Introduction

BigU[1] is a state land grant University. With more than 30,000 students and more than 4,000 employees, it has extensive programs including education, research, and extension missions. Its annual budget easily exceeds a billion dollars. BigU's operations are highly dependent on computer technology and applications so cyberthreats are an ongoing concern. BigU's IT operations are diverse and only partly centralized. Perhaps the most important (and inherently risk-laden) application is its Enterprise Resource Planning (ERP)[2] application with its related sub-systems. BigU's financial operations (including, but not limited to student records) are managed in the system. An IT audit for BigU would focus first on assuring that reasonable controls are in place to ensure that its ERP will help BigU meet its objectives.

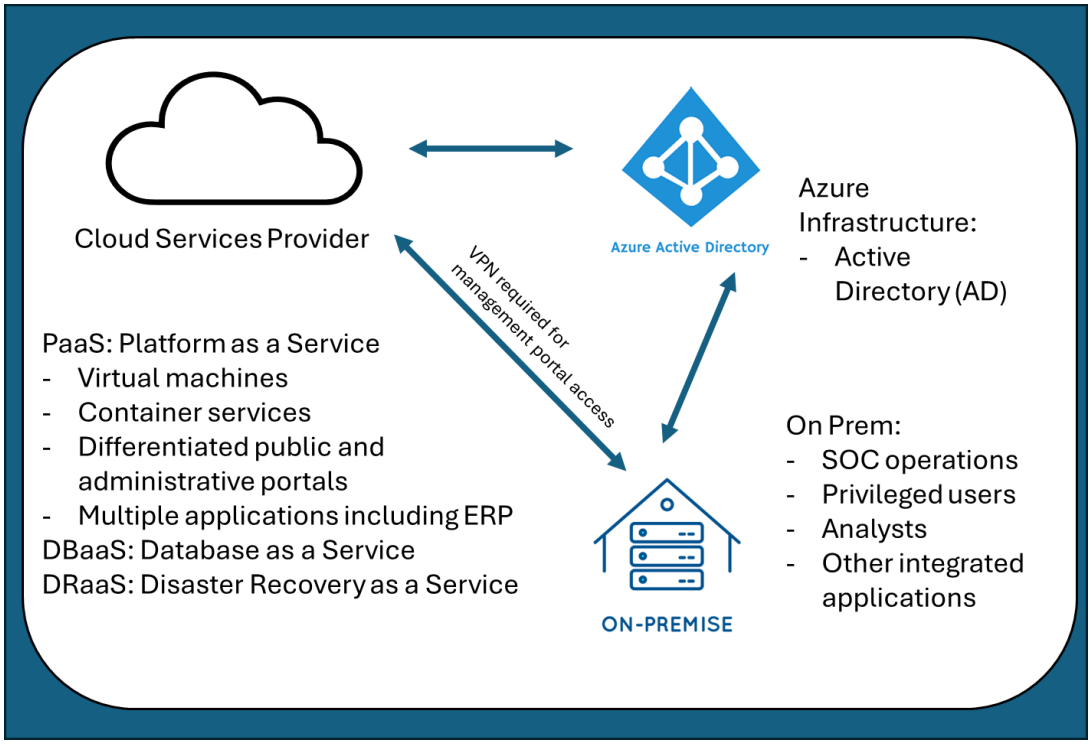
The ERP system was recently redeployed from on premises operation to a cloud provider in a Platform as a Service (PaaS) configuration. The BigU IT eco-system is multi-faceted but the ERP databases, web access, and middleware are run on infrastructure from a cloud provider[3]. Identity infrastructure is hosted by Microsoft. And, as is to be expected, various processes and network interconnections are also in place to connect the cloud system to other BigU applications and operations.

---

[1] BIGU was inspired by Oregon State University (OSU) but numerous details are altered to protect confidential information and to help illustrate class concepts. Many thanks to OSU professionals who helped prepare this case.

[2] We considered how Ellucian's Banner works to help formulate this case, but the case's ERP system details have been altered to illustrate concepts, respect non-disclosure limits, and avoid potential real-world security implications.

