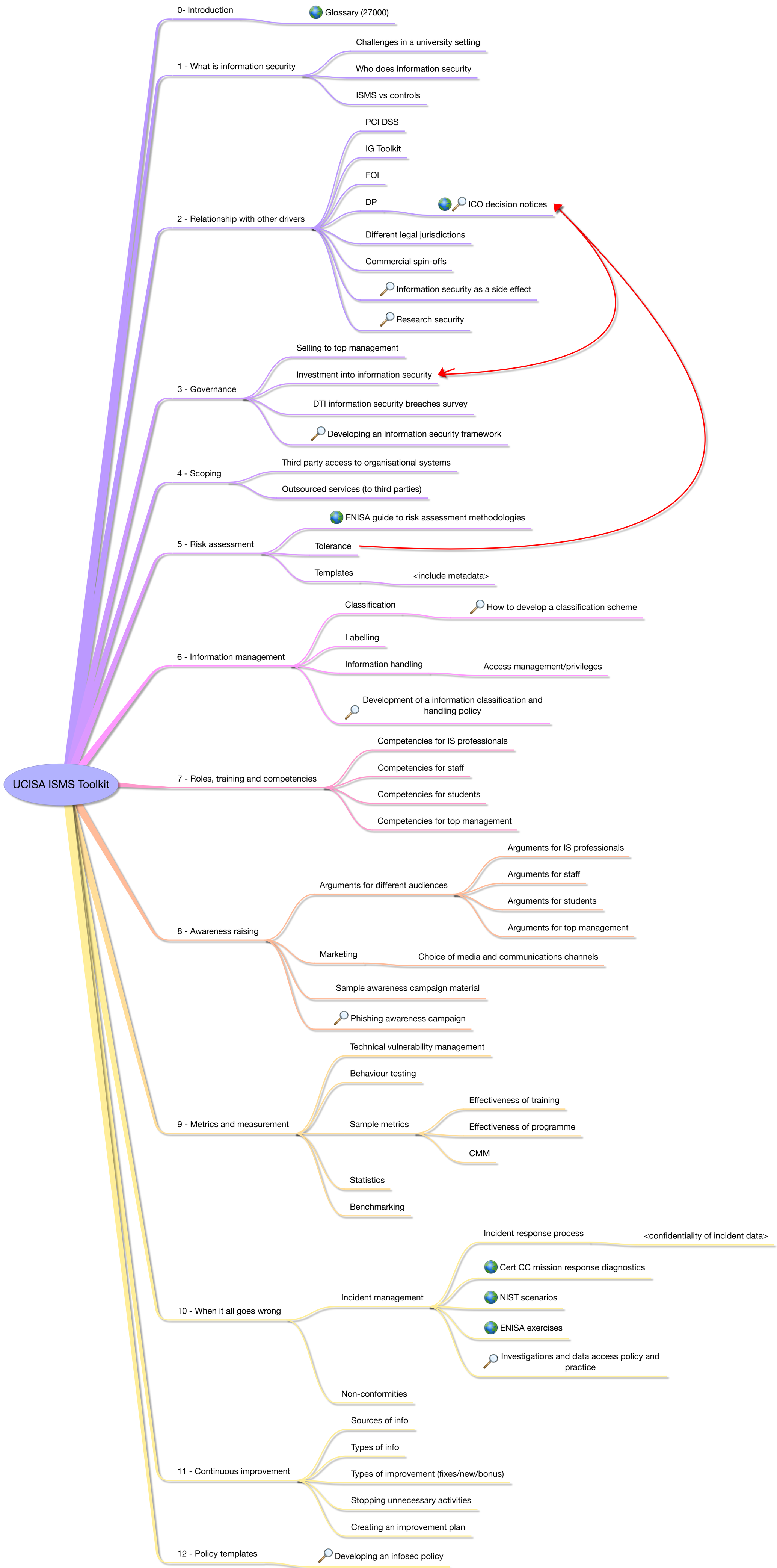
UCISA ISMS Toolkit
0- Introduction
Glossary (27000)
1 - What is information security
Challenges in a university setting
Who does information security
ISMS vs controls
2 - Relationship with other drivers
PCI DSS
IG Toolkit
FOI
DP
ICO decision notices
Different legal jurisdictions
Commercial spin-offs
Information security as a side effect
Research security
3 - Governance
Selling to top management
Investment into information security
DTI information security breaches survey
Developing an information security framework
4 - Scoping
Third party access to organisational systems
Outsourced services (to third parties)
5 - Risk assessment
ENISA guide to risk assessment methodologies
Tolerance
Templates
<include metadata>
6 - Information management
Classification
How to develop a classification scheme
Labelling
Information handling
Access management/privileges
Development of a information classification and handling policy
7 - Roles, training and competencies
Competencies for IS professionals
Competencies for staff
Competencies for students
Competencies for top management
8 - Awareness raising
Arguments for different audiences
Arguments for IS professionals
Arguments for staff
Arguments for students
Arguments for top management
Marketing
Choice of media and communications channels
Sample awareness campaign material
Phishing awareness campaign
9 - Metrics and measurement
Technical vulnerability management
Behaviour testing
Sample metrics
Effectiveness of training
Effectiveness of programme
CMM
Statistics
Benchmarking
10 - When it all goes wrong
Incident management
Incident response process
<confidentiality of incident data>
Cert CC mission response diagnostics
NIST scenarios
ENISA exercises
Investigations and data access policy and practice
Non-conformities
11 - Continuous improvement
Sources of info
Types of info
Types of improvement (fixes/new/bonus)
Stopping unnecessary activities
Creating an improvement plan
12 - Policy templates
Developing an infosec policy