

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

**Part I. Introduction to Information Classification**

Good morning to you all and thanks for coming. The philosophy behind creating this Policy was a little bit different than in the past when you just got a policy. We did not want to give you a policy and standard but also provide you with a process to go along with that so that you just don't have to figure it out by yourself and see how to implement it but rather you have a process behind it which you can methodically follow and actually implement information classification in your agencies.

So that was the fundamental premise behind creating this Policy and the entire set of materials for information classification.

Our primary goal at the end of this class is to make sure that when you go back you not only have the Policy in hand but also a process and you have gone through some examples here so that you can hit the ground running.

Not all of you are going to go back and start implementing information classification right away.

But I think from the experiences you get here, from the training you get here, you would be able to do it in a much quicker fashion when you go back.

And that is the intent behind this.

So before we even start on information classification, let's try to understand the fundamental problem that we face today.

If you look at what is happening is that storage is becoming cheaper and cheaper and we are collecting more and more and more information over time.

And the growth curve is really exponential because the cost of preserving data or the cost of collecting data has gone down, the cost of storage of data has gone down.

That's one problem.

The second problem is the proliferation of data.

The same data is sitting in a computer, the same data maybe on a CD, the same data may be on a thumb drive that you have.

So with this proliferation of data it's becoming harder and harder to manage data because we don't even know what data we have, we don't know where it exists and we don't know what the value of the data is.

The process of information classification will help us get a handle on the data and help us better manage the data.

So now we understand that we have a lot of data, we understand that it's getting unmanageable but the question is why do we need to protect data.

And that's one fundamental question that we need to answer so that we can motivate ourselves to actually do information classification or go through the process.

So let's see.

Information has some inherent value.

The value of information will differ from person to person and from organization to organization.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)**  
**Enterprise Information Security Office (EISO)**  
**Information Classification Training Transcript**

If I look at information in the private sector, the primary value of that information is competitive advantage.

There are strategies which organizations create.

There is research which they do.

There is data they collect which they want to preserve on their own so that the competition does not gather that information and they're able to maintain their competitive advantage.

It's like a chess game - you don't want the opponent to know what your next moves are otherwise he can always counter them and get ahead of you.

The motivations are quite different in a public sector organization.

It's not really competitive advantage or profit.

The primary motivation that the public agencies have is that they hold the public's trust.

Data is entrusted to the agencies, data is entrusted to the government because the public expects it to protect it, preserve it and have trust in the government, and a breach of data breaks some of that trust.

So there are political consequences to that.

That's one thing.

Another huge issue which comes with such breaches is the loss of productivity.

The machines need to be reset, we need to go back and figure out where the breach has happened and there's a lot of cost associated with that.

And finally but not the least there's a lot of regulatory pressure to make sure that information is protected.

If you look at the different legislations that have been enacted in the last few years, including Sarbanes-Oxley, Health Information Privacy and Portability Act

(HIPAA), then FISMA [Federal Information Security Management Act], FERPA [Family Educational Rights and Privacy Act], there are a whole bunch of different legislations which have been enacted which legislate the protection of data and there are fines associated with not protecting the data.

So all of these things require that we protect the data.

Let's look at what has happened in the last few years.

If you look at this chart, you will see how many large breaches have happened.

The first one we start with is Data Processors - 5 million records.

Followed by America On-Line - 30 million, Citigroup, the Department of Veterans Affairs and the largest one was TJ Maxx - 94 million credit card numbers stolen and personal information stolen.

If you look at this, these are not isolated incidents, but it shows a pattern, that over time, it's happened again and again and again and to a large extent.

And there's a huge cost associated with that and the cost is associated with informing the public about it, making sure the credit cards are replaced, and the cost can be phenomenal.

Now a lot of these are in the private sector.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

Let's look at what's happening in the government sector since 2009. The government sector is not immune to the breaches.

If you look at the first one here, in Charleston - 11,000 records, again, in Indiana - 8,700 records, then in Alabama - 37,000 and so on and so forth. If you go to the University of Florida - 330,000 and finally in the Arkansas Department of Information Systems - it's 807,000 records stolen.

So again, this is a pattern.

This is not an isolated incident, it just keeps happening over and over again in different states, different agencies, everywhere.

And if you look closer to home, if you look at New York State, since 2007 we have had 4 million NYS records stolen for 4 million people - and that's a large number.

According to the Ponemon Study it's about \$200 lost with each breach that is reported, with each breach.

And all of the costs of clean up after that, informing the public, and ensuring information security plus all the regulatory fines that come with that.

So given the 4 million records that are stolen, that's 800 million dollars lost.

That's a large fraction of the budget deficit we have today. 800 million dollars is a lot of money.

So again, it becomes very important for us to protect information.

So now we've established that information needs to be managed, it's getting unmanageable.

We have established the value of information.

We've also established the fact that there are consequences of not protecting the information.

The question is - why does classification help?

Why do we need to classify?

The reasons for that are economic.

The reasons for that are we can't protect all the information to the same level because protecting information is expensive.

You can not give the same level of protection to everything.

So what do we do instead?

We need to find out the inherent value of information in the different pieces of information we own.

In no case do you want to spend more money protecting a piece of information than it is worth.

So this is an economic decision that you need to make.

What information classification helps you do is figure out the real value of information so that you can decide how much money you are willing to spend protecting it and to figure out what kind of protection it needs and what level of protection it needs.

So that's why we need information classification - it helps you manage your resources efficiently and economically.

So how do you make this decision -

how much the value of information is, what is information worth?

Inherent to all of this decision making, is risk analysis.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

You need to be able to figure out the risk associated with a breach of data.  
You sit down and figure out what happens if a piece of information is lost or stolen, if it is compromised - what are the consequences of that.  
And that's what this whole process is about.  
Figuring out what the consequences of data loss is.  
You make risk decisions every day in your life.  
You cross the street, you make a decision about risk - will a car coming run me down or will I have enough time to cross the street.  
That's a risk decision you make.  
You go and buy a hamburger - you make a risk decision.  
You figure out, well, am I going to like it, is it worth it, am I going to get sick eating it, will I get Mad Cow disease, will I get fat after eating it, will it increase my cholesterol.  
You look at all of these factors while you are making a decision.  
The same thing goes here.  
You take a piece of information - what happens if I lose this piece of information.  
Will the public get upset, will my manager get upset, will we have to pay a regulatory fine?  
So all of these decisions similarly come in to your thinking.  
And that's what this is about.  
It's figuring out what the value is and figuring out how you need to protect it and risk analysis is fundamental to it.  
So this is a brief introduction of why we need to do what we're doing and how we're going to go about doing it, conceptually.  
So what we've figured out is, information again, is getting unmanageable today.  
We have an ever growing set of pieces of information in our repository today.  
Second, we understand the inherent value of information and there are associated problems with losing the data which are economical.  
Next, we've established that we can't protect all information to the same level because of economic reasons.  
So that's why classification helps figure out the right level of protection for all the information that you own.  
And finally, we've realized that, it's a decision problem - we need to figure out what are the consequences of losing data.  
And that's why we need to engage in this exercise.

**Part II. Information Classification Materials**

So what will we do today?  
Now that we've established what we need to do - the information that you have in the blue packages here will help you go through the information classification.  
Like Will Pelgrin said earlier, it's a daunting task.  
There's a lot of work involved in this.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

What we've tried to do is make this task as easy as possible by providing you with the materials, providing you with the process, the templates as well as several worked out examples which you can just follow along with that will help you in your decision making ability.

I do want to reiterate one thing which I'll say several times again.

Is that - you have all the materials, you have the processes in place, but in the end, the decisions that you are making, they are your own decisions.

The CSCIC Policy, the processes, will not make the decisions for you.

They will just facilitate the decisions, they will show you the process.

In the end, it's your decision, it's your thinking, it's your ability to judge the value of the information correctly that's going to give you the classification.

There are 3 steps which we are going to follow today in this whole class.

The first is figuring out what you have; basically making an inventory of all of the information assets that you have.

That's your first task for today.

And that will include identifying everything that you have, grouping the assets together, and figuring out the owners of the data and so on and so forth.

So that's the first task.

The second task will be the actual classification.

What you do in that is - we have provided you with templates - we use the templates, answer a series of questions and figure

out what the value of that information is or what the classification of that information is.

And the third thing is selecting the controls.

Basically figuring what controls you need for different pieces of information.

And this talk will go through all the 3 different parts.

The materials that you have in here - they will provide you with everything you need to perform information classification in your organizations.

It's called the Policy and Standard , plus it's got several templates which you can use as a guiding principle in your information classification.

So let's go into detail of what you have here.

So let's look at the first piece.

This is the Policy and the Standard. What the Policy and Standard does is, it provides you with the overview of the information classification, the purpose, the goal and the scope.

All right - that's the first thing which you have.

Then you go on to Appendix A . What Appendix A contains is an exemption form. In case you are not able to comply with some of the guidelines of the Policy, you need to fill in an exemption form.

We are going to go over the details of this as to when do you fill it out and why do you fill it out.

