# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- How do you put a new security policy in place at a large organisation - can you just email and say 'we're doing it this way now?'

- How do criminal record checks differ internationally?

- I read that the Risk Register should be confidential - doesn't that make it useless?

- How do corrective actions during incident management differ from risk treatments?

- How can data breaches alter public perceptions of organizational ethics?

- How does pseudonymization differ from anonymization under GDPR?

- Why do we separate into the five phases of incident management?

- Is 'Risk Appetite' the same as 'Risk Culture'

- How does security management work for a computer games company?

- How can organizations use GDPR principles to build trust with customers?

- Have you ever been scammed?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- How does security management work for a computer games company?

- Can I pass an audit by putting nothing on the statement of applicability?

- Is a statement of applicability public?

- Tiger kidnappings seem really interesting - do you have any thoughts?

- What's the most important job of an Incident Response Team (IRT)?

- In lots of the case studies a company calls in external consultants - is there a rule for when you do that?

- What is the role of risk assessment in disaster recovery planning?

- At what point in a security incident should you tell the police??

- I heard some guy say that you could use NIST controls for an ISO27001 audit - is that okay?

- What are the implications of the right to be forgotten in modern business?

- How do systemic biases affect diversity in cybersecurity careers?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- I heard some guy say that you could use NIST controls for an ISO27001 audit - is that okay?

- Why do we separate into the five phases of incident management?

- Can I pass an audit by putting nothing on the statement of applicability?

- Given that equipment is really cheap compared to the cost of employees, why is the return of assets important when an employee leaves?

- Surely many policies are irrelevant if people have work email on their phones?

- How do systemic biases affect diversity in cybersecurity careers?

- What's the difference between Risk Management and Enterprise Risk Management?

- At what point in a security incident should you tell the police??

- How do organizations balance trust with thorough screening processes?

- I read that the Risk Register should be confidential - doesn't that make it useless?

- Is 'Risk Appetite' the same as 'Risk Culture'

# IY3501: Question and Answer Lecture

Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- What's the difference between Risk Management and Enterprise Risk Management?

- I read that the Risk Register should be confidential - doesn't that make it useless?

- How do organizations determine the scope of their disaster recovery plans?

- Can I pass an audit by putting nothing on the statement of applicability?

- What is the difference between data controllers and data processors?

- What's the most important job of an Incident Response Team (IRT)?

- Surely many policies are irrelevant if people have work email on their phones?

- Have you ever been scammed?

- How can data breaches alter public perceptions of organizational ethics?

- Is a statement of applicability public?

- Should we talk about stakeholder communication in incident management? It seems important...

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- How does security management work for a military unit?

- How do criminal record checks differ internationally?

- Say that I write a security policy and an employee ignores it and there is a breach - can I be blamed?

- In lots of the case studies a company calls in external consultants - is there a rule for when you do that?

- How does security management work for a computer games company?

- Is a statement of applicability public?

- Should we talk about stakeholder communication in incident management? It seems important...

- Why is training staff to recognize incidents a top priority?

- What are the implications of the right to be forgotten in modern business?

- Why do we separate into the five phases of incident management?

- How can organizations use GDPR principles to build trust with customers?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- Can I pass an audit by putting nothing on the statement of applicability?

- How do organizations balance trust with thorough screening processes?

- How does security management work for a computer games company?

- Is a statement of applicability public?

- How do you put a new security policy in place at a large organisation - can you just email and say 'we're doing it this way now?'

- How do phishing simulations contribute to employee training?

- How do systemic biases affect diversity in cybersecurity careers?

- What's the most important job of an Incident Response Team (IRT)?

- Why is the 'sliding scale' of spam relevance a key concern in marketing ethics?

- How does pseudonymization differ from anonymization under GDPR?

- Why do we separate into the five phases of incident management?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- Say that I write a security policy and an employee ignores it and there is a breach - can I be blamed?

- How does pseudonymization differ from anonymization under GDPR?

- I read that the Risk Register should be confidential - doesn't that make it useless?

- Why is the 'sliding scale' of spam relevance a key concern in marketing ethics?