[3] While OSU is using Oracle for cloud services, and some exercises employ publicly available documentation of Oracle services, details related to both OSU's use and Oracle's offerings have been adapted for illustration.



BigU manages a number of other important systems and services including laptops and workstations, computer labs, printers, facilities management systems, other application-specific programs and systems, and productivity tools such as email, word processing, spreadsheets and more. Taken together, risks in these systems are substantial. A wide variety of processes are needed to protect these systems from compromise or disruption.

Controls, objectives, and procedures in IT audit

Protecting interconnected systems requires controls/safeguards/protections. Controls are designed, deployed, and monitored by control processes. Auditors make sense of things even when they don't completely understand. This section begins with concepts and paradigms to help you organize your thoughts about how the ERP would be protected and how an auditor might go about assuring stakeholders that risks are understood and addressed.

Controls are safeguards put in place to achieve control objectives. But broader control definitions – for example the definition from FISCAM included in an appendix – emphasize that internal control is a process. **Control processes** are ongoing efforts. You need good processes if you want a system of controls that are and will remain effective over time. Auditors validate controls and processes intended to achieve **control objectives**. In general conversations, the term "control" is used ambiguously. But, at the end of the day, internal control audits should focus on whether or not management assertions about how risk is addressed are justified.

Consider this control objective: "*Accounts with administrative or elevated access to shared resources (privileged accounts) are controlled and monitored to ensure they are used only for authorized activities.*" One or more processes manage 'privileged' accounts. Roles that require

such access are identified, requests for access are reviewed and approved, user directory settings are adjusted, appropriate policies for passwords and multi-factor authentication are created and enforced, usage is recorded and monitored, and – importantly – the whole mix of activities should be reviewed to make sure it remains effective.

Some elements are tangible. Multi-factor authentication tools are installed and configured. Logs of activity (especially privileged account activity) are collected, protected, and monitored. Password rules are configured. And some activities that seem “process like” are also considered controls. For example, there need to be procedures to be sure that when an employee with privileged access leaves, their access rights are suspended. Tangible things are directly observable. Process things often need documentation. For example, you can look to see who is able to make configuration changes by inspecting system settings, but if management approval of a new authorization is to be auditable, the approval might need to be documented in a ticket or memo.

IT audit objectives are often closely related to control objectives. If management implicitly or explicitly asserts that privileged access is appropriately managed, monitored, and secured an auditor maybe be charged with providing assurance of this assertion in an objective such as: “Determine whether privileged access is appropriately managed, monitored, and secured.” Building on some authoritative guidance about how such accounts should be managed, the auditor would then develop a set of procedures that inspect, test, confirm, trace, recompute, inquire, vouch, or compare available evidence in light of expected practices. These procedures employ well-justified criteria. These criteria are generally derived from authoritative sources such as organization policy or standards published by government, semi-government, or industry authorities.

As you work on this case, the goal is to apply concepts from the heart of IT auditing. For the BigU ERP system, privileged access management is of vital concern. But it is only one of many control processes of interest. Networks, applications, devices, data centers, and users are protected by a wide variety of controls and control processes. As you think about the material, try to identify control objectives and think about what it takes to accomplish them. Along the way, you will build skills to formulate audit objectives, procedures, and criteria to collect evidence related to management assertions and thereby fulfill the assurance purpose of an IT audit.

The concepts here are further explored and mastery is evaluated in an exercise. Hopefully students will observe that this discussion applies concepts covered in other course materials.

Identity and Access Functions

Identity and access management (IAM) is the cornerstone of cybersecurity and plays a huge role in other IT management processes. BigU’s IAM processes facilitate Single Sign On (SSO) using three tools: Microsoft’s Active directory, an identity governance and administration (IGA) system, and dual authentication services. Some credentials do exist outside of that environment for specialized purposes, particularly for some IT management processes, but these tools and the related oversight processes largely harmonize identity and access functions.

User Access to Devices and Productivity Tools

As in any digitized organization, phishing-related risks where a user introduces vulnerability in a network or system through credential compromise or installation of malware are a huge threat to BigU's operations. BigU primarily Microsoft 365 tools for email, word processing, spreadsheets, and other productivity applications. But, as would be expected in a University setting, tools from Google, Box, and other familiar vendors are supported. BigU uses a Learning Management System that needs to integrate various services, including role-based access and identity services. "Connectors" between active directory and other systems are needed for BigU to fulfill its mission.