Appendix B contains the Information Classification and Control Manual.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

So, the Policy and the Manual, they go hand in hand.  
The Policy and Standard tells you what you need to do and this Manual tells you how you are going to do it or the process you are going to follow.  
And you are going to make extensive use of both of these.  
You come down to Appendix C - it has got two templates in there.  
The first template is an asset inventory worksheet which you will fill in for all the information assets that you have.  
It basically identifies what the asset is and provides certain attributes for that asset.  
And the next worksheet is a template for classification which contains a series of questions which you will answer that will help you in the classification process.  
And the Appendices D and E - they primarily relate to the controls.  
Appendix D contains all of the control charts which we will discuss later and Appendix E contains a glossary which explains all of those controls.  
So make sure you have all the different pieces in your package.  
Let's move further along.  
Let's get back to our slides.  
Are you guys with me?  
Let's look at the scope of the Policy.  
The Policy applies to all pieces of information regardless of how it is stored and used.  
It applies to all different media types including text, video, including voice - so everything is covered under this Policy.  
Third thing, it covers information in its entire life cycle - from when it is created to when it is being used to when it is being destroyed.  
So the scope is covering the entire thing.  
And the same information may be on a piece of paper and stored electronically.  
And they will both have the same classification independent of the media it is stored on.  
Remember - a lot of people have a tendency of trying to classify the equipment where the information is stored - 'Well, this computer is classified'.  
It's not the computer that's classified, it's the information.  
The same information is transferred onto a thumb drive and the same information is classified (the same way).  
So let's make this distinction clear - that we are classifying information not pieces of hardware which contains that information.  
And the last thing, but one of the most important things is, we need to realize that this Policy and Standard, if you follow this, does not absolve you from following some of the other policies, like the NYS Freedom of Information Law, or the Arts and Cultural Affairs Law [the State Archives Retention Law].  
This Policy is supposed to compliment some of the other policies that you have rather than be an independent policy on its own which can countermand or supersede any of the other policies - it does not do that.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

I want to make sure you understand that.

And lastly, if you look at information classification, as Will also mentioned earlier, it really is a large task which is spread across the whole organization.

We need to make sure that everybody's involved in this.

And there are several stake holders to this.

Let's just discuss who the stake holders are.

First, the Policy covers all State agencies, departments, offices, divisions, boards, bureaus, commissions, and any entity over which the Governor has executive power, which includes all the [NY state] educational institutions, SUNY and CUNY [Central Administration only].

And also public benefit corporations where heads are appointed by the Governor of NY.

So everything is covered pretty much.

The second stake holder in this is the State workforce.

The State workforce includes every employee of the State as well as the contractors who work directly under the supervision of State employees.

For instance, if you hired three contractors who work along with you guys they're also part of the State workforce which need to adhere to this Policy.

Second, we need to understand what an information owner is.

An information owner is a person who is responsible for making decisions about access, decisions about classifications, and figuring out the inherent value of that information,

as opposed to the information custodian who has physical custody of that information and who is responsible for making sure the information is protected.

But the information custodian would typically not make decisions which the owner makes unless they are the same person and we are going to go into the details of that, as we go on.

And last, but not least, is the Information Security Officer.

The role of the Information Security Officer is really to make sure that information classification is followed in an organization but not really directly to [classify] information because the classification is a process that needs to go to the root of the organization where you are doing it as a part of your every day work rather than a special project when one or a few people do it across the whole organization.

And we will discuss that as well as we go along.

So these are the important stake-holders, but, one of the main stake-holders is management.

Why is management important in this?

Management is important in everything because they control everything.

The primary reason management is really important in this information classification is because,

like I said earlier, this effort is not meant really for a few individuals to perform in the whole organization.

It needs to change as a culture of the organization - we need to make sure that information classification is something

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

which is done routinely in different parts of the organization.

Why is it not useful for having just a few people go around and do information classification in the whole organization?

Anybody?

*Audience: You can't be everywhere at once.*

You can not be everywhere at once and as soon as they finish the classification process it is obsolete.

It needs to be institutionalized so that everybody is doing their own classification.

You get more data, you need to classify it.

Laws change, you need to re-classify it and each person needs to be responsible based on their given role.

So that's one thing.

And second thing is, given that we need the whole organization to be a part of this, without the management mandate it will be very hard to get a buy in from all of the people in the organization.

We need to make sure that everybody is involved in this.

One of the most overlooked parts of information classification is the third parties.

One sixth of all the security breaches happen at the third parties and it's often overlooked by the State agencies.

This is very important - if you have a third party taking care of your data, providing you with information, doing analysis for you, make sure that through contractual obligations, they follow the same security guidelines as you guys are supposed to follow as part of this Policy.

And that becomes very important.

And it's your responsibility as the information owner of the agency to make sure that the third parties comply with the regulations.

How many of you own a car?

When you buy a car, what do you look for?

Price – one.

What do you look for in a car?

Safety.

Reliability.

Comfort.

So price, reliability, comfort and safety.

So you can have a car which is very comfortable but it's very expensive, right?

And you can have a car which looks very good, it's very attractive but otherwise it's a lemon and every third day you have to take it into the garage.

So you can basically buy a car with all of these independent attributes or you can buy a car which has everything.

Which is reliable, which is safe, which looks good, which is comfortable but then you end up spending \$100,000 for that one.

So again you have choices to make here.

So why am I telling you this?

Anybody?

Same thing applies to information.

If you look at information, there are different ways

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

in which the information is valuable and different ways in which information needs to be protected and you can make independent decisions.

Just like you can buy a very comfortable and reliable car which looks crappy and which is cheap.

Similarly, in information, you have different dimensions in which you can look at information.

At that's what we're going to look at.

So if you look at information, it has got three primary dimensions of security.

Confidentiality, integrity and availability.

There are other dimensions too but these are the three primary ones that we'll consider in our classification.

So if you look at most of the people when they think of security breaches what do you think of?

Confidentiality.

Right?

That somebody was able to see information which they were not supposed to see and that's an important dimension.

But there are other dimensions which are equally important as we will find out in the following discussion.

So let's look at confidentiality.

Why is confidentiality important?

Exactly.

Trust is one of the most important things and why is there trust?

There are things which you do not want the general public to know for a variety of reasons - for embarrassment, for discrimination purposes or it could even be legal - financial loss. Absolutely.

So let's take an example.

What is information that you have which you would not want anybody else to know?

*Audience: Social Security numbers.*

Why would you not want social security numbers to be publicly available?

*Audience: Because that would lead to other breaches.*

Exactly.

Because it could lead to an identity theft.

Somebody could use a social security [number] and open a bank account, open a credit card, do whatever they want to.

So confidentiality is important.

Why wouldn't the students want their parents to know their grades?

*Audience: Again, financial loss.*

Right - financial loss – absolutely. Well said.

They may cut off all the funding which they are getting.

So there are a variety of ways in which ...

Also for embarrassment.

If somebody has a medical condition right?

A potential employer could discriminate against them because of the financial liability, right?

Why don't people want to give out their ages?

Because it might dissuade a potential suitor into not

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

selecting them because they are too old or they are too young.  
And that's why people want to keep that private.  
So there is a variety of reasons, all different reasons, why people want to keep information confidential.  
So now let's look at integrity - why is integrity important?  
Let's give an example.  
Let's take the case of A-Rod [baseball player Alex Rodriguez].  
A-Rod and his wife are going through a divorce.  
They apparently had a pre-nuptial agreement.  
If integrity was not an issue and A-Rod's wife was able to add another zero to the pre-nup agreement, what happens to the whole integrity issue.  
Suddenly A-Rod is a complete pauper and his wife is very, very rich.  
Right? I'll give you another example...  
Oh, it can be just the opposite too, the same thing could happen.  
You just take and scratch out a couple of zeros and then he gives nothing to his wife.  
So integrity is important.  
Let's take another example.  
During the New Orleans floods, most of the documentation was gone.  
There was probably one archives office which had all the information in there.  
If somebody were to break into that archives office, and be able to change the names of people on the deeds or a piece in the electronic records, what happens in the end?  
That's the only record of who owns a particular house.  
In that case, the person who really owned the house is probably out of his house, right?  
I'll give you another example.  
How many of you went to SUNY Albany?  
How are your grade records stored at SUNY Albany?  
Paper in the old days. It's all changed now - it's all electronic now.  
So what happens - all the grades that you have are stored electronically.  
In my lab, I have a team of very smart hackers.  
They can break into almost anything.  
So when you ask the registrar for a copy of the grades - what do they do?  
The clerk, sitting at the desk, you know, he/she looks up the grades, sends it out to print, puts it in an envelope and mails it out.  
That's what happens.  
If, tomorrow, a couple of smart students from my lab, they go in there, they break into the data base, change all their C-s to A-s - they don't change them to all As because then that will be caught - so A-s, B+s and whatnot and instead of a grade point of 2.2 they suddenly have a grade point of 3.6, 3.65.  
And they go ahead and change all of that.  
And a few days later they call up the registrar's office and they ask for the transcript and what happens?

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

*Audience: They get into a position they weren't getting into before.*

Absolutely.

They get into graduate school, they get into a job they were not getting into before and suddenly they are now the brightest students coming out of the university. Is this possible?