- I heard some guy say that you could use NIST controls for an ISO27001 audit - is that okay?

- In lots of the case studies a company calls in external consultants - is there a rule for when you do that?

- What's the difference between Risk Management and Enterprise Risk Management?

- Is a statement of applicability public?

- Why do we separate into the five phases of incident management?

- Can I pass an audit by putting nothing on the statement of applicability?

- How does security management work for a military unit?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- Why is the 'sliding scale' of spam relevance a key concern in marketing ethics?

- How does security management work for a military unit?

- How does security management work for a computer games company?

- Should we talk about stakeholder communication in incident management? It seems important...

- It feels like all of the ransomware stuff is solved by just 'having a backup' do so many companies really just not back stuff up?

- Say that I write a security policy and an employee ignores it and there is a breach - can I be blamed?

- I read that the Risk Register should be confidential - doesn't that make it useless?

- Is 'Risk Appetite' the same as 'Risk Culture'

- What's the difference between Risk Management and Enterprise Risk Management?

- How do you put a new security policy in place at a large organisation - can you just email and say 'we're doing it this way now?'

- How can data breaches alter public perceptions of organizational ethics?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- Why might attackers exploit vulnerabilities during disaster recovery?

- Why is training staff to recognize incidents a top priority?

- I heard some guy say that you could use NIST controls for an ISO27001 audit - is that okay?

- Why is the 'sliding scale' of spam relevance a key concern in marketing ethics?

- How does security management work for a military unit?

- How do organizations balance trust with thorough screening processes?

- How can organizations use GDPR principles to build trust with customers?

- Is 'Risk Appetite' the same as 'Risk Culture'

- How do criminal record checks differ internationally?

- Say that I write a security policy and an employee ignores it and there is a breach - can I be blamed?

- At what point in a security incident should you tell the police??

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- How does security management work for a military unit?

- What's the most important job of an Incident Response Team (IRT)?

- What is the role of risk assessment in disaster recovery planning?

- How do organizations determine the scope of their disaster recovery plans?

- What are the implications of the right to be forgotten in modern business?

- Surely many policies are irrelevant if people have work email on their phones?

- It feels like all of the ransomware stuff is solved by just 'having a backup' do so many companies really just not back stuff up?

- How does pseudonymization differ from anonymization under GDPR?

- Is 'Risk Appetite' the same as 'Risk Culture'

- What is the difference between data controllers and data processors?

- How does security management work for a computer games company?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- How do you put a new security policy in place at a large organisation - can you just email and say 'we're doing it this way now?'

- I heard some guy say that you could use NIST controls for an ISO27001 audit - is that okay?

- How can organizations use GDPR principles to build trust with customers?

- How do corrective actions during incident management differ from risk treatments?

- Can I pass an audit by putting nothing on the statement of applicability?

- Is 'Risk Appetite' the same as 'Risk Culture'

- Why do we separate into the five phases of incident management?

- What's the most important job of an Incident Response Team (IRT)?

- What is the difference between data controllers and data processors?

- It feels like all of the ransomware stuff is solved by just 'having a backup' do so many companies really just not back stuff up?

- What is the role of risk assessment in disaster recovery planning?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- Should we talk about stakeholder communication in incident management? It seems important...

- Tiger kidnappings seem really interesting - do you have any thoughts?

- What are the implications of the right to be forgotten in modern business?

- How do systemic biases affect diversity in cybersecurity careers?

- How can organizations use GDPR principles to build trust with customers?

- What is the difference between data controllers and data processors?

- Why is training staff to recognize incidents a top priority?

- Why do we separate into the five phases of incident management?

- Given that equipment is really cheap compared to the cost of employees, why is the return of assets important when an employee leaves?

- Is 'Risk Appetite' the same as 'Risk Culture'

- Surely many policies are irrelevant if people have work email on their phones?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- In lots of the case studies a company calls in external consultants - is there a rule for when you do that?

- I read that the Risk Register should be confidential - doesn't that make it useless?

- What is the difference between data controllers and data processors?

- Why do we separate into the five phases of incident management?

- How do organizations determine the scope of their disaster recovery plans?

