ISO Based Controls Playbook

Development Note

The ISO Based Controls Playbook was developed by Rob Dodson, SCF and is based on the Open Information Security Risk Universe and is therefore considered to be available under the Creative Commons Zero v1.0 Universal License.

Please provide updates to Phil Huggins and the Github repository https://github.com/oracuk/oisru.

Risk Universe – Threat Actors

- Malicious External Actor
  - Cybercriminals
  - Nation States
  - Hacktivist
- Malicious Internal Actor
  - Disgruntled Employee
  - Compromised Vendor
- Non-malicious Actor
  - Internal Accidental
  - Internal Ineffective
  - External

Risk Universe – Vulnerabilities

- People
  - Employees
  - Contractors
  - Third Party Suppliers
- Process
  - Security Activities
  - Security Roles
  - Security Documentation
- Technology
  - Operational Support
  - Security Tools

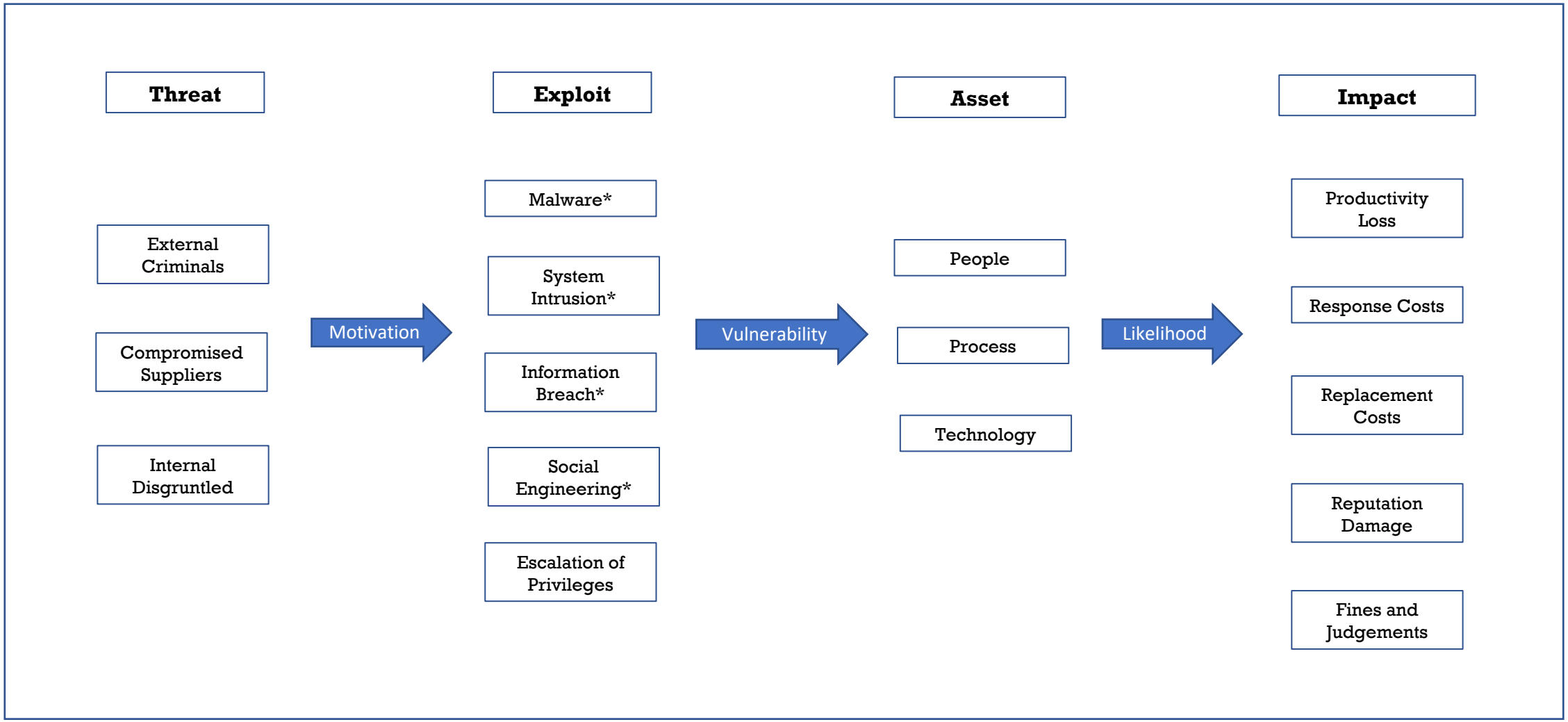
Risk Universe – Exploits

- Malware
  - Ransomware
  - Rootkits
  - Virus
- Service Interruption
  - DDoS
- System Intrusion Breach
  - Cross Site Scripting
- Information Breach
  - Data Theft
  - Supply Chain Attack
  - Escalation of Privileges
- Social Engineering
  - Phishing, Vishing, Smishing
  - Whaling

Risk Universe – Impact

- Productivity Loss
- Response Costs
- Replacement Costs
- Reputation Costs
- Fines and Judgements

Risk Universe



*High level term for a family of risk events. See Bow Tie charts for details.

Controls Explained

Controls presented in this Playbook are either Preventative Controls or Mitigating Controls. These controls are based on the Five Focus Areas outlined in the NIST Cybersecurity Framework (CSF). The Focus Areas have been aligned with other Frameworks. The Focus Areas are:

Identify (Preventative)

Protect (Preventative)

Detect (Mitigating)

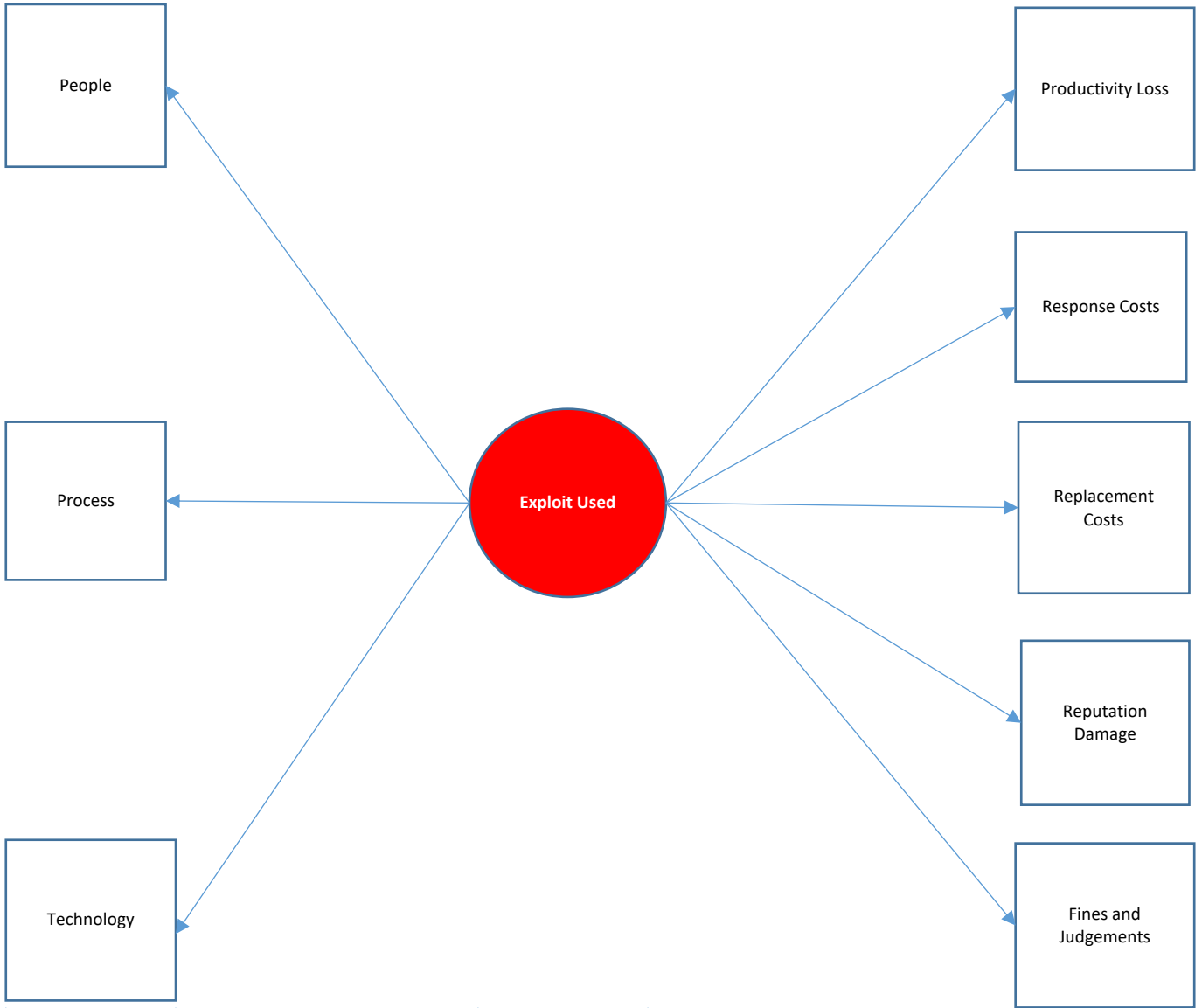
Respond (Mitigating)