Access to ERP Services

This cloud directory service is connected to the ERP system allowing application-level authorizations to be supported by platform level authentication and threat detection tools. However, as is typical for this kind of deployment, administrative functions for managing the cloud services and some other infrastructure elements are not. There are great reasons for this. Consider, for example, what might happen if the connection between the IGA tools and the cloud provider configuration were disrupted. BigU people would not be able to log into the services to fix the problem. Similarly, administrative access to routers, VPN gateways, firewalls, and other network gear might be cut off, leaving service down if access to centralized IAM tools were to be disrupted.

An IT auditor would want to look into the mechanisms associated with these privileged activities. On the one hand, compromise of accounts with administrative control over IGA, cloud service, or network components could be devastatingly impactful as nearly all other security controls could be disabled. But on the other hand, centralized control over the IAM functions for these resources needs to have some independence from regular operations. This tension is a reality for most every significant IT system.

BigU has a variety of controls in place to protect against related risks. The cloud service provider manages accounts for users authorized to reconfigure cloud services. The provider's IAM practices are tightly controlled, intensely monitored, and systematically audited. BigU could create big problems for itself it was careless about how such accounts are provisioned, deprovisioned, or managed, but the cloud provider has established strong practices internally and provides solid guidance for its clients to protect privileged access.

At the application level – that is for security and configuration activities related to the ERP – the cloud infrastructure limits access to administrative consoles to devices coming from identified segments of the BigU network. That means that, in addition to the already strong application controls over authentication and authorization, an outside actor would have to penetrate a carefully protected BigU network segment (or access gateway) before it could even pass web access requests to the ERP configuration console.

The big picture here is that IAM in the cloud is subject to familiar risks. But by placing the services in the cloud, BigU has exposed its systems to access requests from anywhere in the world through networks that are not directly under its control. Many would say that the controls in the cloud are stronger than what an organization can provide locally. Fair enough. Still, the cloud environment calls for different control activities. Auditors need to gain an understanding of the identity infrastructure if they are to provide reasonable assurance.

Major Cloud Service Offerings BigU Relies On

BigU's ERP and related services are hosted in the cloud using a Platform as a Serv ice (PaaS) model. PaaS arrangements vary, potentially employing a variety of different platform services. BigU benefits from several key services including database as a service (DBaaS), Container Services, and Disaster Recovery as a Service (DRaaS).

A Relational Database Management (RDBMS) system manages the data for BigU's ERP system. In the past, when the system was deployed on BigU's premises, BigU resources (people) managed the entire computing stack undergirding the database. They managed servers, networks, installed RDBMS software, backups, and testing environments. In many ways, the skills and tools to keep things at this level functioning had little to do with the specifics of the ERP system software but more to do with operating systems and utility programs. In the cloud environment these "platform" level activities can be largely delivered through a DBaaS offering. BigU people configure, monitor, and interact with the service, but many activities such as network provisioning, hardware investments and maintenance, operating system installation and patching, and storage system management are handled by the cloud provider who has invested in hyper-scale efficiencies and deep expertise. Even with use of the DBaaS offering, BigU database administrators have lots to do to monitor performance, configure and tune database settings, manage the database schema, ensure appropriate availability of backups, and more.

The ERP application is deployed using the cloud provider's container service. Building on vast experience, the cloud provider creates container templates that can be efficient and secure. BigU chooses from available templates and adapts as needed to deploy various underlying components to support connectivity, web interfaces, administrative access, and middleware tools. They can then deploy a container without too much consideration of the underlying virtual machines. As with DBaaS, the cloud provider's expertise and hyper-scale facilities take care of platform-level concerns allowing BigU resources to focus on user-facing features of their customized ERP implementation. The provider monitors various threats, including cyber threats, that can impact the components in the container and provides tested scripts for patching and maintenance. Using the container service allows BigU to perform most ERP maintenance tasks without any down time. They pay for a temporary new container and deploy updated system components. Once that is sufficiently tested, they can seamlessly transfer operations to the newly deployed container and the old container can be retired.