- How does security management work for a computer games company?

- Can I pass an audit by putting nothing on the statement of applicability?

- Have you ever been scammed?

- Tiger kidnappings seem really interesting - do you have any thoughts?

- How does pseudonymization differ from anonymization under GDPR?

- How do systemic biases affect diversity in cybersecurity careers?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- How do phishing simulations contribute to employee training?

- Why is the 'sliding scale' of spam relevance a key concern in marketing ethics?

- I heard some guy say that you could use NIST controls for an ISO27001 audit - is that okay?

- Is a statement of applicability public?

- What's the most important job of an Incident Response Team (IRT)?

- Say that I write a security policy and an employee ignores it and there is a breach - can I be blamed?

- How can organizations use GDPR principles to build trust with customers?

- How do organizations determine the scope of their disaster recovery plans?

- How does security management work for a military unit?

- What is the difference between data controllers and data processors?

- Given that equipment is really cheap compared to the cost of employees, why is the return of assets important when an employee leaves?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- What are the implications of the right to be forgotten in modern business?

- Why might attackers exploit vulnerabilities during disaster recovery?

- How do organizations balance trust with thorough screening processes?

- How can data breaches alter public perceptions of organizational ethics?

- How do corrective actions during incident management differ from risk treatments?

- How does security management work for a military unit?

- What is the role of risk assessment in disaster recovery planning?

- In lots of the case studies a company calls in external consultants - is there a rule for when you do that?

- Can I pass an audit by putting nothing on the statement of applicability?

- What's the most important job of an Incident Response Team (IRT)?

- How do phishing simulations contribute to employee training?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- What is the difference between data controllers and data processors?

- How do corrective actions during incident management differ from risk treatments?

- How does security management work for a military unit?

- How do criminal record checks differ internationally?

- Should we talk about stakeholder communication in incident management? It seems important...

- Are there any companies that shouldn't have an ISMS?

- I heard some guy say that you could use NIST controls for an ISO27001 audit - is that okay?

- What is the role of risk assessment in disaster recovery planning?

- Tiger kidnappings seem really interesting - do you have any thoughts?

- How do you put a new security policy in place at a large organisation - can you just email and say 'we're doing it this way now?'

- How do phishing simulations contribute to employee training?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- How can organizations use GDPR principles to build trust with customers?

- Should we talk about stakeholder communication in incident management? It seems important...

- Can I pass an audit by putting nothing on the statement of applicability?

- I heard some guy say that you could use NIST controls for an ISO27001 audit - is that okay?

- What is the difference between data controllers and data processors?

- How do criminal record checks differ internationally?

- What are the implications of the right to be forgotten in modern business?

- Can we learn more about Cyberwar in the context of places like the Ukraine?

- Why is training staff to recognize incidents a top priority?

- Why might attackers exploit vulnerabilities during disaster recovery?

- Are there any companies that shouldn't have an ISMS?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- Surely many policies are irrelevant if people have work email on their phones?

- Should we talk about stakeholder communication in incident management? It seems important...

- How do you put a new security policy in place at a large organisation - can you just email and say 'we're doing it this way now?'

- How does pseudonymization differ from anonymization under GDPR?

- Have you ever been scammed?

- What is the role of risk assessment in disaster recovery planning?

- Given that equipment is really cheap compared to the cost of employees, why is the return of assets important when an employee leaves?

- How do systemic biases affect diversity in cybersecurity careers?

- Tiger kidnappings seem really interesting - do you have any thoughts?

- Can we learn more about Cyberwar in the context of places like the Ukraine?

- Is a statement of applicability public?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- What are the implications of the right to be forgotten in modern business?

- Can we learn more about Cyberwar in the context of places like the Ukraine?

- How do criminal record checks differ internationally?

- How do you put a new security policy in place at a large organisation - can you just email and say 'we're doing it this way now?'

- What's the difference between Risk Management and Enterprise Risk Management?

- How does security management work for a computer games company?

- How do organizations determine the scope of their disaster recovery plans?

- Is 'Risk Appetite' the same as 'Risk Culture'

- How do organizations balance trust with thorough screening processes?