Absolutely.

So this is where integrity is an issue.

If integrity in education - if people were able to break into their grade records and be able to change their grades - the integrity of the academic institution itself is in question.

And it's not as hard as it looks.

It's a single data base.

You know, you may have all kinds of protection, but again, there are people who are manning the data base, there are graduate students that work with the data base, and anybody can go in and change the records and whatnot.

Now, there are protections in place.

I'm not going to tell you exactly how to do it but it's doable.

So, how many of you would like to change your grades?

So that's when integrity becomes important right?

So that's the second dimension.

The third dimension is availability.

Now what's availability?

See we have a right to things which we expect and if that right is violated then that's a lack of availability.

I'll give you an example.

You all claim that you all have cars, right?

How many of you have garages and homes?

Every morning, what do you do?

You pull out of your garage you come out of your driveway, right?

And head to work, no problem, right?

And typically you're getting late, so you're in a rush, come out and you want to get out of there as soon as possible.

How many of you are in a rush in the morning?

All of you.

OK so tomorrow morning you are running out of the door, you pull out the car from the garage and into your driveway and as you're leaving you see a huge truck parked right in front of your driveway.

What are you going to do?

You beep, curse, complain but the truck is not moving.

Certainly there was an expectation that you have your driveway which gives you access to the road, right?

And what is this?

This is lack of availability.

So similarly, people have a right to information.

There are different agencies seeking information from other agencies.

There is the public which is seeking information from government agencies.

So if that right is breached - if they don't have the right - that's lack of availability.

In case of a disaster, there are mitigation processes.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

In case of a disaster, the people need to know where the health care services are.

The police and the health care services need to interoperate.

In case all of that is denied, the data that is required for critical infrastructure and for supporting operations at that time is not available. That can cause serious consequences.

So again, when you think of security, don't only think of security breaches, there are other dimensions of security beyond confidentiality which are important which include integrity, which include availability.

So these are the three dimensions which we are going to look at as we go along in this classification process.

So what we are going to do is - whenever we look at a piece of information, we are going to consider that piece of information in all three dimensions which is confidentiality, integrity and availability.

And in each of these dimensions, we are going to figure out whether the security requirements are high, moderate or low.

Is this point clear?

We have three different security dimensions - confidentiality, integrity and availability similar to what we have in a car - the price, comfort, safety.

You can use the same thing.

If the price is high, [moderate] or low, comfort is high, [moderate] or low, safety is high, [moderate] or low.

Same thing we will do here.

We will consider confidentiality, integrity and availability and when we classify information we will classify information as high, [moderate] or low in each of these three dimensions.

Is this point clear?

Could we have broken that down into 5 dimensions, between high, [moderate] and low, between high and [moderate] and between [moderate] and low? We could have.

But I think in the collective wisdom of Information Security Officers, to try to balance out between the complexity and the effort involved and the amount of decision we need, we decided on three levels - high, [moderate] and low.

However, in case your specific agency feels that you need finer distinction between levels, you can always have 5 levels or a 7 level scale which you measure along each of these dimensions.

So, let's go to the next slide.

So, this is what you will have.

For each piece of information, you will look at each of the three dimensions and you'll look at the three levels.

Now given the three levels and the three dimensions of security how many different, unique classifications can each piece of information have?

*Audience: Twenty-seven.*

Anybody else have a different answer?

Anybody say nine?

Come on, I want a different answer.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

This one is right, but I want somebody to give a different answer so I can explain why it's wrong.

It's 27. Why? Because if you look at confidentiality -  
- for each level of confidentiality, we have three  
different levels of integrity, and for each level of integrity,  
we have three levels of availability.

So basically if you go through the three's you will have  
27 different combinations.

And 3 cubed is the right answer.

But I always look for a wrong answer and I can say,  
'No, that's not right' and then I'll explain why.

So there's what the cube looks like.

Along the three dimensions you have high, [moderate] and low along  
each of these and that makes 27 different unique combinations

OK, so, this is the end of the second part.

So what did we learn here.

One - there is a three step process that you will  
follow - the first is doing an asset inventory.

The second part is doing the actual classification, and the  
third part is figuring out the controls.

So that's the first thing.

The second thing we learned is the scope. The classification is  
totally independent of the media on which it is stored.

It could be on a data base, it could be on a thumb drive, it  
could be voice, it could be text, it could be video.

They all need to follow this classification Policy.

And the third thing which we identified is there are many, many stake holders.

There is not one single person or group which needs to work  
on information classification.

The State entities themselves are responsible for that,  
which means the management of the State entities.

We have information owners, information custodians, Information Security  
Officers, and each of us has a specific role to play in this  
Information Classification Policy.

And lastly, but not the least, how many dimensions  
of security do we have?

Three.

And how many levels? Three.

So how many total unique different classifications?

Not you, somebody else.

27.

I just want to make sure that, you guys are sitting here for  
3 hours with me and once you go  
back you have your own lives and you'll forget all about it,  
so my goal is to make sure that I drill each and  
everything down here which I'm telling you so that  
you'll remember at least part of it later on for the future.

So, the first part was really related to why information  
classification is important.

And the second part really referred to what the different  
pieces of the classification materials were and the  
overall process of how you are going to go about doing it.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

And finally, figuring out the nomenclature and the different dimensions of security.

**Part III. Information Classification Process**

And this is where the real crux of the whole process starts - the information classification process.

So pay special attention - not that you didn't need to pay attention before, but even more attention here.

How many of you are still going strong?

Anybody ready to doze off yet?

No?

Zero?

We can go on.

So let's look at the process.

The first part of the process really is identification of all of the information assets that you have and people think that it's an easy process but that's one of the hardest things to do is to figure out all the information you have and where it all exists.

I'm not only talking about work.

If you look at your own personal information.

you have so much information, it's probably very hard for you to catalog each and every piece of information that you have.

You know you have your bank records, all of your passwords, all of your financial information, your grades, your certificates - the names of all of the people who have worked on your house, your deeds, your stocks and whatnot.

You have so many pieces of information, if you start tabulating that you will fill several pages.

And a lot of you probably don't even know where it is and how to protect it.

So getting a good idea of what information you have is probably hard.

How many of you know precisely what pieces of information are on your computer?

One, ok.

No, you cannot raise your hand any more.

So that's a problem.

If you look at it, we have so much information and we don't know where all that information is stored. We don't know what it is worth and we don't know where it is.

So that's the first thing which we need to figure out is an inventory of all the assets.

So before I even go forward - what is an asset?

OK - you can raise your hand - I was just kidding.

*Audience: Any piece of information is potentially an asset.*

It does not have to be information - an asset can be anything, anything of value - right?

Your spouse could be an asset - for some of you it might be an asset, for others it might be a liability, so either way.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

But again, it could be anything.

It could be value - some people value their children a lot, some people value their properties, some people value their stocks and bonds, some people value their jobs - anything could be an asset - something that you value.

What we are going to focus here on is information assets.

So if you look at an asset, an asset can be both tangible and intangible.

A tangible asset is something that is physical - something which we can hold, something which you can value easily - right - just like property, stocks, bonds, patents.

Say that again?

*Audience: Cash*

Cash, right, that's definitely the most tangible asset.

If you look at intangible assets, what are the intangible assets?

Trust is an intangible asset and morale.

What happens if there are security breaches - there might be loss of morale.

What happens if there are security breaches, trust might be broken - right?

So these are non tangible assets and they are both very important.

And if you look at large corporations, a lot of the corporations value the non tangible assets a lot more.

A company like GE - we did a study there.

They really don't care too much about the physical assets. They can always replace computers and what not - and even people.

What they really care about is their reputation, their brand name, their trust.

That's where they've invested the most.

So again, what you value more really depends on your contacts, your organization and how you feel about it.

So what we're really focused here on is information assets which is considered tangible assets because you can put a value to the information.

There are three parts to it.

One is just doing a pure inventory.

Second thing, is grouping those assets together into some logical groupings.

And finally, identifying certain attributes of that information, including the owner, the custodians, where it is used, how it is used which will help you in classification.

First of all is doing an asset inventory - finding out where all the assets are.

So how do you go about doing this?

Take a step back.

If you had to do an asset inventory of all of the pieces of information that you have, how do you go about doing it?

Somebody.

If your job is that tomorrow you have to go and do an asset inventory of all the information assets that you have, what process will you follow?

You go back to the information owners as to

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

where the information is coming from.

It's not one single person where all of this information resides.

It is basically spread across your whole household

That's the answer I was looking for.

And the same thing happens in an organization, one single person does not know where all the pieces of information are .

One single person does not know the value of all of the information.

This has to be a devolved effort which is spread across the whole organization.

And that's a very important point that you must note.

Each business unit must be responsible for their own asset inventory.

It starts at the top - you basically spread out the mandate that each business owner needs to do it and each business unit can further subdivide it based on how large the unit is, how many people they have and the resources they have. Basically, it is a devolved process.

And typically the process will start with the unit leader or unit head who is basically going to give a dictum on that.

I was told that some of you already have your information asset inventories, based on previous laws like the NYS Archives Law and so that might be one good place to start this process.