Recover (Mitigating)

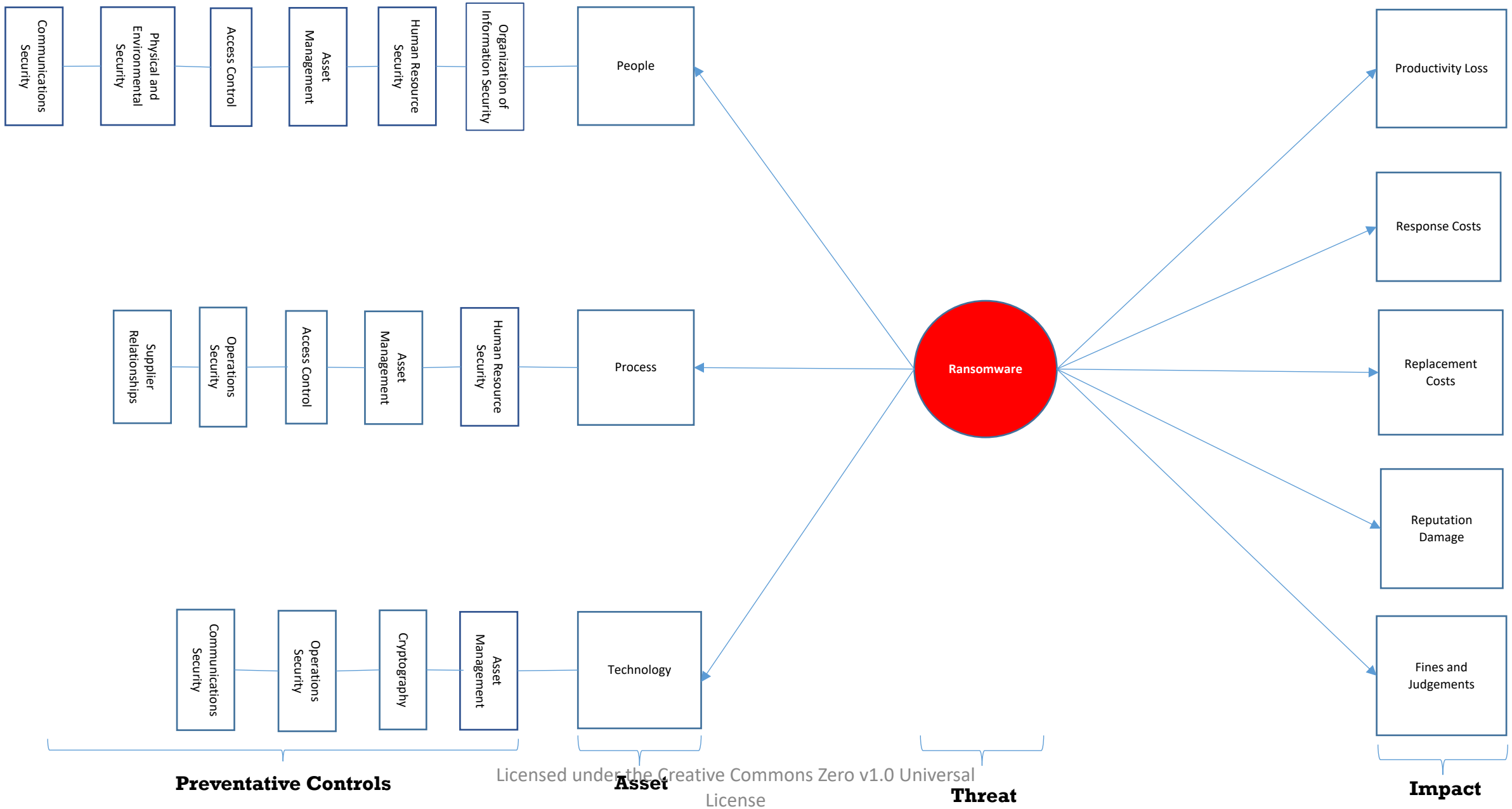
Controls Explained, continued

- The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to people, Process, and technology.
- The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.
- The Detect Function enables timely discovery of cybersecurity events.
- The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.
- The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Threat Action – Threat Actor



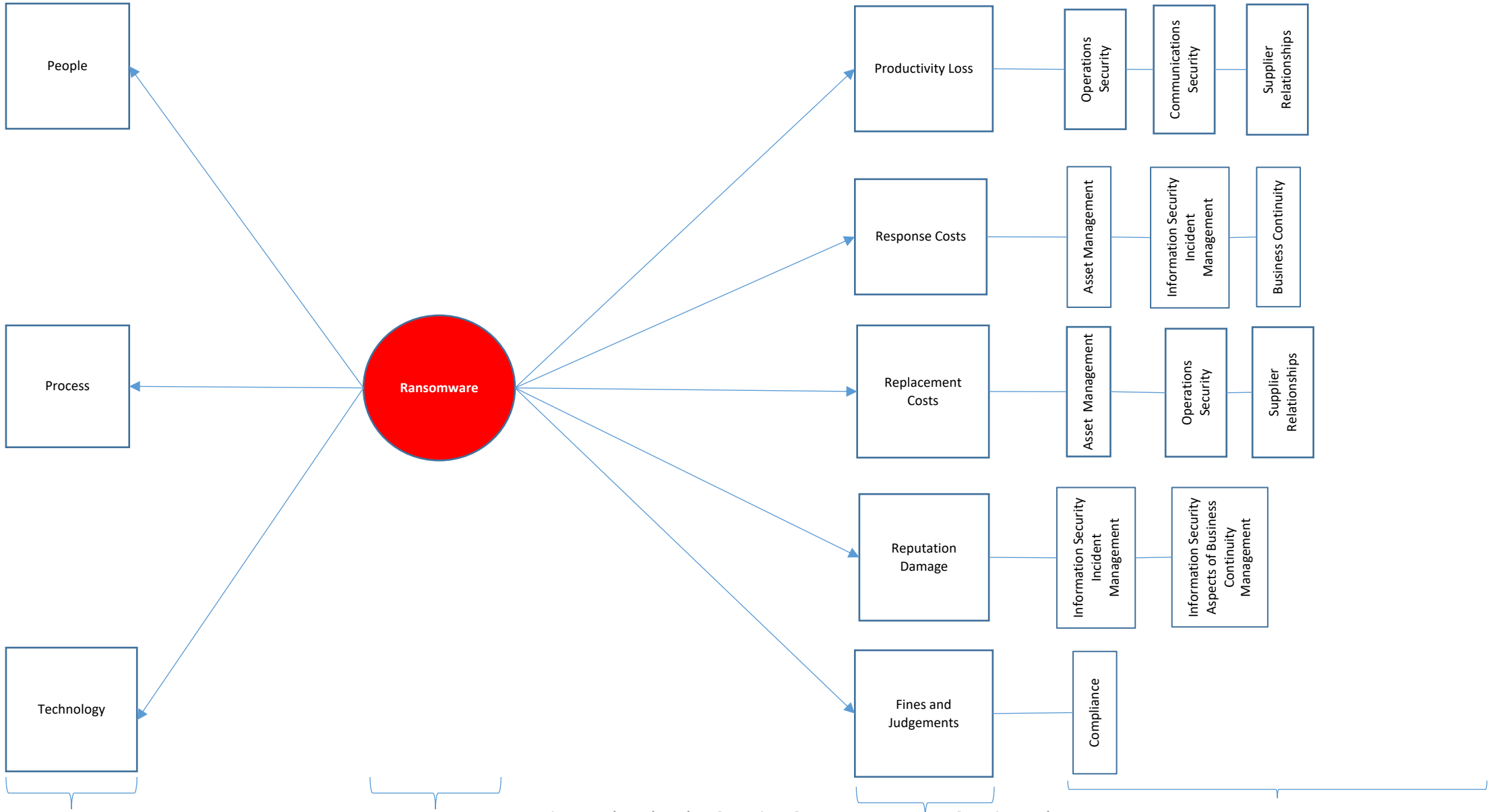
Malware – External Threat Actor (Preventative)