- What is the role of risk assessment in disaster recovery planning?

- Why might attackers exploit vulnerabilities during disaster recovery?

# IY3501: Question and Answer Lecture

Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- How do criminal record checks differ internationally?

- How do corrective actions during incident management differ from risk treatments?

- Have you ever been scammed?

- Given that equipment is really cheap compared to the cost of employees, why is the return of assets important when an employee leaves?

- How do organizations determine the scope of their disaster recovery plans?

- Is 'Risk Appetite' the same as 'Risk Culture'

- Can I pass an audit by putting nothing on the statement of applicability?

- How do phishing simulations contribute to employee training?

- How does pseudonymization differ from anonymization under GDPR?

- How does security management work for a computer games company?

- How do you put a new security policy in place at a large organisation - can you just email and say 'we're doing it this way now?'

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- How does security management work for a military unit?

- Surely many policies are irrelevant if people have work email on their phones?

- Why might attackers exploit vulnerabilities during disaster recovery?

- Are there any companies that shouldn't have an ISMS?

- What is the role of risk assessment in disaster recovery planning?

- How do organizations determine the scope of their disaster recovery plans?

- What are the implications of the right to be forgotten in modern business?

- What's the most important job of an Incident Response Team (IRT)?

- How does security management work for a computer games company?

- Given that equipment is really cheap compared to the cost of employees, why is the return of assets important when an employee leaves?

- How do you put a new security policy in place at a large organisation - can you just email and say 'we're doing it this way now?'

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- Why might attackers exploit vulnerabilities during disaster recovery?

- How do criminal record checks differ internationally?

- How do phishing simulations contribute to employee training?

- Why is training staff to recognize incidents a top priority?

- I heard some guy say that you could use NIST controls for an ISO27001 audit - is that okay?

- What's the most important job of an Incident Response Team (IRT)?

- Should we talk about stakeholder communication in incident management? It seems important...

- Have you ever been scammed?

- Surely many policies are irrelevant if people have work email on their phones?

- It feels like all of the ransomware stuff is solved by just 'having a backup' do so many companies really just not back stuff up?

- What are the implications of the right to be forgotten in modern business?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- How do systemic biases affect diversity in cybersecurity careers?

- Given that equipment is really cheap compared to the cost of employees, why is the return of assets important when an employee leaves?

- How can data breaches alter public perceptions of organizational ethics?

- Tiger kidnappings seem really interesting - do you have any thoughts?

- Why might attackers exploit vulnerabilities during disaster recovery?

- I read that the Risk Register should be confidential - doesn't that make it useless?

- Should we talk about stakeholder communication in incident management? It seems important...

- How do phishing simulations contribute to employee training?

- What is the difference between data controllers and data processors?

- At what point in a security incident should you tell the police??

- How do you put a new security policy in place at a large organisation - can you just email and say 'we're doing it this way now?'

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- How do systemic biases affect diversity in cybersecurity careers?

- How do phishing simulations contribute to employee training?

- What's the difference between Risk Management and Enterprise Risk Management?

- Say that I write a security policy and an employee ignores it and there is a breach - can I be blamed?

- What is the difference between data controllers and data processors?

- How does security management work for a military unit?

- Is 'Risk Appetite' the same as 'Risk Culture'

- Why might attackers exploit vulnerabilities during disaster recovery?

- How can data breaches alter public perceptions of organizational ethics?

- How do organizations balance trust with thorough screening processes?

- Why is training staff to recognize incidents a top priority?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- How do phishing simulations contribute to employee training?

- I read that the Risk Register should be confidential - doesn't that make it useless?

- How do organizations balance trust with thorough screening processes?

- How does security management work for a computer games company?

- How do corrective actions during incident management differ from risk treatments?

- Why do we separate into the five phases of incident management?

- Are there any companies that shouldn't have an ISMS?

- Why is training staff to recognize incidents a top priority?

- How can data breaches alter public perceptions of organizational ethics?

- What are the implications of the right to be forgotten in modern business?