So let's say you did identify your assets. And before you figure out how to protect them, the first thing you might want to do is start grouping those assets.

What do you mean by grouping those assets?

What does somebody mean by grouping of assets?

Why would you want to group the assets?

You have all the assets - you've done your inventory - what is the purpose of putting them in groups?

Economies of scale, and that's a perfect answer for that.

Because you don't want a million pieces of data sitting together.

You need to organize it such that you are able to look at them as groups of pieces of information rather than individual pieces of information.

Right.

Because otherwise it will become as unmanageable as it was before.

You have a million pieces of information floating around.

You really need to put them in groups.

How would you group it?

You would group it based on the level of protection that you think that the data needs.

If several pieces of data need similar kinds of protection you want to group them in the same asset.

Why would you want to do that?

So that you don't have to classify them separately, you don't have to provide separate controls for each of them.

So management of data becomes much easier because of the economies of scale.

You are looking at a lot of different things at the same time rather than as individual pieces.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

Now is it always wise to group the data?

*Audience: No*

Somebody else, is it always good to group the data?

Why not?

*Audience: Different control levels.*

Different control levels.

There are two disadvantages of just grouping the data indiscriminately.

One, by adding a piece of data to a large set of information that you already have, you might escalate the security requirement for all of the data. That's one disadvantage.

The other disadvantage is that you are going to protect, give the same level of protection to, the entire group of data.

So the second big disadvantage is some pieces of information which should really be more freely available will now get restricted because they are in a group which is a restricted group and it should be freely available.

If there is some aggregate information about spread of epidemics and whatnot which researchers need or the public needs to know -

if it is basically mixed in with a group of

personally identifiable information then you can not release it because it has a level of protection which it does not require and it does not deserve.

Does that answer your question?

So grouping is not always smart because it can unduly restrict your data, one, and second, it can escalate the privileges of the entire data.

Just adding a personally identifiable information to a group of data which would be public, you're trying to make it private and sensitive which does not make sense.

So you have to be smart about this as you are grouping.

What we're going to do now is - now that you understand the grouping of data and whatnot - we are going to do some sample inventory sheets.

So for that, I want you to go to the right side of your folder, sorry, left side of your folder and pull out this process chart [see Exercise Materials – Process Mapping/HR Employment Process].

We are going to use this example throughout the whole lecture and we will base our classification on this so that you can figure out how this is happening.

Initially we were going to show you an example from one of the pilot studies we did at an agency but because of privacy reasons and security reasons we pulled out a very benign piece of process which we are going to use in our training here.

Now this is a human resources employment process.

The process starts after a person has been interviewed and identified for being hired and these are the instructions sent to the HR department for hiring a new person.

So that's where the process starts.

So you should think of it as such.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

The first part is the new employee form that is sent to the candidate. The forms are returned by the candidate to personnel, it's sent to the human resources, to the hiring department for signatures.

Once it is signed, it is sent to the budget for review and so on and so forth.

This whole process follows along.

So we're going to use this process through the exercise.

So the first thing that you need to do is fill out an Asset Inventory Sheet [Appendix C – Information Asset Identification].

This is how you identify all of the assets and you fill this thing out.

This is just a template of what you could use.

You could create your own asset inventory sheet as you would like.

What does this contain?

Once you have an asset identified basically get your template where you can put information about the asset.

The things to note here really are the owner, the custodian, and the user.

They're all three distinct entities and this distinction is very important as you will know as we go forward.

The other thing that you need to note here is that

- how many of you have computers?

You all have computers, right?

Does your computer have an asset tag number?

The same thing needs to be done for information now.

You need to define an identifiable number which is a unique numbering scheme for the different information assets that you have.

Same thing.

You can create similar to what you have for your asset tags.

You can have, similarly, information tags.

There is no mandate on what the numbering scheme should look like but typically it makes more sense to have a numbering scheme which is more mnemonic, which kind of lists the agency first and then the department first and the sub-department and then some kind of a number so that it can be easily identifiable as you are just looking at the asset tag.

So now comes the important part - what is an information owner?

An information owner should be a person who is in management, who understands the value of the data.

It may be the person who created it or it may not be the person who created it.

It's somebody at a management level who understands the value of that information.

The primary role of that information owner is to identify the value of the information, to classify that information and be the gatekeeper of information in terms of authorizing access of the information to other people.

The information owner may or may not have created the information.

The information owner may or may not have physical custody of

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

the data.

So this is a point which you need to remember - that there is a clear distinction between the information owner and the information custodian.

Typically the information owner will be a person designated by the management who has the responsibility for making these decisions about information classification as well as about access control.

An information custodian, on the other hand, would be a person who has physical custody of the data, who gets the classification from the information owner and who implements the controls.

So don't expect IT [Information Technology] who will typically have large databases to be the owners of the information.

The information owners should reside in functional units, who understand the value of the information, which have also probably created that information. But it may or may not be the person who actually created the information. It may be the management at the top level who is the information owner who is making decisions about the classification of that information and about access to that information.

Is this point clear?

So we need to make sure we are absolutely clear about the distinction between information owner and the information custodian.

Owner is a management person who makes decisions about classification and about access.

Custodian is a person who typically has physical access to the data, gets the information controls or the information classification from the information owner and implements security controls and provides access and authorization very often which lies in the IT [Information Technology] support.

Questions?

This is important.

Whenever there is a conflict about who is going to be an owner in an agency, in a department, or in a sub unit.

If there is a conflict, who should be the owner? Move one level higher and the management at the top can become the owner of the information, if there is a conflict or issues to be resolved.

But it should logically be a person who understands the business value - somebody at the management level.

Should you have multi-owners to the same information?

Exactly - that is the right answer - there can be conflicts in what the two people decide.

If one person thinks that confidentiality is high and the other person thinks it is low, what should the confidentiality be?

So, typically you want to have one single owner to a piece of information and whenever there is a conflict go one level higher to a higher level management who owns the information.

And ownership of information comes with responsibilities and

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

one of the responsibilities is that you need to consider all of the risks for information exposure. We need to understand the issues of trust, legal issues and so on and so forth.

And very often a person may not have all that information. So an information owner should also have access to the legal as well as subject matter experts in the area as they are making decisions.

Now again - I've already discussed it - who is the custodian?

The custodian is a person who has physical access to the data, who basically stores the data.

If a third party has your data, they are just information custodians, you are still the owner of that so you have to do the classification.

You have to decide who can get access to it and you need to communicate that to the third party which maintains controls. The owner and the custodian can be the same person, for instance like you said.

I've generated my file, I own it and at the same time it is on my computer. So you could be the owner and the custodian if need be.

Can we have custodians with the same data?

*Audience: Yes*

Absolutely. right.

Why is that, why is it 'absolutely'?

As soon as you make a copy of the data and you give it to someone else on the thumb drive, the laptop, or whatever else, then there are two people that are custodians of the same data. So whereas you want to have only one owner, most often you will have multiple people who are custodians of the same data because the data is replicated, the data is duplicated, and so on and so forth.

And the third thing is the user.

Can we have many users?

*Audience: Yes*

Absolutely, we can have many users.

Can the same person be the owner and the custodian?

Yes.

Can the same person be the owner and the user?

*Audience: Yes.*

Yes. Can the same person be the owner and the custodian and the user?

Yes.

There are instances of all kinds.

So, what we've done here is - given all of this that you have learned about owner, and custodian and what not - lets try to fill out this Asset Identification Form.

What this contains is basically all of the information about the asset which you have.

The asset which we are looking at today is the HRM form or we can expand it to consider the entire group of files which are listed here, which is the HRM Form, the Health Insurance Form, the Benefits Package, Tax form, I-9 and so on and so forth.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

If you start filling it from the top, completed by...your name,  
you have the date, this was the date when I created this slide,  
the department ....HR, and the department head,  
name of the information... HRM form.

Instead of HRM form, if you are grouping the asset  
you could use the entire group here.

You can use the HR file, which contains all of  
these other forms.

What is the use of the asset...hiring, payroll and benefits.

And information asset format...

What is the information asset format?

From here, if you can look at the process chart and  
figure out both electronic - it's stored in a  
database and a filing cabinet where it is stored.

So both of these. And the source of the information is  
the employee.

Similar to the health records, the source of the information may be  
the person whose health records you're storing or the physician  
who is reporting them to you and at the same time you become  
the owner and custodian of the data.

So that's where the distinction comes in.

And - information owner.

Why is the information owner the department head?

What happens in this case?

Because there are several HR staff - people there who work with  
different units of the university, who manage hiring, and what not processes.

So we cannot take one person out of them, they are  
all our owners in their own rights.

So we went one level higher which is the head of  
the department of HR here.

So now we are going to do the actual classification process.

So how is the classification done?

The information owner sits  
down and he talks with a set of experts.

And they use the Information Classification Worksheet.

Now do you guys want to pull out the Information  
Classification Worksheet? [See Appendix C]

Because we will start using that.

So pull out the Information Classification

Worksheet and also the Appointment Request Form. [See Exercise Materials – University at Albany  
Appointment Request]

They are the two forms on the left hand side.

