# CISA Certification Prep Course Overview

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISA® Certification Prep Course</td>
<td>2</td>
</tr>
<tr>
<td>Notices</td>
<td>3</td>
</tr>
<tr>
<td>CISA® Certification Overview</td>
<td>4</td>
</tr>
<tr>
<td>CISA Certification Requirements -1</td>
<td>5</td>
</tr>
<tr>
<td>CISA Certification Requirements -2</td>
<td>7</td>
</tr>
<tr>
<td>The Exam</td>
<td>8</td>
</tr>
<tr>
<td>Applying for Certification</td>
<td>10</td>
</tr>
<tr>
<td>CISA Task and Knowledge Statements</td>
<td>11</td>
</tr>
<tr>
<td>CISA Domains -1</td>
<td>12</td>
</tr>
<tr>
<td>CISA Domains -2</td>
<td>13</td>
</tr>
<tr>
<td>CoBIT – ISACA’s Recommendation for IT Control Practice</td>
<td>15</td>
</tr>
<tr>
<td>CoBIT Emphasis in Domains -1</td>
<td>16</td>
</tr>
<tr>
<td>CoBIT Emphasis in Domains -2</td>
<td>18</td>
</tr>
</tbody>
</table>
This is the
**002 introduction to the CISA certification prep course.
I want to talk a little bit about the certification before we begin, kind of how it works, how you actually get into it. Obviously, you know a little bit about it, otherwise you wouldn’t be taking this course.
CISA Certification Requirements

CISA is an ISACA certification
- Formally known as Information Systems Audit and Control Association (now just ISACA)

Pass the CISA Exam
- Passing score valid for five years with required work experience

Adhere to ISACA’s Code of Professional Ethics

Agree to Comply with Continuing Education Policy
- Maintenance fees and a minimum of 20 hours required annually
- Additionally, a minimum of 120 hours is required during a fixed 3-year period

Adhere to the Information Systems Auditing Standards

**004 So, let’s talk about the requirements. Well first off, this comes from ISACA. And so, that used to be the information systems audit control association. Now, they just shortened it to ISACA.

Okay, so how do you do this? Well, you follow what ISACA lays out for you. You have to pass that exam, adhere to their code of ethics. And then the real trick with this is continuing education policy. If you take this exam, and you go through all this work to prep for it, and then you don’t keep up with it, you’re going to lose your certification and have to retest.
So, the continuing education policy is not that difficult. You need forty hours per year. If you think about that, if you came to one course every year, one five day course every year, that would take care of your forty hours as long as they were within the domains of the CISA.

Also, when you're dealing with ISACA's code of ethics, one of the things that I always say to people is at a minimum, if you're going to follow the code of ethics because my ethics and your ethics may be different, at least don't cheat on the exam. And it's very difficult to cheat on this exam. But even if you could, remember you're devaluing the certification itself.

Then you also have to adhere to the information systems auditing standards and they're laid out by ISACA themselves.
Work experience

- Verified minimum of five years of professional information systems auditing, control, or security work experience
- Must be gained within the ten-year period prior to the application date for certification or within five years after passing the exam
- Substitutions and waivers of such experience may be obtained
  - If certain education and general IS or audit experience requirements are met

**005 At a minimum, you have to have a certain amount of work experience. And that's five years of work experience. You can trade a higher degree for one or two years here and there.

But you've got to have gained all that five years of work experience in the auditing area over a ten year period of time. You can get those waivers on certain things that you've done as far as your work experience are concerned.
**006 Okay so, what's the exam like? Well first off, it's only given twice a year. That's the thing you have to understand. Second off, it's graded on a curve. So, all of the people that are taking it at the same time you are, globally, all of those results are being rolled up. And then they're saying here's the curve of the people. Those people there, they don't pass. These people here, they do pass.

So, that means if you do what everybody else does, you'll be in the middle of the curve. I don't know about you, but when I take a test, I want to be-- I don't want to be the...
curve breaker. But I want to be just ahead of the curve here. So, that means you’re going to have to do something more. I’ll give you a couple of little hints as to what more you can do in just a minute.

Now, this exam requires that you enroll for it way early. So, if you want to take the December exam, you have to register in October. And registration closes in November. If you say, "Oh well--" And I’ve had students come into my class. They show up like right before Thanksgiving. And they say, "I’m ready to take the exam." And I say, "Have you signed up for it?" And they go, "No, that’s no big deal." I go, "Go get your money back because it isn’t going to do you any good. You’re not going to be able to get into the exam to take it. Or fine, register for next year’s exam."

Now, here’s the problem with next year’s exam. The exam’s a little bit different every single time. They take all the results that they got from this six months’ exam, and they say, "Okay, how do we move the profession forward. Then we’re going to change the questions."

So, here are the main sections of the exam itself. Process and auditing costs fourteen percent, governance and management fourteen. And notice that information systems acquisition and development is little bit higher. And information systems security operations, maintenance, and support is a little bit higher. And
then here’s the big one. Protection of information assets is the biggie. So, you want to focus a little bit more of your time and attention there.

Applying for Certification

Applying for Certification

Pass the exam.