Malware – External Threat Actor (Preventative)

Asset	Organization of Information Security	Human Resource Security	Asset Management	Access Control	Physical and Environmental Security	Communications Security
People	6.1 Internal Organization	7.2.2 Information Security Awareness, Education and Training	8.2 Information Classification	9.1.2 Access to Networks and Network Services	11.2.8 Unattended User Equipment	13.2 Information Transfer
	6.2 Mobile Devices and Teleworking		8.3 Media Handling	9.4.1 Information Access Restriction		
Processes	**Human Resources**	**Asset Management**	**Access Control**	**Operations Security**	**Supplier Relationships**	
	7.2 During Employment	8.1 Responsibility for Assets	9.1.2 Access to Networks and Network Services	12.1 Operational Procedures and Responsibilities	15.1 Information Security in Supplier Relationships	
		8.2 Information Classification	9.4.1 Information Access Restriction			
		8.3 Media Handling				
Technology	**Asset Management**	**Cryptography**	**Operations Security**	**Communications Security**		
	8.3 Media Handling	10.1 Cryptographic Controls	12.3 Backup	13.1 Network Security Management		
			12.4 Logging and Monitoring	13.2 Information Transfer		
			12.6 Technical Vulnerability Management			
			12.7 Information Systems Audit Considerations			

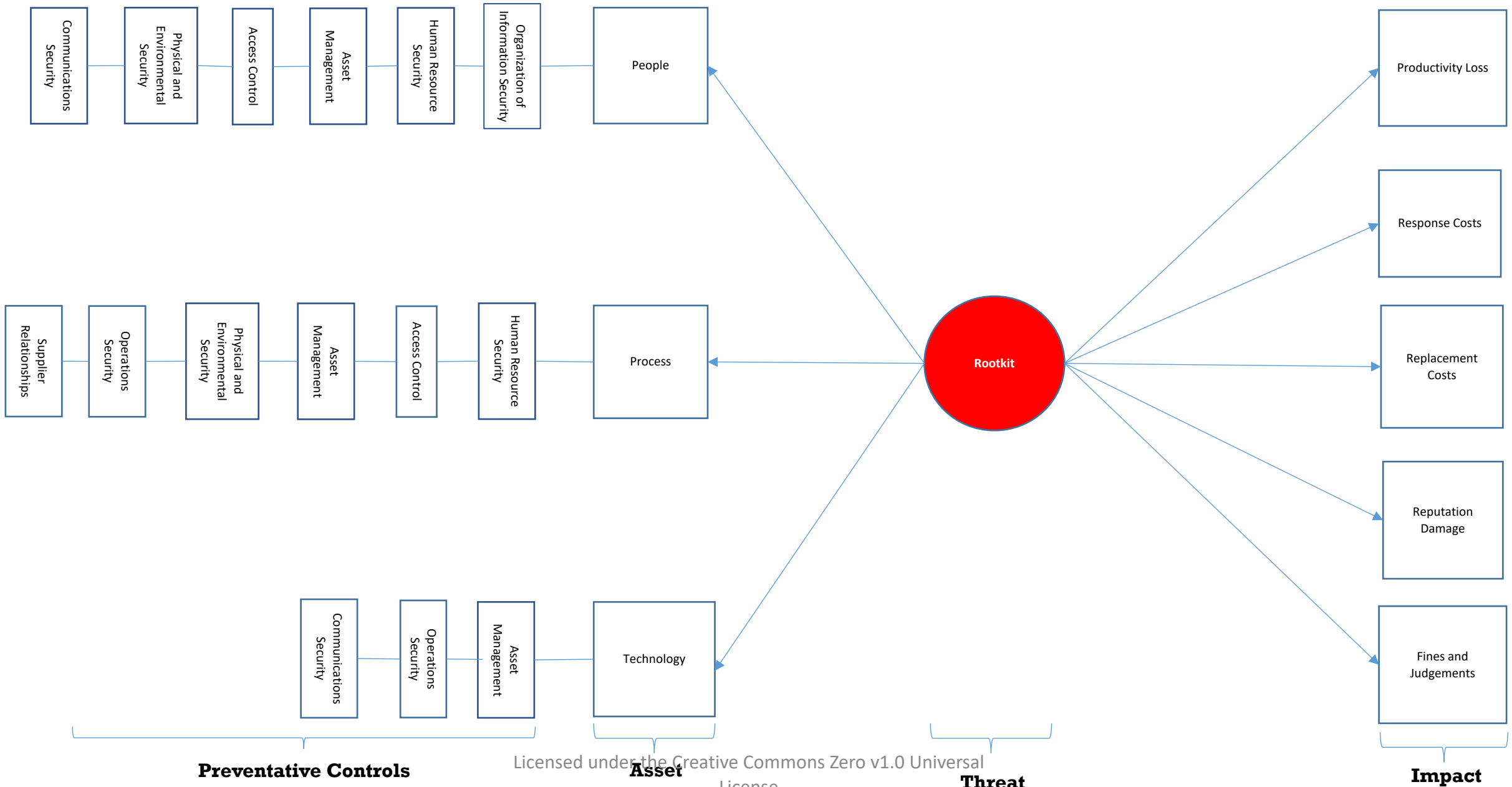
Malware – External Threat Actor (Mitigation)



Malware – External Threat Actor (Mitigation)

Impact	Operations Security	Communications Security	Supplier Relationships
Productivity Loss	12.3.1 Information Backup	13.1 Network Security Management	15.1 Information Security in Supplier Relationships
	12.4 Logging and Monitoring		
Response Costs	**Information Security Incident Management**	**Business Continuity**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Replacement Costs	**Asset Management**	**Operations Security**	**Supplier Relationships**
	8.1 Responsibility for Assets	12.2 Protection from Malware	15.1.2 Addressing Security within Supplier Agreements
		12.3 Backup	15.3 Information and Communication Technology Supply Chain
		12.4 Logging and Monitoring	15.2.1 Monitoring and review of supplier services.
		12.5 Control of Operational Software	15.2.2 Managing Changes to Supplier Services
		12.6 Technical Vulnerability Management	
Reputation Damage	**Information security Incident Management**	**Information Security Aspects of Business Continuity Management**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Fines and Judgement	**Compliance**		
	18.1 Compliance with Legal and Contractual Requirements		
	18.2 Information Security Review		