What we are going to do is if you look at this form,  
this worksheet has three columns.

What the worksheet gives you is; remember I told you  
that whenever you do classification it is really a  
decision analysis problem where you are considering  
several different factors while you are deciding.

What we have done is provided you with a set  
of questions which considers all the different aspects that we  
could think of, in terms of what you would need to consider when  
classifying information.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

We have the first column for confidentiality, the second column for integrity, and the third column for availability. As you step through all of these questions you would have considered all of the different aspects. For instance what is the impact on health and safety? What is the impact on finances? What is the impact on trust and so on and so forth. That will help you figure out what the classification is because at the end of this worksheet you should have confidentiality, integrity and availability classifications. What we also have here is your Manual. If you look at Appendix B here, this gives you the Information Classification Manual where several of the questions have been answered. So if you go down to page six of this. Do you have answers to some of these questions? So what I would like you to do is, I would like you guys to look at some of these questions on the sheet and look at some of the example answers that they have so that if you have any question you can ask me now. What we will do then is use this appointment form that we have, which you just had, and start classifying that form. And you guys are going to answer all of the questions and not me and that way we will have an interactive session of trying to do classification. Ok. Now, you all have this appointment form, right. We are just going to use this form now, not the whole group, and we are going to use this for classification purposes and you are going to classify this information. Now, as we go through each column of questions, as soon as we hit a high on something, what do we need to do? Jump over to the next column. Why is that? Once you have the highest classification and once we know it meets the highest classification it cannot go any higher and it cannot go any lower because it already had the highest classification. We just move onto the next one, and if you don't hit the highest one then we go onto the end of the questions, why? Exactly. Because it's still a possibility that you might hit the highest one. I just want to make sure that you guys are thinking about these things as we go along. So let's answer the first question. Does the information include or contain PPSI - Personal, Private or Sensitive Information? If you go to the website they have an entire list of everything which constitutes PPSI. This is your personal information which can be used for identity theft, that's the primary motivation behind this - we don't want to disclose this publicly.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

So, which means that it is PPSI.

So what do we do then?

Go onto the next column.

All right, so let's start answering this one.

Does the information include medical records?

No.

Is the information relied upon to make critical security decisions?

Who says yes?

Who says no?

How many people say no?

How many people say yes?

What happened to the rest of you guys?

The rest are all maybe?

This is again context dependent.

Who said yes here?

So why did you say 'yes'?

*Audience: If somebody is going to be coming into the building.*

So basically the door access determined what is in here?

Because the country of citizenship is here and I can remember this from my work at GE.

We use to have export control issues - I was designing aircraft engines at that point.

So we used to have to work in large wards - concrete bunkers under the ground - and we would not let anybody else in unless they had a US Citizenship and what not.

So, again, it could depend.

But again it depends upon the institution.

In some institutions they use HR forms to do that.

In other institutions they have separate access control lists from where they use information from.

So again it depends on the individual organization, what kind of security processes you have.

There are some people here who said no.

Who says no?

Come on - I know some people said no.

You have to be brave enough.

Raise your hands again.

So for now lets consider that the answer is no, just so we can go onto the next question otherwise it will be very quick.

You need to go through some questions or you won't get the experience of this.

What impact does an unauthorized modification or destruction of the information have on health and safety - and that is an interesting one.

Now lets look at an overall perspective, lets look at health and safety first.

First of all if you look at this form, because of the wrong information on this form if somebody needs emergency medical care would someone be denied emergency medical care if something is wrong on this form.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

No, right, so that takes care of that one.

The second thing is that basically in case of emergencies, emergencies can include evacuation or include death.

In case of an emergency you need to know where different people are that can be evacuated. So whenever an emergency like that happens do you think people go into HR forms to find out where people are?

Probably not, right.

So it depends on your specific business processes here.

In case everything links onto this form, whenever anything changes here then everything else changes in your whole, in that case it might be, but otherwise not.

So you have to make a decision based on what you think is the situation in your specific organization.

Like I said, you are making decisions here. This is not giving you the answer so this is where you need to do the thinking and this it is where decision analysis comes in.

And you need to figure out – ‘is it really useful?’ - and for that purpose we always recommend that you have all of the business processes in your organization with you.

So that you can consult and see in case there will be an issue or not.

Anybody else have any comment?

So we will go on with the answer to be.....

impact is limited or minimal.

So that we can answer some more questions here.

What is the financial impact of unauthorized modification or destruction of information?

I think we still can say it's limited.

I say that the impact is severe, when it becomes very hard for the institution to continue on with their business.

If they can recover from it, then it really is a moderate impact.

But again, that really is the perspective of the organization. That's my perspective.

That is how it is considered severe -

that the impact is so severe that they cannot get on with their operation, or they cannot recover from their losses that they have.

So let's say it was limited here.

Ok, what impact does unauthorized modification or destruction of information have on the SE mission?

So let's take the example of SUNY Albany.

If somebody were to change one or a few HR forms - the primary mission of the institution is education - will that be impacted?

All right, we'll go with a minimum here.

What impact does unauthorized modification or destruction of information have on public trust?

Minimal.

The reason being that if people were to come in and change their grades at random in that case the impact would be huge, but somebody changing their HR form by mistake or due to duplicity,

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

it's not going to make a big impact on the institution.  
So the public trust is not going to get that impacted.  
Is integrity addressed by law and regulation?  
If yes, determine the impact on unauthorized modification or destruction of information.  
Is there a law, a Federal Law, a New York State Law, which governs the integrity of the information on this form?  
Which law?  
*Audience: The Social Security Law.*  
So there is a law.  
So what happens if whenever there is a law, then you want to find out what the impact is.  
If the impact is moderate.  
Low?  
Low.  
All right, because if somebody changes it sooner or later you find it out and correct it.  
You'll figure it out.  
And the last question is a catch-all.  
Is the information, for example, financial transactions, performance appraisals, relied upon to make business decisions?  
If yes, the impact of unauthorized modification or destruction of information.  
Yes.  
No.  
Minimal.  
Alright, so we have answered all of these questions.  
What is the highest level you selected?  
Limited, right.  
So what happens, in the end, you look at all of these, look at the highest level you have selected.  
So confidentiality was?  
High.  
Integrity is?  
Limited [moderate].  
Limited [moderate], so then we jump onto the next one.  
Is availability of information essential for emergency response or disaster recovery?  
No.  
This information needs to be provided or available 'as time permits' ...'1 to 7 days' ...'24 – 7'.  
1 to 7 days.  
Now why did you pick '1 to 7 days'?  
Just because it was convenient right in the middle or do you firmly believe it's '1-7'.  
*Audience: It doesn't appear to be an emergency.*  
Right.  
Which - could it be 'as time permits'?  
So how many of you have 'as time permits'?  
How many of you have 1 to 7 days?  
Oh, so there is a balance here.  
Again, see I want to keep reiterating that.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

There is no right or wrong answer, it depends really on your perspective, what your institution needs.

For instance if an institution puts in a lot of grants and they constantly need this information for getting people's salaries and what not - which they get from the HR database - then you might need '1 to 7'.

If all you do is periodic reviews of what's going on, then

'as time permits' would be fine.

Again it depends on the institution.

Ok, what is the impact to health and safety if the information were not available when needed.

Again, to your point, this is exactly the same question.

If you are using this primarily for all of your disaster recovery and what not it can become very important.

If not, if you have other processes in place and you don't use this, then this is not as important for health and safety.

But I think that in a lot of institutions the HR forms really are not the primary source for disaster recovery and there are other ways in which people are going to do that.

For instance, at GE, each building and each room had a specific person who owned that room or that building and their phone numbers were always kept current and they were listed on there.

So whenever something happened they would call so they knew exactly who all were in the lab and who was supposed to work in the lab and that is how they maintained it.

They basically devolved it across all of the management in the institution. So that is how it was done, it varies from place to place.

What is the financial impact if the information were not available when needed?

I don't think there is much of a financial impact here.

What is the impact on the SE mission if information were not available when needed?

Minimal I would say.

What is the impact to public trust if information were not available when needed?

I don't think the public needs to see everybody's HR forms.

So, it's pretty minimal.

So, what was the highest one we selected in availability?

Minimal [low] I think, right.

No.

Wait, wait a minute.

No.

One to seven - that is, that's moderate.

Right, so confidentiality is high, integrity is moderate and availability is minimal [low],

depending upon your perspective, whether you need it 1 to 7 days, or you need it as time permits.

So, you have just classified your first piece of information.

Now what is the most important thing here to note?

Something which I have always reiterated.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

The fundamental to information classification is figuring out your risks.

What do you lose by an information breach?

Right, and all this template provides you is a way of thinking about it, a way of considering all the different things which you need to consider.

Your mission, your health and safety, your financial impact, your trust, and so on and so forth.

So, you have all of the questions here, but this spreadsheet is not giving you the answers.

You are giving the spreadsheet the answers.

So you are doing the thinking not the spreadsheet.

So I want to make sure, that look, in the end you cannot say well I followed the spreadsheet so you know, if the classification is wrong, it's not my fault.

It's nobody's fault, it was your perspective.