Disaster recovery capabilities are much stronger for BigU since they moved to the cloud. BigU had previously invested in various remote site functions to make it possible to bring up key functions in the case of a disaster. But the cloud provider's hyper-scale facilities allow well-tested disaster recovery capabilities. This one feature alone might have justified the move to the cloud. The configuration details of the system containers are backed up and stored where they can be initialized in an alternate data center in the unlikely event that the primary datacenter shuts down. The DBaaS service is similarly capable. Frequent and remotely distributed backups of the database logs allow BigU to claim that no more than 15 minutes of data would be lost in a disaster - recovery point objective (RPO) – and the system can be back

up in two hours – recovery time objective (RTO) – even if services need to be transferred to the backup datacenter.

On prem or in the cloud, none of these services are inexpensive. But many risks have been reduced through standard cloud capabilities that would have otherwise been infeasibly expensive. The hardware investments (capital and ongoing) are now included in the bill as an operating cost. And the PaaS arrangement reduces BigU's need to recruit and retain some expensive and hard-to-hire expertise.

Understanding Systems and Processes

Management asserts that controls are in place to reasonably protect IT systems from failures and cyber threats. This assertion is deemed "In Scope" for the audit.

A relevant control objective from FISCAM was considered in planning the audit: "CM.03.02 Critical updates and patches for information systems are implemented, and unsupported information system components are replaced on a timely basis."

An Interview[4]

The auditors interviewed Luis Smith, Senior Technology Director, who has many years of experience with the BigU server environment. Here is a portion of the conversation:

Auditor: You've told us that the database runs as a database as a service (DBaaS) so the cloud provider is responsible for the database software and the servers it runs on. What about the ERP application and the servers it runs on?

Luis: We are using a PaaS model for the system. We have recently moved to the provider's Kubernetes container service, this has lots of advantages.

Auditor: Great. Let me check my understanding, containers run on virtual machines. Both the virtual machine and various components inside the container need to be kept up to date. Does that line up with how you think about it?

Luis: Yes. That's one of the best things about using containers. We can stand up a new one, make sure it is working properly and up to date, migrate our production workload to it, and then shut down the older one. No down time! And from a security perspective it helps that the provider keeps the containers patched and up to date.

Auditor: We auditors like to ask "How do we know…?" So, how do we know that the cloud-deployed components the ERP system runs are up to date and will stay up to date?

Luis: The provider keeps their containers up to date with the latest security patches.

Auditor: Do they update the ERP containers for you?

---

[4] This hypothetical interview was modeled after a real one, but details were changes substantially to illustrate audit concepts

Luis: No, we do the updates using the container templates they provide and update scripts they develop.

[…]

Implications

Nearly everyone interviewed by an auditor intends to be helpful and honest. Auditors generally assume good-faith but also need to consider conditions that might result in ineffective controls. Trust, but verify.

Consider Luis' statement "The provider keeps their containers up to date with the latest security patches." An auditor might easily hear that and move on to another topic, concluding that patching the deployed ERP containers is the provider's responsibility and therefore not something to take up with Luis and his team.

This is where knowledge and a commitment to verification comes in. The auditor follows up with a pointed question. Once it is clear that BigU has to take action to safeguard this risk area, it is also clear that a number of potential control or control process details need to be captured in the audit plan. A few useful references are provided below. The auditor would likely have prepared by reviewing similar resources.

References and citations from illustrative resources:

Oracle Security Overview:

https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_overview.htm

Shared Security Model:

"In a shared, multi-tenant compute environment, we're responsible for the security of the underlying cloud infrastructure (such as data center facilities, and hardware and software systems). You're responsible for securing your workloads and securely configuring your cloud resources (such as compute, network, storage, and database)."

Workload Security

"You're responsible for protecting and securing the operating system and application layers of your compute instances from attacks and compromises. This protection includes patching applications and operating systems, configuring operating systems, and protecting against malware and network attacks.

Oracle is responsible for providing secure images that are hardened and have the latest patches. Oracle also lets you to use the same third-party security solutions that you already use on-premises."