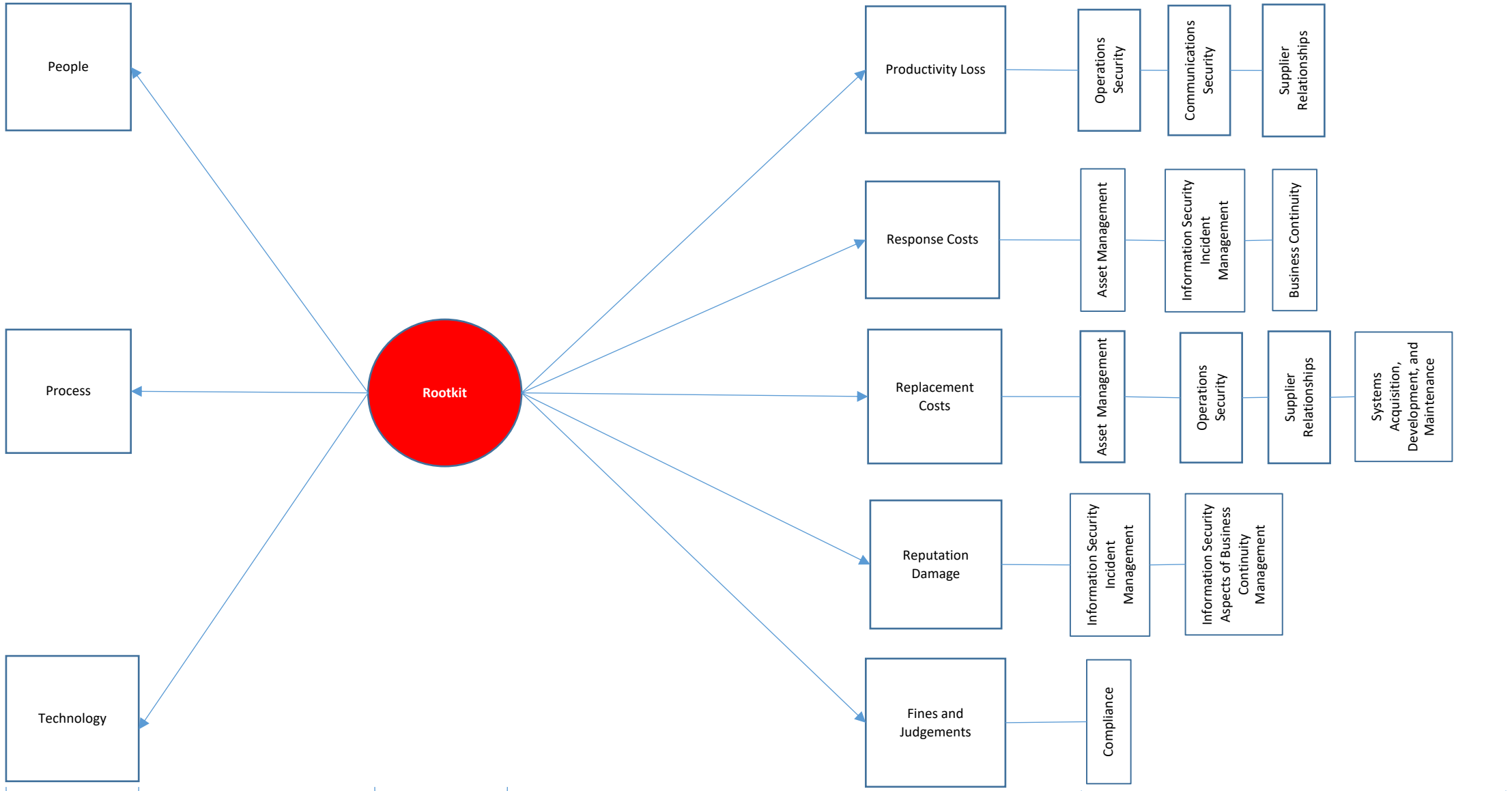
Malware – External Threat Actor (Preventative)



Malware – External Threat Actor (Preventative)

Asset	Organization of Information Security	Human Resource Security	Asset Management	Access Control	Physical and Environmental Security	Communications Security
People	6.1 Internal Organization	7.2.2 Information Security Awareness, Education and Training	8.2 Information Classification	9.1.2 Access to Networks and Network Services	11.2.8 Unattended User Equipment	13.2 Information Transfer
	6.2 Mobile Devices and Teleworking		8.3 Media Handling	9.4.1 Information Access Restriction		
Processes	**Human Resource Security**	**Asset Management**	**Access Control**	**Physical and Environmental Security**	**Operations Security**	**Supplier Relations**
	7.2 During Employment	8.1 Responsibility for Assets	9.1.2 Access to Networks and Network Services	11.1 Secure Area	12.1 Operational Procedures and Responsibilities	15.1 Information Security in Supplier Relationships
		8.2 Information Classification	9.4.1 Information Access Restriction			
		8.3 Media Handling				
Technology	**Asset Management**	**Operations Security**	**Communications Security**			
	8.3 Media Handling	12.3 Backup	13.1 Network Security Management			
		12.4 Logging and Monitoring	13.2 Information Transfer			
		12.6 Technical Vulnerability Management				
		12.7 Information Systems Audit Considerations				

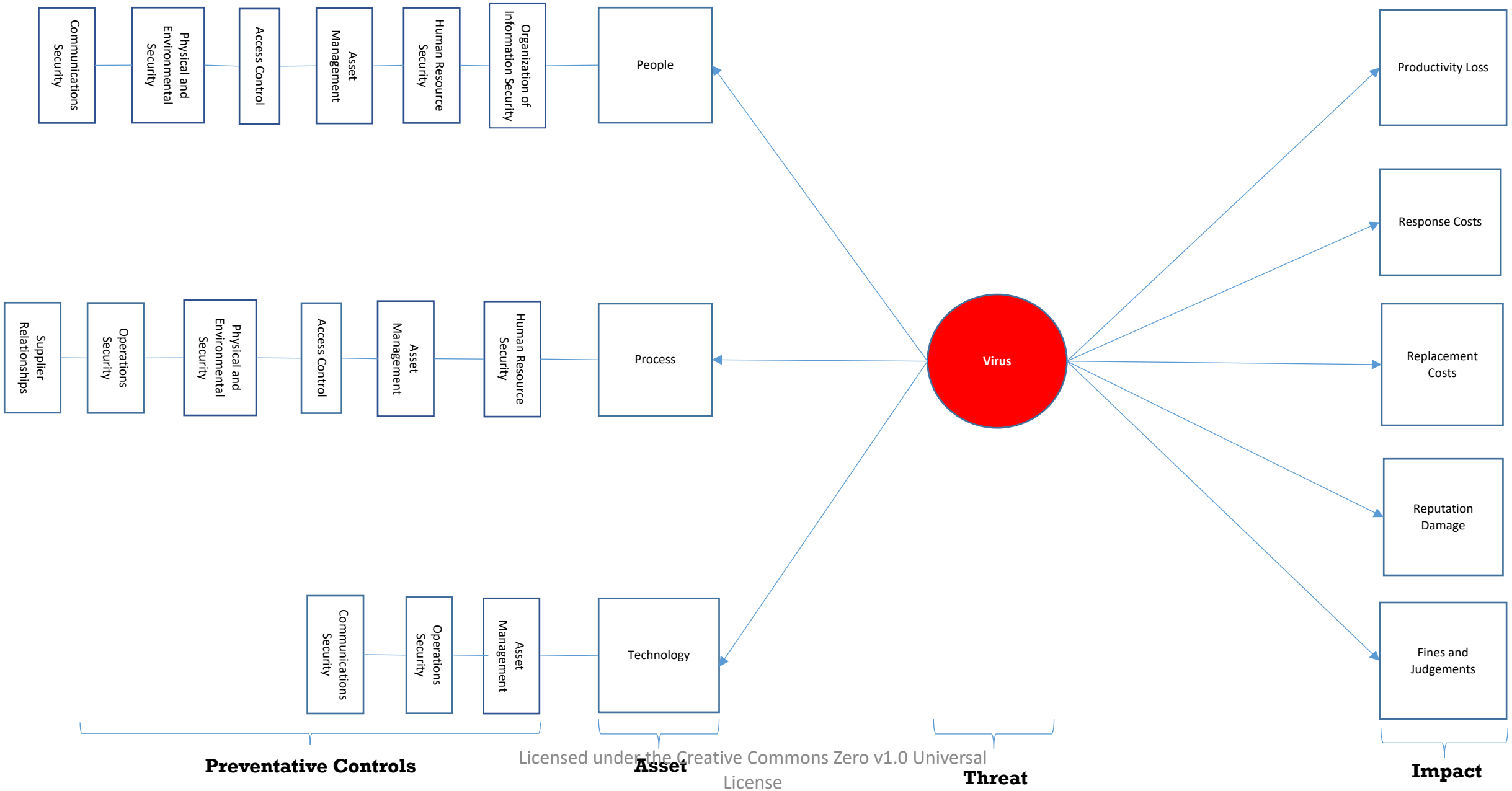
Malware – External Threat Actor (Mitigating)