Again, this is just a template. This is just a support tool to help you in the decision analysis process.

Now the question really is, boils down to is, if I'm looking at it, should we have consistency in decision making across the whole organization?

That's what you are referring to.

And that is, there should be consistency, but you know it takes time before you achieve this consistency.

So, I will go through later in the talk how you go about the process by which you can actually achieve this consistency.

You roll it out slowly, make sure there is a team of people who are answering questions for the directors and whoever else is engaged in classification so they can get a similar input across.

In the end there should be somebody who is trying to oversee and make sure that there is a consistency across.

Because very often it will not be feasible for all the directors to come together to the same training at the same time in the same place and they might have different perspectives, different views, but overtime consistency needs to be built and can be built slowly.

But that is a good question. We are going to refer to it more in detail towards the end of the lecture.

Okay, we have already looked at the Manual and you have used the HRM form.

See, what was the classification I came up with?

High, Moderate and Low - it's very similar to what you guys came up with, so, I've been trying to push you guys towards these classifications.

All right, so we've already covered this.

Okay, just certain rules of thumb.

As soon as you see PPSI, don't even go forward.

Confidentiality is high you move on to integrity question.

And if you don't know what the confidentiality should be, by default the confidentiality of information is high.

The third rule...in case you have a group of data, the classification of the entire group depends on the highest level that is required in each of the three dimensions for any single piece of data.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

Whenever you merge two pieces of data, what happens?  
What should be the classification of the resultant dataset?

*Audience: The highest of either one.*

'The highest of either one,' is that the right answer?  
If you are merging two pieces of data, they have their own  
classifications, what should be the classification of the  
resultant dataset?

*Audience: The higher of the two.*

The higher of the two?  
How many people think the higher of the two?

*Audience: Start over.*

Yes, that's the right answer.

Why is that?

Because sometimes when merging two pieces of information, we  
can actually escalate the security requirements of the data.

You have a list of names here, you have a list of  
social security numbers, meaningless...you put  
them together, what happens?

It certainly becomes PPSI.

Exactly...so, whenever you're merging two pieces of  
information together, you need to reclassify it.

You just cannot use the highest level of classification from  
the two sets.

Whenever you make a copy of a piece of information,  
what is the classification of that copy?

Don't look it up...answer me.

The same as the original...absolutely.

If you make a partial reproduction of data, right,  
if you take a small part, what happens to the classification?

*Audience: You have to look at it again*

Say that again.

Well, either you can have the highest level,  
the level before, or you can reclassify it to see if  
it has gone down or not.

But you have an option in this case that you can just use  
the one which you had before.

Because by taking a subset of the data it's not going  
to increase the classification levels.

Okay...so you are going to go and inventory all of the data  
that you have, all of the information that you have,  
and you will have information classification of inventory  
sheets...and the  
classification sheets.

It's a good idea to make a central repository of all  
of those pieces of information in the  
classifications that you have for several reasons. First of all, it's easy to see if  
there is consistency across and secondly, it's a central  
repository. If somebody wants to find out if I have access  
to a certain piece of information, you can just go  
to a single repository and see what the level of information  
classification was and whether a person can get  
access or not based on that.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

What should be the confidentiality level of this repository of all of the classification documents, and why?

Very often it should be high.

Unless the information that you store is all public information.

Why?

Just because people knowing what confidential information is, that itself can make it more vulnerable to other people.

Because it has a repository or a map of all the information, people knowing what all information you have - what the level of confidentiality it has, makes it more vulnerable to people wanting that information.

If you look at confidentiality, if anybody can go and read that, let's say it's public.

What happens if it's public.

People outside know precisely what pieces of information are stored there, and what pieces of information are confidential, and that itself makes it a target. People like terrorists, people like criminals and what not, know what information they can steal from there.

And for that reason it becomes very important to make sure that people don't know what you have.

Sometimes obscurity is the best defense.

And you're losing that obscurity because you're making that information available to the public.

They know what all information is stored with you, and that makes it more amenable to hacker attacks. It makes it more amenable to people wanting to steal information.

But again, if you don't feel that's important, the decision is yours, but typically it should have high.

What about integrity?

*Audience: High.*

Why should it be high?

*Audience: Controls are based on that.*

Controls are based on that.

If I can go in and change the classification, the confidentiality of a piece of information from high to low or to make it public, what happens?

Suddenly I can get a piece of information which I am not supposed to get because I am able to change the classification levels in the repository.

Especially if that repository is being used for making decisions about who to give access to and how.

And, what about availability?

*Audience: People in my unit need to know.*

*People outside my unit don't need to know.*

Okay, the availability really depends on the business process.

We need to periodically review classifications.

Why is that?

The classification changes over time, why?

Because information which is very important today may not be important tomorrow.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

The legislation changes, the laws change.  
Something which is not covered under the law may be covered tomorrow.  
And the third thing is the business priorities change.  
If something which you think is very important in the business today, you know, the next director comes in and he does not feel it is very important, the mission changes.  
So based on that, it needs to be periodically reviewed and updated.

How often should you do it?  
This is another first question that should come to your mind.  
Okay, so how often should I go back and review my classification?

*Audience: If there is a major change, then I...*

Absolutely, one of the three reasons is, if there's a major change in legislation you might want to do it. If there's a major change in the organization you might want to do it.

Or you might just also have a process in place that, look, every two years we're going to do it anyway; every six months we're going to do it anyway.

Depending on the amount of resources you want to spend, depending on how volatile your information is, you will make an internal decision about how often you want to review this.

But if you don't review it, just maintain it static over time, it's going to get obsolete.

It's going to become useless.

And this brings us to your point.

How do we validate it across the whole organization?

How do you build this consistency?

You know there's a validation issue.

You know if I'm doing classification, how do I know I'm doing it right?

Does anybody have this question?

How would you show that you're doing it right?

Where do you get the validation from?

Typically for validation, that's what I was telling you, there should be a central unit.

Maybe involving the ISO [Information Security Officer], people from the legal department, and a team of people who basically go about advising people about how to do classification or reviewing the spot checks or totally across the whole organization to make sure there is consistency across this whole thing.

So this kind of validation is important.

And, you know, it's important to involve lawyers in this or the legal folks in this because if something goes wrong, you need to make sure that you're covered, that you've gotten through the legal review.

And you also have other laws like the records retention law and you might want to make sure that what you are doing also complies with the other laws that you have.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

Okay...so what did we learn from all of this?

This really was the process which you learned in this section.

How are you going to go about doing the inventory of all of the data;

how to fill out the Information Inventory Worksheet; the distinction between the owner and the custodian, and that's very important; and how do you go about selecting the owner and the custodian. What's the difference between an owner and a custodian? The owner is the person who makes a business decision about the importance of the data, analyzes the risk and does the classification, whereas the custodian takes that information about the risks and the classification and actually implements the controls, so there is a clear distinction between the two which you must uphold.

What we also saw is we went through an example of information classification using the worksheet.

Like I said before, the worksheet is divided into three columns to jog your mind into thinking about confidentiality, integrity and availability.

And as you thought through the processes you were able to classify the information based on the three criteria that we have or the three dimensions that we have - confidentiality, integrity and availability - and you're going to use this process.

As you use this process over and over again and again the decision making will become easier and easier because you will have some reference to compare it with.

And we have a Manual provided which will help in classification and in bringing consistency to what you are doing.

#### **Part IV. Information Classification Controls**

The third part--the controls.

So what have we done so far?

What we have done so far is, we figured out why protecting information is important, how this is becoming an unmanageable problem.

And then we figured out what the process of managing your information security is by first identifying what you have, by classifying information then putting in controls.

We figured out what different pieces of information you have.

We've also figured out what the dimensions of security are and what the levels are.

And finally, we went through the process of classifying it by forming the spreadsheet, which is a template that you will use.

Now, for the last major chunk.

You know what your information is, you know how to classify it...how do you pick out the controls?

That's the last major chunk.

Once you have the controls, your information is protected and

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

so on and so forth.

So the question is, what is a control?

And what's the purpose of a control?

The idea of a control is to be able to minimize the risk to a manageable level.

This is something you need to remember.

That in no way can you have perfect security.

The idea of controls is to not to prevent anything from happening--things are still going to happen--but to reduce the probability, to reduce their loss potential to such a level that you can manage it and you will not go bankrupt or you will not destroy your business based on that.

It's kind of an economic decision as to how much money you would invest in controls, and what you would invest.

If you look at the controls, it has several purposes to it.

One is deter, protect, detect, respond and recover from it.

So these are the different five elements of that.

We are going to do an example

of a house and then I'm going to compare that to what happens in the information technology world to compare how we have different kinds of controls.

And then I'll go through and explain the processes that we have set up for you guys to figure out the controls.

If you look at the deterrence, what are the different deterrent measurements that you use for protecting your own personal houses?

The ADT sign, that's one thing.

Having a dog, that's another one. That is a deterrence - people don't even come.

You may or not have ADT, but, you know, if you just stick a sign in your yard saying ADT protected, a lot of people are not going to come.

You may or may not have a dog, just have a, you know, a tape recorder, a record player just barking every now and then.

