# 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[[1]](#footnote-1)

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?

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?
   1. **Formulate an audit objective** adapted from the identified control objective from FISCAM.
   2. Maybe that first objective is too specific. **Formulate a more general audit objective**.
   3. 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 of 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.

1. This hypothetical interview was modeled after a real one, but details were changes substantially to illustrate audit concepts [↑](#footnote-ref-1)