Malware – External Threat Actor (Mitigating)

Impact	Operations Security	Communications Security	Supplier Relationships
Productivity Loss	12.3.1 Information Backup	13.1 Network Security Management	15.1 Information Security in Supplier Relationships
	12.4 Logging and Monitoring		
Response Costs	**Systems Acquisition, Development, and Maintenance**	**Information Security Incident Management**	**Business Continuity**
	14.1 Security Requirements of Information Systems	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity
			17.2 Redundancies
Replacement Costs	**Asset Management**	**Operations Security**	**Supplier Relationships**
	8.1 Responsibility for Assets	12.2 Protection from Malware	15.1.2 Addressing Security within Supplier Agreements
		12.3 Backup	15.3 Information and Communication Technology Supply Chain
		12.4 Logging and Monitoring	15.2.1 Monitoring and review of supplier services.
		12.5 Control of Operational Software	15.2.2 Managing Changes to Supplier Services
		12.6 Technical Vulnerability Management	
Reputation Damage	**Information security Incident Management**	**Information Security Aspects of Business Continuity Management**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Fines and Judgement	**Compliance**		
	18.1 Compliance with Legal and Contractual Requirements		
	18.2 Information Security Review		

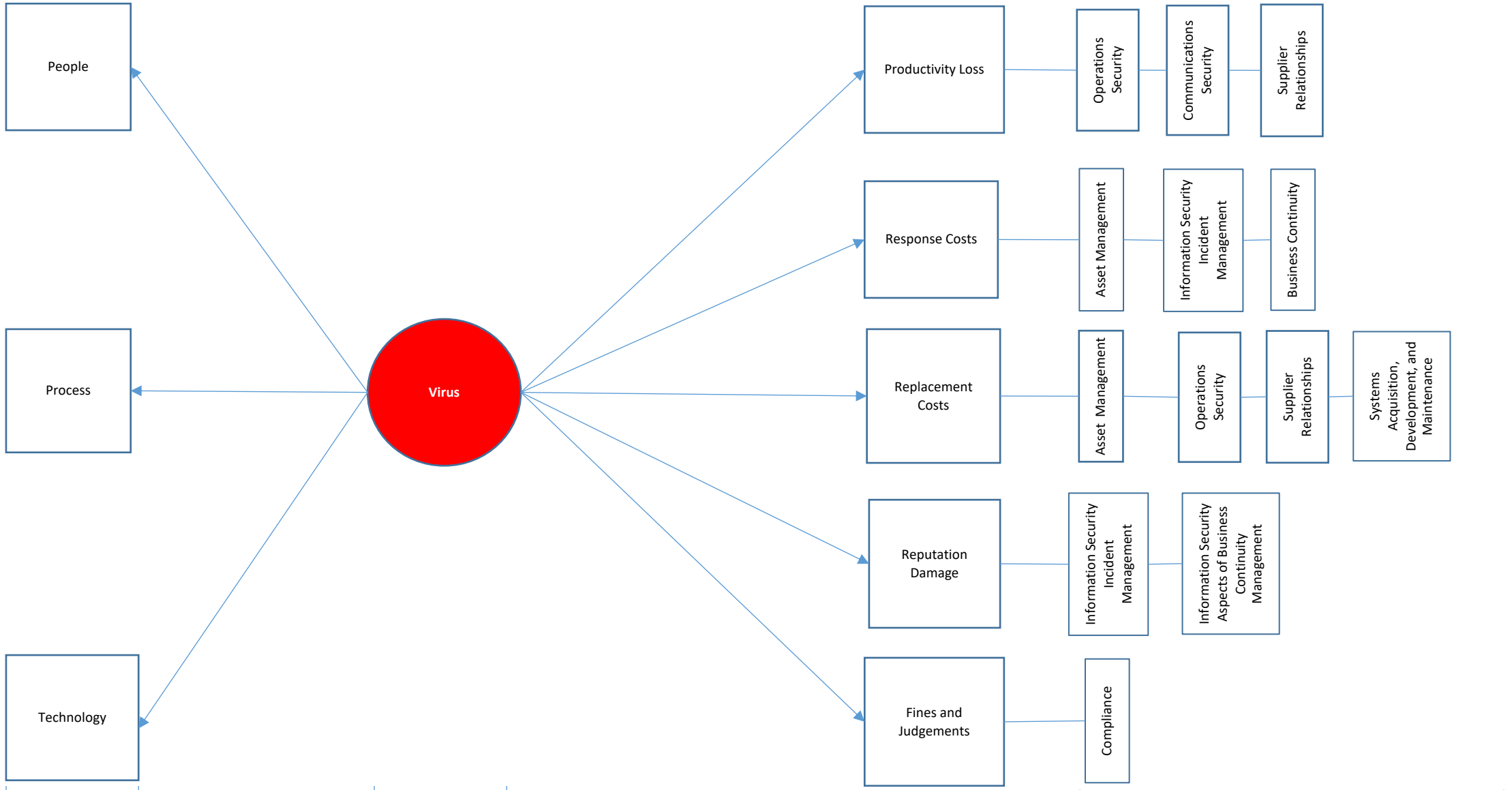
Malware – External Threat Actor (Preventative)



Malware – External Threat Actor (Preventative)

Asset	Organization of Information Security	Human Resource Security	Asset Management	Access Control	Physical and Environmental Security	Communications Security
People	6.1 Internal Organization	7.2.2 Information Security Awareness, Education and Training	8.3 Media Handling	9.1.2 Access to Networks and Network Services	11.2.8 Unattended User Equipment	13.2 Information Transfer
	6.2 Mobile Devices and Teleworking			9.4.1 Information Access Restriction		
Processes	**Human Resource Security**	**Asset Management**	**Access Control**	**Physical and Environmental Security**	**Operations Security**	**Supplier Relations**
	7.2 During Employment	8.3 Media Handling	9.1.2 Access to Networks and Network Services	11.2.8 Unattended User Equipment	12.1 Operational Procedures and Responsibilities	15.1 Information Security in Supplier Relationships
	7.3 Termination and Change of Employment		9.4.1 Information Access Restriction			
Technology	**Asset Management**	**Operations Security**	**Communications Security**			
	8.3 Media Handling	12.3 Backup	13.1 Network Security Management			
		12.4 Logging and Monitoring	13.2 Information Transfer			
		12.6 Technical Vulnerability Management				
		12.7 Information Systems Audit Considerations				