That will deter some people from entering.

The third thing is some people have the automatic light switches which switches on and off in different rooms when they're traveling.

That's a part of the deterrence, because if people know that somebody is in the home then they are not going to come.

So, that's your first level.

What is the corresponding control for information security in organizations?

What are the deterrence controls that we use?

How many of you are IT [Information Technology] staff here?

Very few.

What kind of controls do we have corresponding to this.

What will prevent people from actually doing this?

Right, absolutely, the policies with repercussions.

Now look, if you do this, you will get fired.

The second thing is that, look, we are monitoring all of your email.

You may or may not monitor it because half the people are

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

not going to do it.

Right?

If you say that, you know, precisely what you are doing, you can monitor what you do on a computer, people are not going to go to gambling sites, people are not going to go to pornography sites, because they fear.

So that's a deterrent.

But saying that you are going to do it will prevent people from doing this.

So let's go to the next level.

That's a deterrent which prevent people from doing this.

The second thing is protection.

Now, how do you protect your house?

Locking is one of them.

How else do you protect it?

*Audience: Shotgun.*

Say again, oh, let's not go there, I'm a non-violent person here.

*Audience: An alarm system.*

Right.

If you look at an alarm system, it can be construed as protection, but it typically is more of a detection system. That is, if somebody comes in, that's a detection system.

So, how else do you protect it? By having your iron bars on your windows, like they do in New York City in some areas. You'll have, you can't have glass windows. Somebody is going to break in and come in.

You have to have the iron grills on windows, and so on and so forth.

So there are several different ways in which you protect.

So what is the same protection mechanism [in the information technology world]?

*Audience: Encrypting the data.*

What?

*Audience: Encrypting the data.*

Encrypting the data could be one of them, right, what else?

The firewall.

You create a firewall so that people can't penetrate into that, passwords that people can't break. Those are your protection mechanisms.

Let's go on to detection.

How do you do detection?

*Audience: Have cameras installed.*

Cameras installed.

That can be one of them.

ADT- that's a detection if somebody breaks in.

The third way is if you come in and your locks are broken and everything is strewn around.

You are the detector in that case.

So there are different detection mechanisms.

What is equivalent in the IT [Information Technology] world?

*Audience: Intrusion detection/response systems.*

Intrusion detection system is one of them.

The second thing could be a log analysis.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

You basically look at logs constantly, periodically review the logs to see if there is some activity which is going on which should not have gone on.

That's the second way of doing that. And the third way of doing that would be, basically, periodically do an audit.

That is a third way of detecting if there is some fraud going on or something else.

There are several detection mechanisms.

So, you come in and you see a break in at your house.

So how do you respond?

*Audience: Call the cops.*

Call the police.

You run out of the house, say, 'Oh my God,' call all the neighbors, create a ruckus there, but mainly, you call the police.

You know, you basically go into safer surroundings, you make sure that you're safe.

And, what do you do in the IT [Information Technology] world for that?

Say that again?

Right, you basically do forensic analysis to see what's going on, right?

The second thing which you do is, if you find any issues with that, then you basically protect your systems better.

You change your passwords. You sometimes have to reimage your machines.

Change your firewall - change the settings on the firewall, upgrade the rules on the firewall.

That's how you respond and the final thing is recovery.

Your recovery is - in your house, if something happens - you call your insurance company, you buy new stuff, you change the locks, and so on and so forth. That's your recovery.

And what's the equivalent in the IT [Information Technology] world?

*Audience: You restore any damaged data. You update your security protocols.*

Exactly, the most important part of your recovery is to update your security protocol, make sure that this does not happen again.

That's part of a recovery.

And also, updating whatever you have lost in the incident.

So you understand where the controls are coming from.

You do controls all of the time.

In the IT [Information Technology] world - a new world, again - the same kind of controls, the same motivations - preventing people from entering, blocking people from entering. And if they do enter find out what's going on, respond to it and then finally recover from anything that happened and protect yourself better for future.

The same thing happens here, so think of it in this context when you think of controls.

What we are trying to do is - it's just like your house

Protection - you're protecting your IT [Information Technology] world in the organization.

What you are trying to do is, clearly remember that you need a risk analysis, try to figure out what can you lose

if information is breached, whether it's confidentiality, integrity or availability.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

What you're doing in control is a risk mitigation activity.

In risk analysis, you can find out what can go wrong, how much you can lose. In risk mitigation, how can you protect what you can lose to a manageable level.

I'll give you an example of how you reduce your risk to a manageable level.

Sometimes you get insurance on your car or your home, and you have a deductible...\$100, \$250, \$500, why is that?

You're making a compromise between your ability to withstand the damage and the amount of money you need to invest in insurance.

The same thing happens here.

You have controls.

You only want to have controls to an extent that you can withstand the damage and somehow optimize it so you're not spending too much money, at the same, you're not losing too much money.

So it's really the compromise between the two of them.

The same thing happens in controls.

So what you want to do here is select all of your baseline controls.

What you have here, the way we have created these controls for you here is that it can be a daunting task if you go about finding out each and every individual control, so what we have done for you is, we have done a predigested risk management plan for you whereby, based on the classification, we have pre-specified the controls that you will need to implement.

So you have a baseline set of controls which will be provided to you.

What you will need to do is, in case you need controls beyond that, you can supplement them, but at least you have baseline controls to start with.

And that's what we provide you in this control section.

Some of the, well, a lot of the controls you already have, should be in place because of your security measures already in place and because of the CSCIC [Office of Cyber Security and Critical Infrastructure Coordination] security policy.

But, what we will show you is that, based on the classification, what controls you will need and how to figure out the missing controls.

So where did we come up with these controls?

These controls are not something which we created from scratch.

A lot of the controls are mentioned in some of the standards handbooks-like NIST [National Institute of Standards and Technology] comes out with security handbooks.

We have looked at the NIST handbooks.

And in addition to that the International Standards Organization (ISO) has a security guideline or security bulletin, 17799 [27002] that's a standard.

We have used these extensively to figure out the controls that you will need to implement.

In addition to that, we have looked at periodicals, we have

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

looked at the papers, and we have also consulted with experts and ISO's [Information Security Officers] in figuring out the control data required. So it's not something which we have just pulled out.

We have basically taken a lot of wisdom from several different sources to get you a set of comprehensive controls.

Like I said, given the three dimensions of security and the three levels, how many different unique classifications can we have?

Twenty-seven.

So, what we've done is, for each of the 27 different classifications, we have a corresponding control chart which comprehensively lists the controls that you will need.

Selecting the control list perhaps is the easiest part for you guys.

You figure out what the classification is and you have a set of 27 control charts and you figure out the right control chart based on the classification level and you have all of the controls that you need.

It's as simple as that.

But we'll still go through the process and I'll explain to you where the controls are.

Before I even go there, let me explain to you what that looks like.

Your control charts are really an Excel spreadsheet.

What it has is, it has an index page in the front which lists all different 27 classifications.

And corresponding to each of them, hyper-linked to them, is a separate worksheet in your Excel workbook which lists all of the controls that you need.

It is just like a book.

You can go through it and figure out all of the controls.

What I'm going to go through is more the mechanics of the controls on how to select controls rather than the controls themselves.

Let me go directly to the spreadsheet.

No, this is not the right one...ah, this is it.

This is what you will see.

If you look at the bottom here, you see the rating menu.

Can you guys read this rating menu?

If you go further down you see 1LLL, 2LLM and so on and so forth.

Each of the separate tabs, they represent a different classification and corresponding to that classification you have a tab which lists all of the controls.

So how do you get to that?

Well, you know, you can just tab. Let's go to one of them.

If you look at this index page, you have the page number corresponding to the different classifications and you have a hyperlink and it describes what classification it is.

Let's just click on this and go to low, low, and low.

What do you see here?

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

What you see here is your sample control chart, which is for low confidentiality, low integrity and low availability. And what it lists is all of the different controls that you would need.

The largest column, the middle column, it basically lists what the control is, and the right hand column tells you why that control is required, whether it's for confidentiality or integrity or availability or for multiple things.

The same control can be required for multiple things or multiple dimensions.

What you also see is that there are separate subsections in this control chart.

What the separate subsections tell you is a suggested role for who should be responsible for those controls - the State Entity, or the Information Owner, or the Information Custodian, the User, the Information Security Officer.

What we have tried to do is, we have provided you with all the controls, suggested certain roles for each of the controls as to who should be managing that control, or implementing that control and we have provided you with such a sheet for each and every single classification.

Now remember, this is a minimal set of controls. You can add more security controls if you need to.

What it also says is if you need to change the suggested roles, feel free to change the suggested roles.

This is not something which we mandate.

We just suggest these roles so that it makes it easy for you to start in assigning the roles for different people or assigning the controls for different people.

And to the left of this you have a column which gives you the glossary reference number. Now, what is that?

We have a separate document which describes in detail all of these controls.

It basically refers to the index number of the specified control into that glossary.

So what you have here is, you have a control spreadsheet and a glossary.

The control spreadsheet gives you controls for each different possible classification of information and the glossary is a reference Manual which gives you details of all of these controls.