Meet the work experience requirements.

Complete the CISA Application for Certification.

• Three ways to apply: online, download form (PDF), and mail http://www.isaca.org/CERTIFICATION/CISA-CERTIFIED-INFORMATION-SYSTEMS-AUDITOR/APPLY-FOR-CERTIFICATION/Pages/default.aspx

**007 When you apply for the certification, what you do is you pass the exam. You meet the work experience. And then you apply for the-- you do the application online for the CISA. And then you become accepted.

Now, I want to switch gears here just a little bit.
CISA Domain are also referred to as CISA Job Practice Areas.

ISACA defines Tasks for each Domain, these are the tasks that an IS Auditor performs in the course of performing the IS Audit job function.

CISA Knowledge Statements describe the knowledge necessary to execute those tasks.

ISACA explicitly defines the relationship between tasks and knowledge statements for each Domain on its website: www.isaca.org under “CISA Job Practice Areas.”

**008 And talk about the knowledge statements and the tools that you want to use. So, when you look at the domains you also look at them from a job practices standpoint. So, if you look inside of the ISACA location, and they talk about the job practice areas, they divide this down into tasks that are performed. You should be able to look at that task list and go "Yep, I can do all of these things on this list. And I'm okay with it."

Now, those knowledge statements describe the knowledge necessary to execute those tasks. But it doesn’t tell you how to do those tasks. So,
CISA Domains -1

Candidate must have a thorough understanding of task and knowledge statements in order to pass the CISA exam.

CISA Domain Overview

- Domain 1 – The Process of Auditing Information Systems
  - Provide audit services in accordance with IT audit standards to assist the organization in protecting and controlling information systems.
- Domain 2 – Governance and Management of Information Technology
  - Provide assurance that the necessary leadership and organization structure and processes are in place to achieve objectives and to support the organization's strategy.

**009 When we look at the domains, let’s look at domain one and two here just for a second, the process of auditing in information systems. How do you dispassionately look at a system and say this system meets the policy requirements or does not meet the policy requirements. They're saying what they do. And they're doing what they say they did.

Governance and management in information technology, how do we
know that the leadership of the organization and the organization structure is actually working for us? How do we know that those people support the organization’s strategy? We have to examine that.

**CISA Domains -2**

- Domain 3 – Information Systems Acquisition, Development, and Implementation
  - Provide assurance that the practices for the acquisition, development, testing, and implementation of information systems meet the organization’s strategies and objectives.
- Domain 4 – Information Systems Operations, Maintenance, and Support
  - Provide assurance that the processes for information systems operations, maintenance, and support meet the organization’s strategies and objectives.
- Domain 5 – Protection of Information Assets
  - Provide assurance that the organization’s security policies, standards, procedures, and controls ensure the confidentiality, integrity, and availability of information assets.

**010 In domain three, we talk about information systems acquisition, development, and implementation. I package this under a nice neat thing called system development lifecycle. So, I like the look there. It provides all of those acquisition, and development, and testing of these particular tools. Remember, in SDLC when we**
actually release this into our environment, we have tested it and made sure that it actually achieves our goals.

When we talk about operations maintenance and support, this after the SDLC. This is actually at the end of the SDLC that says okay now, we've got this product up and running, how do we support it on a regular basis, things like change control.

And then finally the biggie, domain five, protection of information assets. What do the controls look like? What are the policy standards and procedures? What are the paperwork that is around that organization that asserts that these controls are in place that are going to protect our confidentiality, integrity, and availability of those resources?
Now, I said how are you doing to do more than everybody else. That was my first question. And my answer is that you’re going to dig deep into one of the ISACA resources called CoBIT. So, here’s a general diagram that comes from CoBIT. What I want you to do is I want you first-- by the way, in order to take your exam you’re going to have to register with ISACA. When you do, you will get a discount. And you will also get downloadable files from them for free. Well, you have to pay for your membership. But then after that, you have their list of resources that are available there.
One of them is CoBIT. Get CoBIT and read it. Yes, it is very long. But it describes exactly what a CISA does from their perspective. It looks at the auditing profession.

**012 Now, if you map this to the particular domains, what you'll see is that in domain one the process of auditing, we look at monitor and evaluate, and plan and organize because we say, "Here's the policy." And then, "Here's how the policy's put in place and how we go ahead and map back to that."
In domain two, when we talk about governance, we reach back to the exact same things. But we look at it first from the plan standpoint and then from the monitor and evaluate.

For domain three in acquisition, we take CoBIT. And we say, "Okay, we've got it planned and organized. How do we do acquisition on this? How do we make that fit within our organization?"

Domain four says, "I have to do operations, maintenance, and support. That includes delivery and support, acquiring, but also monitoring and evaluating." It's got to report correctly outside. Those event logs have to be generated.

And then finally domain five, protection of information assets, how do we put these controls in place? And what assets are they protecting? We look into the delivery and support a little bit more. That's CoBIT.

And what I want to say to you is that CoBIT is emphasized heavily on your exam.
CoBIT Emphasis in Domains -2

**013 So, you need

 to be ready for it. And that’s the

 introduction to our course.