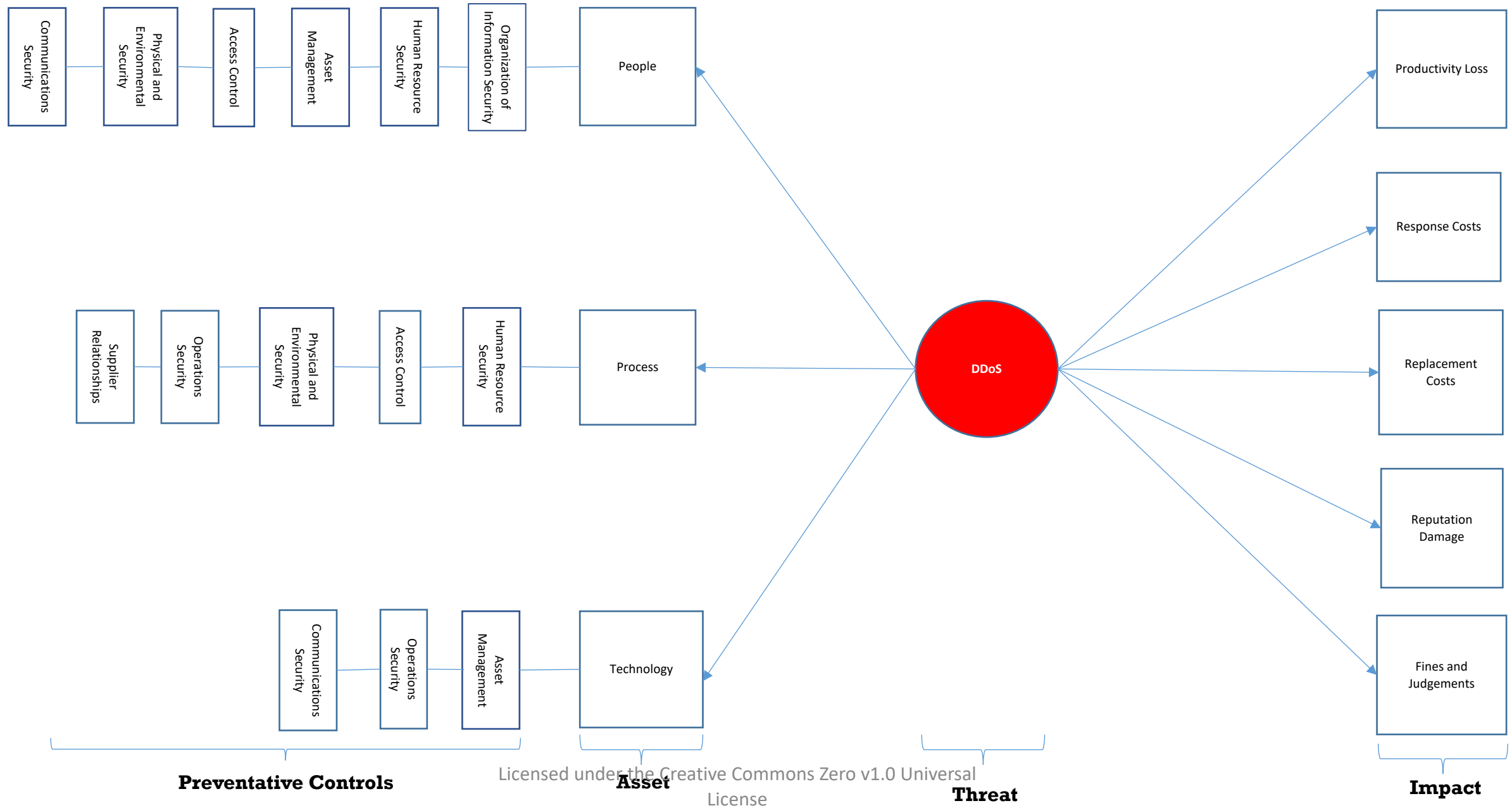
Malware – External Threat Actor (Mitigating)



Malware – External Threat Actor (Mitigating)

Impact	Operations Security	Communications Security	Supplier Relations	
Productivity Loss	12.3.1 Information Backup	13.1 Network Security Management	15.1 Information Security in Supplier Relationships	
	12.4 Logging and Monitoring			
Response Costs	**Information Security Incident Response**	**Business Continuity**		
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity		
		17.2 Redundancies		
Replacement Costs	**Asset Management**	**Operations Security**	**Supplier Relations**	**System Acquisition, Development and**
	8.1 Responsibility for Assets	12.5 Control of Operational Software	15.3 Information and Communication Technology Supply Chain	14.1 Security Requirements of Information Systems
	8.2 Media Handling		15.2.1 Monitoring and review of supplier services.	14.2 Security in Development and
Reputation Damage	**Information Security Incident Response**	**Information Security Aspects of Business Continuity Management**		
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity		
		17.2 Redundancies		
Fines and Judgement	**Compliance**			
	18.1 Compliance with Legal and Contractual Requirements			
	18.2 Information Security Review			

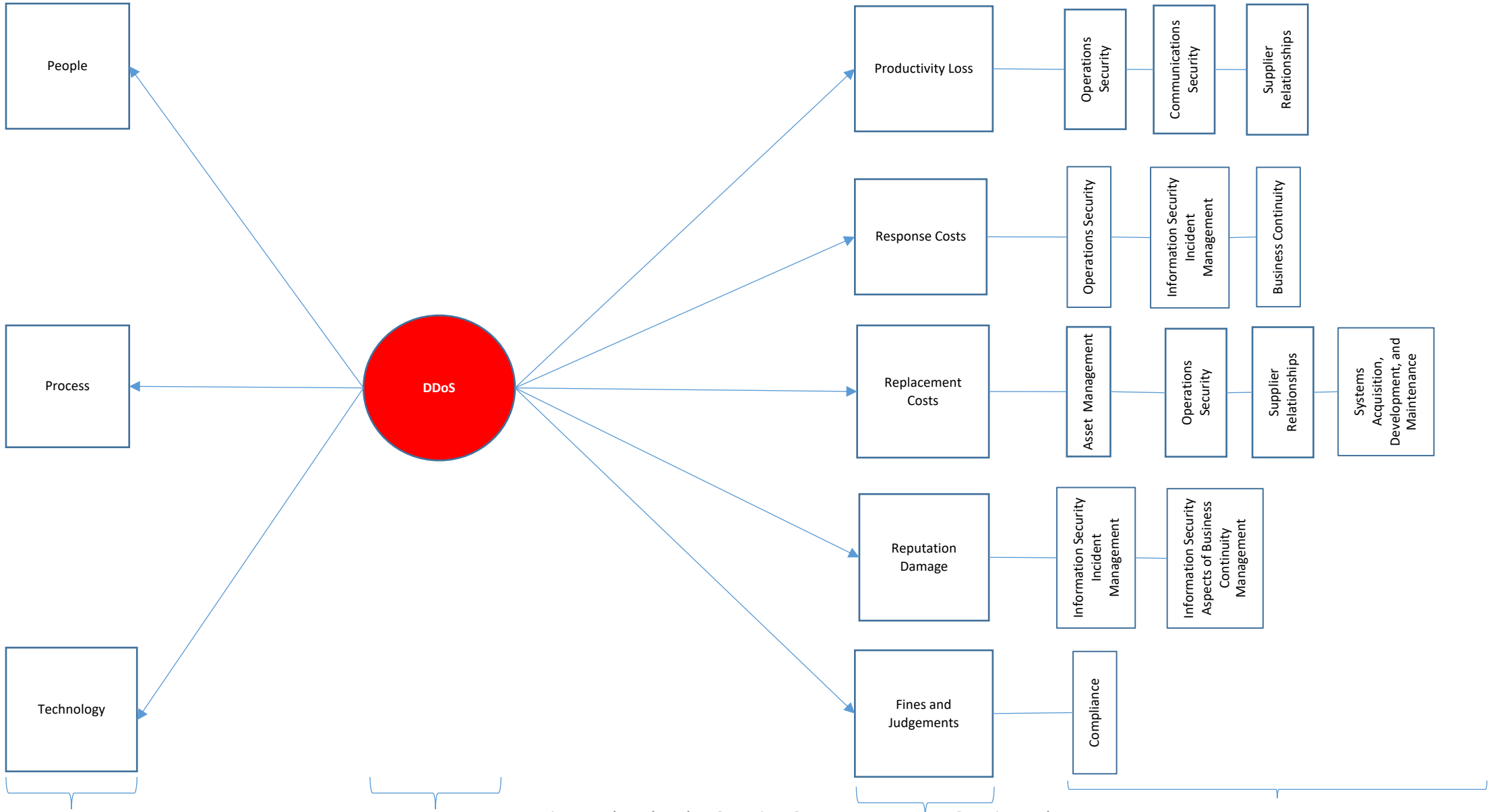
Service Interruption – External Threat Actor (Preventative)