So what you have here

is...you have the explanation of the control which is right in column E, you have why

it is needed in column F--confidentiality, integrity, or availability, and what kind of a control rating it is and the suggested role, and whether it is required or it is optional. When it's an 'R' it is required, otherwise it's an optional.

And what we have also done is we have segregated the controls based on types, for instance authorization, backup storage, so on and so forth. There is a list of categorizations here.

But this is just more for explanation.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

And a neat feature - if you hit Alt/Left Arrow it's going to take you back to the original one.

Alt/Left Arrow, that's something which I didn't know before.

If you hit Alt/Left Arrow it will take you back to the original one so you can keep navigating back and forth.

But, all of this does not have to do with the content of this.

These are just navigation arrows which you guys can figure out.

Fundamentally you need to understand why controls are implemented.

Fundamentally, you also need to understand that the controls have been provided for all different 27 possible classifications.

The third thing which you must know is that the controls are cumulative.

For instance, if you have low, low, and low, if you have a set of controls, for low, medium and low, the controls are cumulative. You just add a couple of more controls.

If you go from low, low, low on to higher, the controls become larger and larger and larger because they keep adding on.

For high, high, high, you will need to have all of the controls off low, low, low, plus some additional controls will be required for the higher classification.

The spreadsheet is available on the website--CSCIC website [<http://www.cscic.state.ny.us/lib/policies/>].

So, all of the information that we have here in this package, it is also available electronically,

which you can go to the CSCIC website and obtain [<http://www.cscic.state.ny.us/security/conferences/>].

All the information is publicly available.

Okay, so we have looked at the index page, we have looked at the sample control charts, and, we have also looked at the glossary.

So these are the three components that you need to worry about.

And based on the classification of the Human Resources management form, we had high, moderate, and low.

This would be the sample control chart for that.

And you will see that the number of controls has really gone up.

The State Entity controls are almost a dozen compared to just three for low, low, and low.

So as you can see, the number of controls has gone up for confidentiality.

You have done your inventory now, right?

You've done your classification, you've figured out the controls that you need.

What do you do next?

Well, gap analysis.

Figuring out what controls you already have and what controls you need to implement.

That's the next step in the process.

What we have done is, we've just took portions of this spreadsheet, and we basically ticked all the things that were implemented here into green and things

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

that were not implemented we put as red.

What we have figured out is, we need five new controls to implement to comply with this Policy.

This is exactly what you will have to do as you go along doing your information classification.

You will need to figure out what controls are already there, and what controls you need through this gap analysis.

And once you figure out what controls you need, what are you going to do?

*Audience: Implement them.*

Implement them, of course.

It's a simple answer.

And if you can't implement them, then you have an exemption process by which you can get an exemption from this.

There may be some reasons why you don't want to implement it, because you might have a control which is stronger than that, or, there might be financial issues why you don't need to implement it.

But, that reason needs to be justified as I'll explain as we go along.

So this is your exemption form and you will find that in Appendix A, I believe, where you have an exemption form.

When do you need to fill this?

When you do a gap analysis, figure out the controls that you need to implement.

If you don't implement any of those controls, you need to get an exemption for those.

And you basically need to document why you need to, why you can't comply with it and second, what risks are posed to the organization by not complying with that.

And, the most important thing is that it needs to be approved by the owner (information owner), the manager, the ISO [Information Security Officer], CIO [Chief Information Officer], and the executive management.

Why do you need to do that?

To cover yourself.

Absolutely, that's the primary reason for that.

In the end if something goes wrong, if a breach happens, you can always show this.

Look, the management approved this because of financial duress, because of whatever reason, we did not implement this. It's the management's responsibility, not yours.

Everything you don't comply with, just document it.

Make sure you pass it along the chain of command.

Implementing controls is not that hard because...well, okay, let me not say that.

Implementing controls is hard, but figuring out the controls that you need to implement is not that hard.

Once you know the classification, you know precisely what controls need to be implemented because you have a control chart based on each possible classification of information.

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

What you need to do then is...do a gap analysis and either implement the missing controls or file for exemption for any control that is missing.  
That's the entire process of selection of controls.

**Part V. How Does an Agency Begin?**

The last part is very, very small.  
It's about 4 or 5 slides.

Well, I think that this part has more to do with the management of this whole process.

The first thing I must reiterate is that information classification is not something which can be done by a small group of people.

Typically the tendency is in organizations, is to get three consultants or get a bunch or three people who they can spare and say

'okay, you need to comply with this Policy, go run around the whole organization and begin an inventory and do the classification and we'll be done with that.'

That's really not the purpose behind this because the moment you finish your inventory and finish your classification it gets obsolete, because information is changing every day.

This process really needs to be institutionalized.

It's really more of a discipline that you need to maintain.

You're starting new projects.

You have existing projects.

You need to make sure that this is a part of your management.

Otherwise, if you look at you own computers, you have collected data for the last 15 years.

It's a total clutter.

We need to be able to manage our data better.

And this is a part of the management - figuring out what you have, what the value of that is, what you need to keep, what you don't need to keep, and how you need to protect different pieces.

That's very important.

Given that the entire organization needs to be involved in this, what's the first step you need? You need the mandates from the management.

And how will the mandates come from the management?

They obviously have their different priorities - conflicting priorities.

The first thing is you need to develop a business case like anybody would do for a good business plan.

Where does the business case come from?

It comes from several sources.

First, you know, the data is really becoming unmanageable - one - and this is a better way to manage data to understand what you have.

Second, in the long run it will be more cost effective.

The longer you wait, the deeper a hole you are digging for yourself in being able to pull out old data and try to classify

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

it and manage it and what not - number 2.

Third, the regulatory pressures which are coming on which will only get worse over time for which you need to do information classification and information protection, so you need to start early.

And finally, you need to be able to demonstrate a methodology which will pervade throughout the whole organization without making a serious impact at any given time that this will be slowly rolled out.

So, as you're rolling it out, what do you need to do?

That would be my recommendation, is to make a team.

The ISO [Information Security Officer] itself, or just one person in the organization, cannot really go through this whole process.

It needs to be a multi-disciplinary effort.

Try to get people from different, from cross-functional areas.

Create a team-we should have somebody from legal, somebody from senior management, somebody from IT [Information Technology], and somebody from the ISO [Information Security Officer] or CIO [Chief Information Officer] staff.

That would be a good team to start with, a minimal team, where you have several different perspectives come together.

And once you have a team, make sure that somebody on that team can write well

because, writing will be an important part of documenting and what not.

The second thing I want to make sure is sometimes the tendency of a team like this, because they understand things better than some of the other people who are new to this, is to just do it for other people.

The job is not to do it, but to train other people to think in this way so that they can do it themselves.

Because, in the long run, you cannot sustain it, it is too large a task for a small team to do and it's a repetitive task, it needs to be done over time again and again and again.

You don't want to get into the habit of people just asking you to do it.

Your job is to facilitate this and create other people to think about how to do it so that they can do it themselves and that's very important.

Third.

For any project, especially this one, they say you need the first application which is really successful.

So, find an organization, or sorry, a sub unit, which is a reasonable size where the management is able to do these things.

If you start with your fist fights in your first one, when people don't want to do it, you almost have to pull teeth to get them to do information classification, you're not going to be successful.

The success rate will be slow, it'll be very hard for you to roll out.

So the best thing is start with a sub agency, start with a

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.

**New York State Office of Information Technology Services (ITS)  
Enterprise Information Security Office (EISO)  
Information Classification Training Transcript**

department or a unit which is more amenable to do things, which is more amenable to do new things.

Start with them, show your success in that and then, roll it out to 4 or 5 other units, which are where you feel there will be more success.

Once you have it in 4 or 5 units then its own weight will carry it across the whole institution because management will realize the importance of this.

Because remember, everybody knows security is important. You cannot have security without knowing what the value of the information you have is and how you need to protect it.

This really is the foundational element of your information security practice in the organization.

You need to find out what you have, what its value is so that you can figure out how to protect it and to what level you need to protect it.

Given that this is a foundational element, that this is you putting your own house in order, figuring out what you need to protect and how.

This makes a foundational element and that's why we have spent so much time not only giving you a Policy and Standard, but also creating a process behind it so that rather than just dumping something on you, we facilitate it, make it easier for you all to implement it.

And having said that, this is my concluding slide, this is number 5 like I promised.

As you know, the whole idea behind this was to make sure that you're not here to learn classification, but to work with it.

What you have here is...you have what to do and how to do it.

The how to do is in the Manual, what to do is in the Policy.

And you need to use the templates that are provided to facilitate your thinking.

Again, one last point before I let you guys go is remember the spreadsheets, the templates, the

Manual, they are not doing the thinking for you.

It's your own thinking. You have to do the decisions. You have to make the decisions. You have to analyze the risk. You have to figure out whether you want to buy the hamburger or not.

This is not going to tell you.

So that's the bottom line.

This is basically a process which is telling you how to think and how to go about making rational decisions about the value of information in your organization.

Thank you all very much.

The class is done.

*Music*

Disclaimer: The opinions expressed in this transcript by the instructor do not necessarily represent the opinions of ITS.