- It feels like all of the ransomware stuff is solved by just 'having a backup' do so many companies really just not back stuff up?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- What is the difference between data controllers and data processors?

- Why is the 'sliding scale' of spam relevance a key concern in marketing ethics?

- Say that I write a security policy and an employee ignores it and there is a breach - can I be blamed?

- What is the role of risk assessment in disaster recovery planning?

- Should we talk about stakeholder communication in incident management? It seems important...

- What's the difference between Risk Management and Enterprise Risk Management?

- I heard some guy say that you could use NIST controls for an ISO27001 audit - is that okay?

- How do phishing simulations contribute to employee training?

- Why is training staff to recognize incidents a top priority?

- How do organizations determine the scope of their disaster recovery plans?

- Can I pass an audit by putting nothing on the statement of applicability?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- How do organizations determine the scope of their disaster recovery plans?

- Should we talk about stakeholder communication in incident management? It seems important...

- Is a statement of applicability public?

- I read that the Risk Register should be confidential - doesn't that make it useless?

- Why might attackers exploit vulnerabilities during disaster recovery?

- Is 'Risk Appetite' the same as 'Risk Culture'

- It feels like all of the ransomware stuff is solved by just 'having a backup' do so many companies really just not back stuff up?

- How do systemic biases affect diversity in cybersecurity careers?

- Surely many policies are irrelevant if people have work email on their phones?

- In lots of the case studies a company calls in external consultants - is there a rule for when you do that?

- How do you put a new security policy in place at a large organisation - can you just email and say 'we're doing it this way now?'

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- Should we talk about stakeholder communication in incident management? It seems important...

- What is the difference between data controllers and data processors?

- In lots of the case studies a company calls in external consultants - is there a rule for when you do that?

- What's the difference between Risk Management and Enterprise Risk Management?

- What is the role of risk assessment in disaster recovery planning?

- How do criminal record checks differ internationally?

- How can data breaches alter public perceptions of organizational ethics?

- Are there any companies that shouldn't have an ISMS?

- At what point in a security incident should you tell the police??

- What's the most important job of an Incident Response Team (IRT)?

- How can organizations use GDPR principles to build trust with customers?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- Why is training staff to recognize incidents a top priority?

- Surely many policies are irrelevant if people have work email on their phones?

- What is the role of risk assessment in disaster recovery planning?

- How do phishing simulations contribute to employee training?

- At what point in a security incident should you tell the police??

- Say that I write a security policy and an employee ignores it and there is a breach - can I be blamed?

- Can I pass an audit by putting nothing on the statement of applicability?

- How does pseudonymization differ from anonymization under GDPR?

- How do systemic biases affect diversity in cybersecurity careers?

- Given that equipment is really cheap compared to the cost of employees, why is the return of assets important when an employee leaves?

- How do criminal record checks differ internationally?

# IY3501: Question and Answer Lecture

## Joe Reddington

## Introduction

We're going to do another question and answer session today. This time I'd like to focus on the second half of the course but I am happy to take questions from any section of the course, or from any of the recommended readings.

If you are short of questions, then I suggest:

- looking through previous slides and seeing if there are any parts you don't feel like you 'get';

- looking through past papers and seeing if there are any questions you don't feel like you could answer;

- asking some of the starter questions.

You can ask questions by putting up your hand or with Teams.

Particularly interesting questions will be added to the database and may be starter questions for next year.

## Starter Questions

Here are some randomly generated questions for you to try asking:

- Why is the 'sliding scale' of spam relevance a key concern in marketing ethics?

- Why do we separate into the five phases of incident management?

- I read that the Risk Register should be confidential - doesn't that make it useless?

- How does pseudonymization differ from anonymization under GDPR?

- What is the role of risk assessment in disaster recovery planning?

- Say that I write a security policy and an employee ignores it and there is a breach - can I be blamed?

- How do systemic biases affect diversity in cybersecurity careers?

- Can I pass an audit by putting nothing on the statement of applicability?

- I heard some guy say that you could use NIST controls for an ISO27001 audit - is that okay?

- How do organizations determine the scope of their disaster recovery plans?

- How do corrective actions during incident management differ from risk treatments?