Service Interruption – External Threat Actor (Preventative)

Assets	Organization of Information Security	Human Resource Security	Asset Management	Access Control	Physical and Environmental Security	Communications Security
People	6.1.3 Contact with Authorities	7.2.2 Information Security Awareness, Education and Training	8.3 Media Handling	9.1.2 Access to Networks and Network Services	11.2.8 Unattended User Equipment	13.1 Network Security Management
	6.1.3 Contact with Special Interest Groups					
	6.2 Mobile Devices and Teleworking					
Process	**Human Resources**	**Asset Management**	**Access Control**	**Physical and Environmental Security**	**Operations Security**	**Supplier Relationships**
	7.2.2 Information Security Awareness, Education and Training	8.3 Media Handling	9.1.2 Access to Networks and Network Services	11.2.8 Unattended User Equipment	12.1 Operational Procedures and Responsibilities	15.1 Information Security in Supplier Relationships
Technology	**Asset Management**	**Operations Security**	**Communications Security**			
	8.3 Media Handling	12.3 Backup	13.1 Network Security Management			
		12.4 Logging and Monitoring				
		12.6 Technical Vulnerability Management				

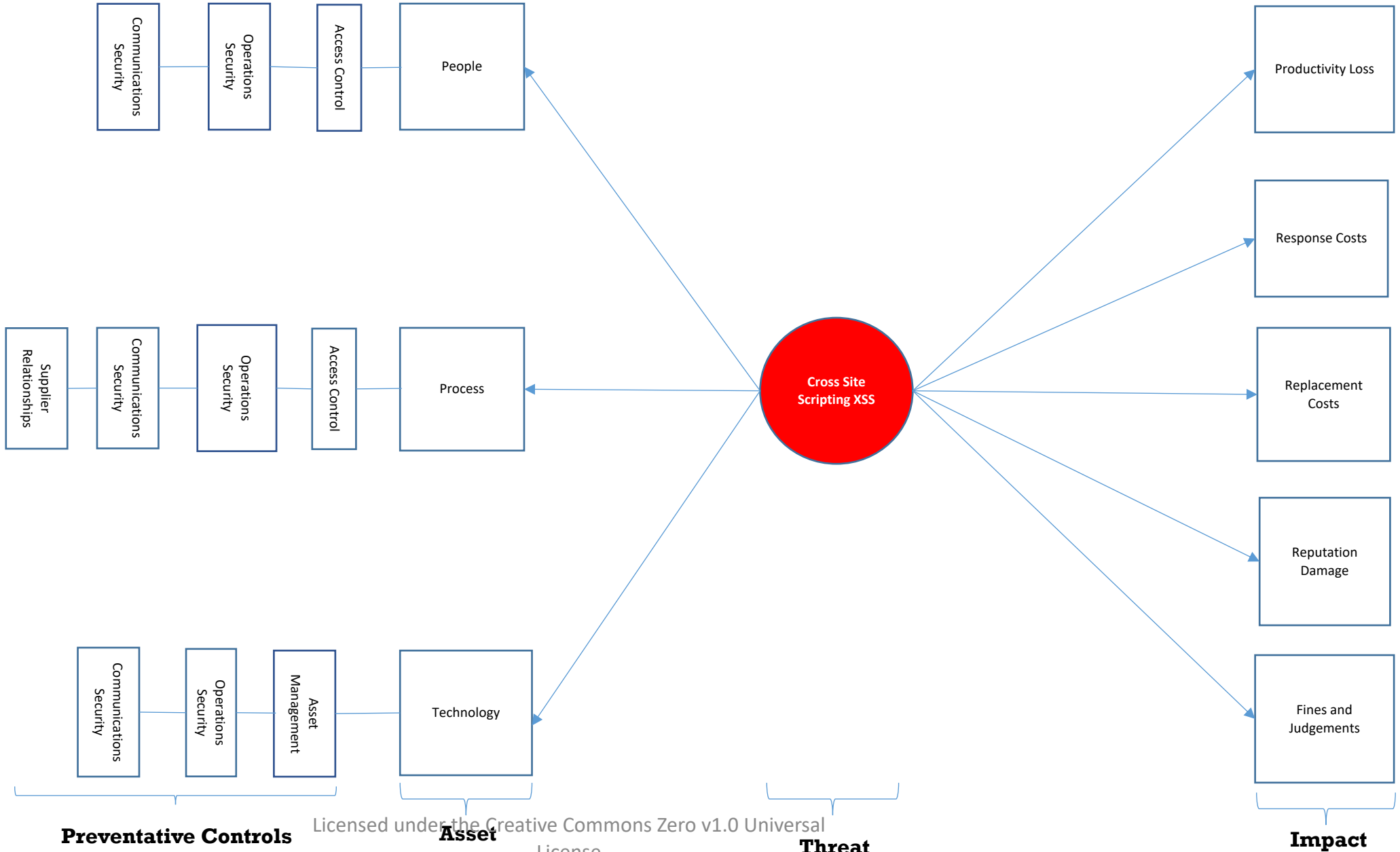
Service Interruption – External Threat Actor (Mitigating)



Service Interruption – External Threat Actor (Mitigating)

Impact	Operations Security	Communications Security	Supplier Relations
Productivity Loss	12.3.1 Information Backup	13.1 Network Security Management	15.1 Information Security in Supplier Relationships
	12.4 Logging and Monitoring	13.2 Information Transfer	15.2 Supplier Service Deliver Management
Response Costs	**Operations Security**	**Information Security Incident Response**	**Information Security Aspects of Business Continuity Management**
	12.3.1 Information Backup	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity
			17.2 Redundancies
Replacement Costs	**Operations Security**	**Supplier Relations**	**System Acquisition, Development and Maintenance**
	12.2 Protection from Malware	15.3 Information and Communication Technology Supply Chain	14.1 Security Requirements of Information Systems
	12.3 Backup	15.2.1 Monitoring and review of supplier services.	14.2 Security in Development and Support Processes
Reputation Damage	**Information Security Incident Response**	**Information Security Aspects of Business Continuity Management**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Fines and Judgement	**Compliance**		
	18.1 Compliance with Legal and Contractual Requirements		
	18.2 Information Security Review		

