controls on an *ad hoc*, one-time only basis.

## SoD

Separation[5] of duties is the great-granddaddy of all controls. It is:

> *...a basic building block of sustainable risk management and internal controls for a business…based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department.*[6]

With regard to control over information resources, RBAC is a valuable tool for achieving SoD, inasmuch as formalizing roles requires consideration not only of what a role is permitted to do and access, but what it is prohibited from doing and accessing. Thus, in building an RBAC model, attention must be paid to avoiding the concentration of responsibility within a small number of roles. If that small number is one, SoD is definitely violated.

As more functions are automated, especially with the advent of artificial intelligence (AI) and robotics, it becomes increasingly difficult to separate duties between two or more people. As the number of people is reduced, will there be enough who remain to split the work? Whether it is sufficient for one of those “people” to be a machine process is an open question that I believe needs to be resolved.

## SoD and BCM

If the answer to the open question is that a machine is not a person (a reasonable conclusion on its face), can an exception be made in responding to a disruption? In other words, if SoD can be reasonably circumvented in emergencies, can a machine process act as a compensating control for the duration of a disruption?

As with so many questions in information security, the answer to this one only raises further questions. Who determines when a disruption is sufficiently severe to allow SoD to be bypassed? What forms of monitoring might mitigate the risk? If a machine can provide adequate control in times of disruption, why not in normal times? These conundrums are not really new. We have faced them repeatedly since we introduced computers into business operations. Alan Turing predicted that AI would raise the stakes for answering this question and our times, once again, have proven Turing correct.[7]

## SoD and RBAC and BCM

As long as I am talking about intelligence, I would like to quote F. Scott Fitzgerald’s dictum that “The test of a first-rate intelligence is the ability to hold two opposed ideas in the mind at the same time and still retain the ability to function.”[8] What would Fitzgerald—or Turing for that matter—make of holding three opposed ideas (the topics of this column)? Or are they really opposed?

For most of us in information security, this is irrelevant. We must have SoD; we need BCM; and we will have RBAC. We must make them all work, together if we can or bumping into one another every now and again if we cannot. I might say that solving this sort of dilemma is why we make the big bucks, but we do not and that is not why, anyway. But going beyond the job of passwords and firewalls is what makes this profession of information security endlessly fascinating.

## Endnotes

1 Computer Resource Center, "Role Based Access Control," National Institute of Standards and Technology, USA, *https://csrc.nist.gov/Projects/Role-Based-Access-Control/faqs#:~:text=Rudimentary%20forms%20of%20role%20based,%2C%20and%20Youman%20(1996).*

2 Ferraiolo, D. F.; D. R. Kuhn; *Role-Based Access Controls*, 15th National Computer Security Conference, Baltimore, Maryland, USA, 13–16 October 1992, National Institute of Standards and Technology, *https://csrc.nist.gov/CSRC/media/Projects/Role-Based-Access-Control/documents/ferraiolo-kuhn-92.pdf*

3 Lawless, S.; "RBAC—Is It Implemented in Your Organization?" *Data Privacy + Security Insider*, 23 December 2015, *https://www.dataprivacyandsecurityinsider.com/2015/12/rbac-is-it-implemented-in-your-organization/*

4 International Organization for Standardization (ISO), ISO 22301 *Societal security—Business continuity management systems—Requirements*, Switzerland, 2012, p. 2, *https://www.iso.org/standard/50038.html*. Actually, that is the definition of "business continuity." Business continuity management is defined there as a "holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities." Once again, I would like to state my dismay at definition by committee.

5 Some people prefer the term "segregation of duties." The American Institute of Certified Public Accountants (AICPA) says "segregation." Wikipedia says "separation." I was raised to think segregation was a bad thing, so I am sticking with "separation."

6 American Institute of Certified Public Accountants (AICPA), "Segregation of Duties," *https://www.aicpa.org/interestareas/informationtechnology/resources/value-strategy-through-segregation-of-duties.html*

7 Alan Turing was the towering genius who conceptualized computers as we know them in the 1930s. In 1950, he proposed a test that would determine whether a machine could think. Simply put, Turing hypothesized that if we cannot tell whether a computer or a human being was responding to an interrogation, then we could call the computer "intelligent." See Hodges, A.; *Alan Turing: The Enigma*, Princeton University Press, USA, 1983, p. 523.

8 He wrote it for *Esquire* magazine in 1936. But because an article I have read treads the same ground as I have, I prefer to quote it from Sonderegger, P.; "Forget the Turing Test—Give AI the F. Scott Fitzgerald Test Instead," *Quartz*, 21 May 2018, *https://qz.com/1247378/forget-the-turing-test-give-ai-the-f-scott-fitzgerald-test-instead/*.