Host Infrastructure Security

"You're responsible for securely configuring and managing your compute (virtual hosts, containers), storage (object, file, local storage, block volumes), and platform (database configuration) services.

Oracle shares responsibility with you to ensure that the service is optimally configured and secured. This responsibility includes hypervisor security and the configuration of permissions and network access controls."

For more see: CIS Oracle Cloud Infrastructure Container Engine for Kubernetes (OKE) Benchmark v1.5.0 - 05-21-2024

Thought questions

1. What audit objective is addressed by this interview?
    a. **Formulate an audit objective** adapted from the identified control objective from FISCAM.
    b. Maybe that first objective is too specific. **Formulate a more general audit objective**.
    c. Audit scope is important. **Think about** – that means no answer required - how you would adapt the objective for a financial audit, a risk assessment for the ERP system, or a more general IT risk assessment for BigU.
2. **Identify** two or three negative events or conditions might arise if controls are not effective here.
3. **Identify one or more controls/management processes** you think should be in place to address those risks.
4. **Identify three questions the auditor might want to ask next.** Remember: auditors should ask relevant (or at least potentially relevant) questions.

    Hints on questions: General issues that arise for most controls include:
    - *Responsibility: Who is charged with monitoring and acting on this risk area?*
    - *Triggering events: How do we know action is needed?*
    - *Procedure: Who does what, how do they know they are doing it right?*
    - *Observable technical artifacts: How can we observe the current state or history?*
    - *Control activity documentation: How do we know if people have taken appropriate action?*

Evaluate your answers:

Audit objective:

- Does your objective begin with “Determine whether..?” It probably should. There are other words that can be used, but this formulation helps us stay on track.
- Did you cut and paste a good portion of your first objective right from the FISCAM text? Good! Auditing has creative elements, but tight reliance on authoritative sources is often a good thing.
- Did you create a “higher level” objective that might include a number of different objectives similar to your first one? Audit plans usually include no more than a handful of audit objectives. The scope of the audit guides granularity. For example, audit plans with hundreds of audit procedures will likely specify aggregated objectives while more limited investigations will tend to have objectives that more closely aligned with moderately specific control objectives like the ones specified in FISCAM. Auditors dial up and dial down specificity as they formulate an audit plan.

Risk: Audit questions should always be formulated considering how controls reduce risk. Knowing the risk is an important first step. Do your risks relate to the topic of the interview? Can you see ho BigU would be harmed?

Controls/processes:

- Are your control examples “policies, procedures, practices, or organizational structures”?
- Control ideas:
    - Did you identify a process that would systematically inform BigU that updates were needed?
    - Did you envision checklists or procedures to make sure that updates were effectively applied?
    - Did you consider how changes would be tested or verified to avoid disruption?
    - Did you consider how current patch status would be monitored?
    - Did you think about how the activities would be documented?

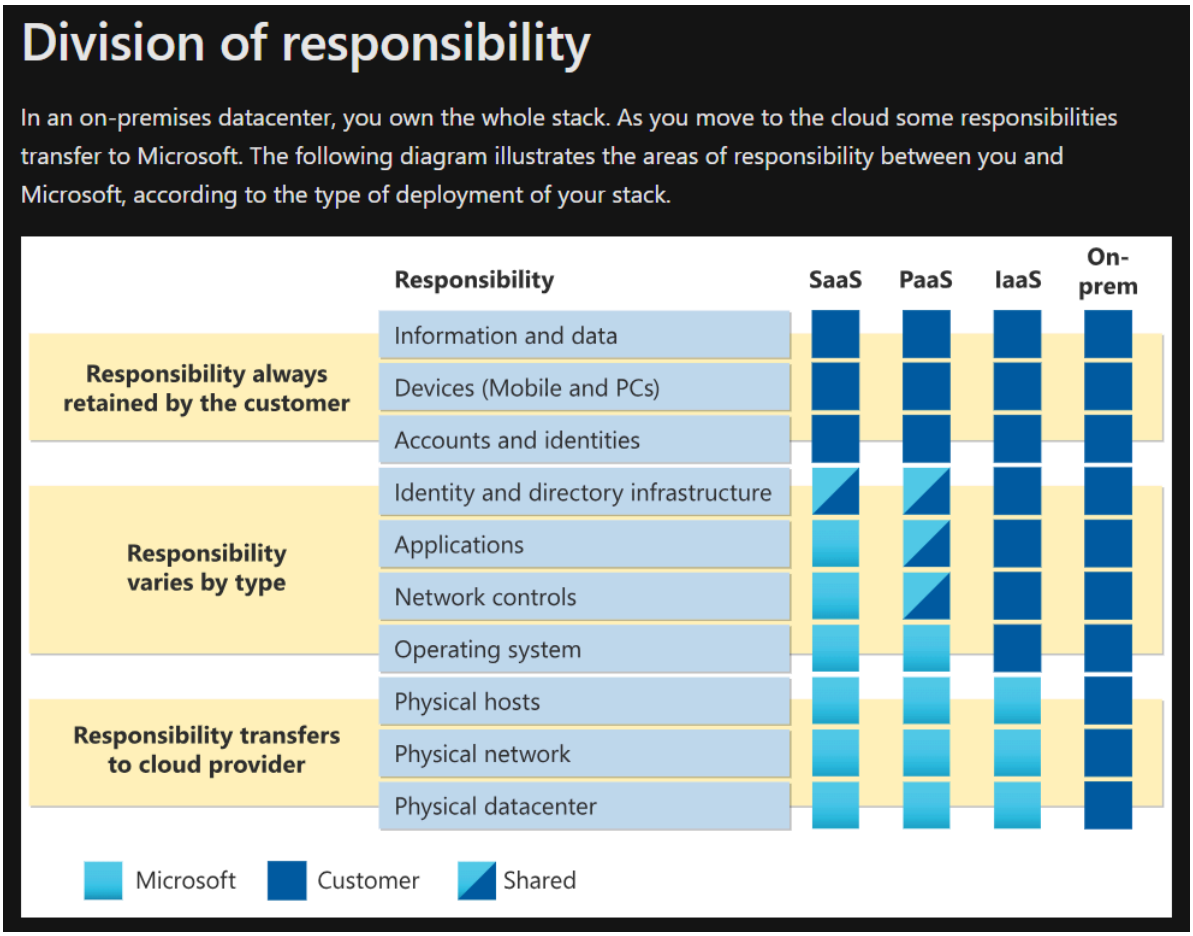
Your Auditor Questions:

- Do your question(s) match up with the risks you identified? Which one(s) does each question support? If you can’t say, you probably should refine your question.
- Consider the tone of your questions. Does it sound accusatory? – that’s usually not a good thing.
- Is it appropriately open-ended? Notice that some questions in the narrative were open ended and would prompt the user for lots of information while the last question is more pointed. Both kinds of questions have their place. Did you accomplish what you intended?
- Imagine how the interviewee would answer. Do expected answers productively lead towards formulation of an audit procedure or gathering of audit evidence?

Similar expectations apply for lots of controls. Auditors want to think about ongoing processes that result in solid controls, not just conditions that indicate risk.

Shared Responsibility

Shared responsibility for a PaaS application is shown in this chart distributed by Microsoft.



-

https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

The responsibility elements in the diagram constitute an integrated system. The parts rely on one another for reliability and security. An auditor would need to understand which control groupings are assigned to the client or the cloud vendor. Further, the client needs to understand how to configure its controls to avoid cloud vulnerabilities. The characterizations on this chart suggest that some network controls are managed by the cloud provider while others are managed by the client. As noted in an appendix, some other PaaS shared responsibility diagrams divide things differently, for example assign “all” network controls to the cloud provider.

The reality for BigU, and for most medium to large organizations, is that special connections are made into and out of the PaaS environment. To facilitate protected administrative access and because of interactions with other systems, most client organizations need to have some solid network controls in place if the PaaS environment is to be secure. This illustrates an important reality for an IT auditor assigned to provide assurance that controls over cloud systems are effective. They need to understand the client’s use of a cloud platform so that they can see if management assertions about the effectiveness of controls are true. Numerous impactful

incidents have happened when a client uses a well-regarded cloud provider but fails to properly secure relevant controls on the client side.