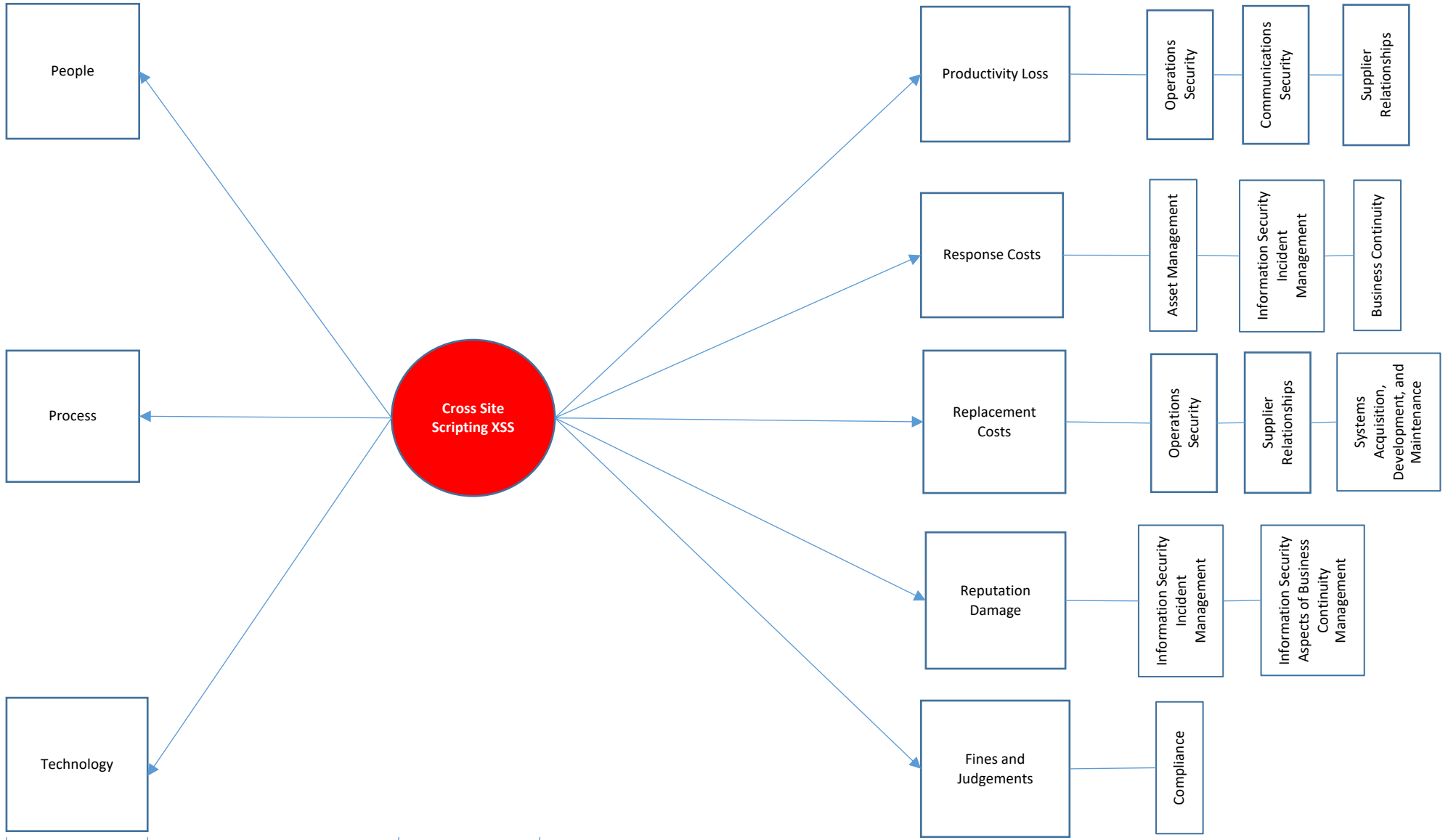
System Breach – External Threat Actor (Preventative)



System Breach – External Threat Actor (Preventative)

Asset	Access Control	Operations Security	Communications Security	
People	9.1.2 Access to Networks and Network Services	12.4 Logging and Monitoring	13.1 Network Security Management	
	9.4 System and Application Access Control	12.6 Technical Vulnerability Management		
Processes	Access Control	Operations Security	Communications Security	Supplier Relationships
	9.1.2 Access to Networks and Network Services	12.1 Operational Procedures and Responsibilities	13.1 Network Security Management	15.1 Information Security in Supplier Relationships
	9.4 System and Application Access Control	12.4 Logging and Monitoring		
		12.6 Technical Vulnerability Management		
Technology	Access Control	Operations Security	Communications Security	
	9.1.2 Access to Networks and Network Services	12.1 Operational Procedures and Responsibilities	13.1 Network Security Management	
	9.4 System and Application Access Control	12.4 Logging and Monitoring		
		12.6 Technical Vulnerability Management		

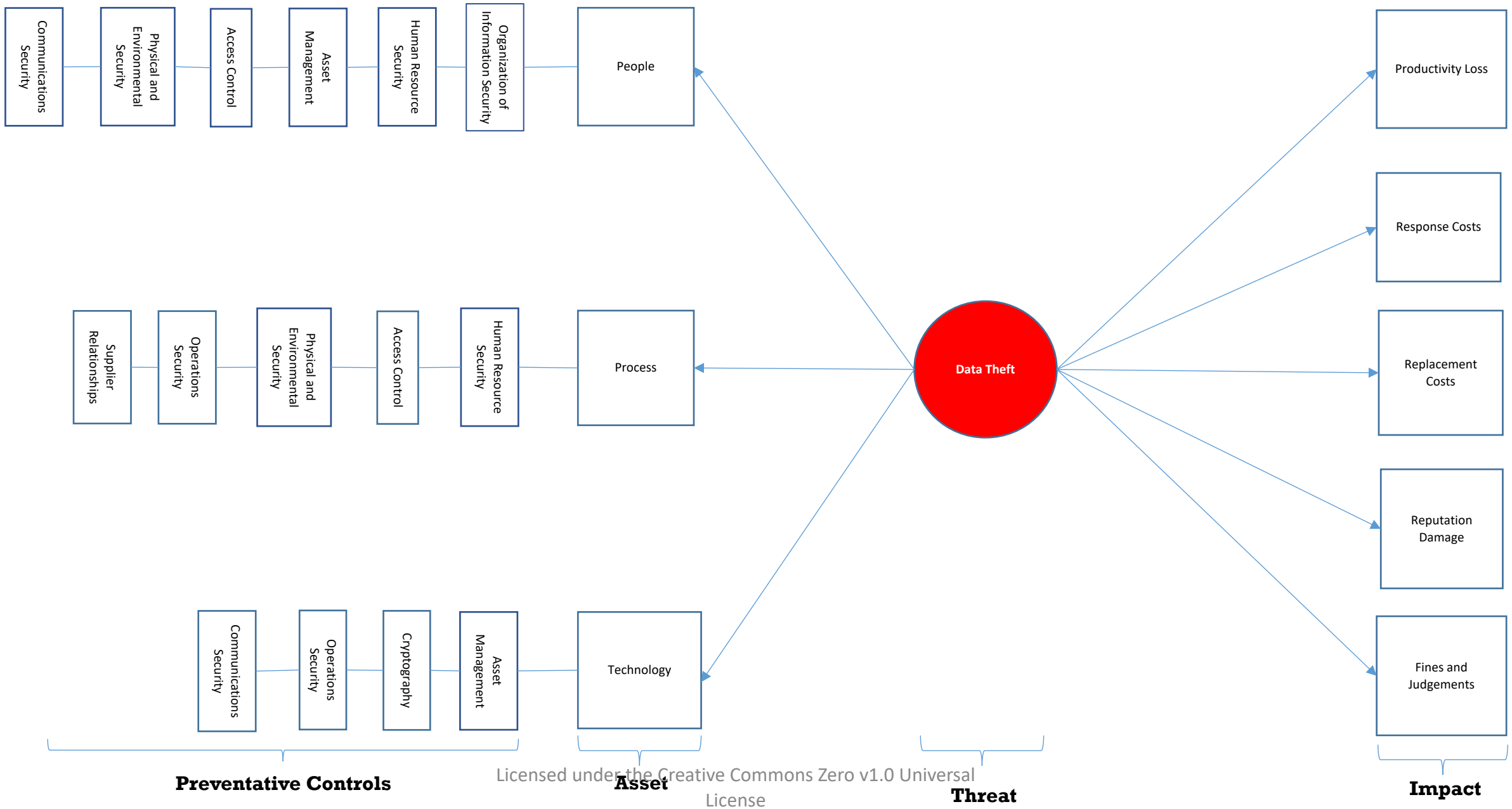
System Breach – External Threat Actor (Mitigating)



System Breach – External Threat Actor (Mitigating)

Impact	Operations Security	Communications Security	Supplier Relationships
Productivity Loss	12.3.1 Information Backup	13.1 Network Security Management	15.1 Information Security in Supplier Relationships
	12.4 Logging and Monitoring		
Response Costs	**Information Security Incident Response**	**Information Security Aspects of Business Continuity Management**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Replacement Costs	**Operations Security**	**Supplier Relationships**	
	12.5 Control of Operational Software	15.3 Information and Communication Technology Supply Chain	
		15.2.1 Monitoring and review of supplier services.	
Reputation Damage	**Information Security Incident Response**	**Information Security Aspects of Business Continuity Management**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Fines and Judgement	**Compliance**		
	18.1 Compliance with Legal and Contractual Requirements		
	18.2 Information Security Review		

Information Breach – Insider Threat Actor (Preventative)



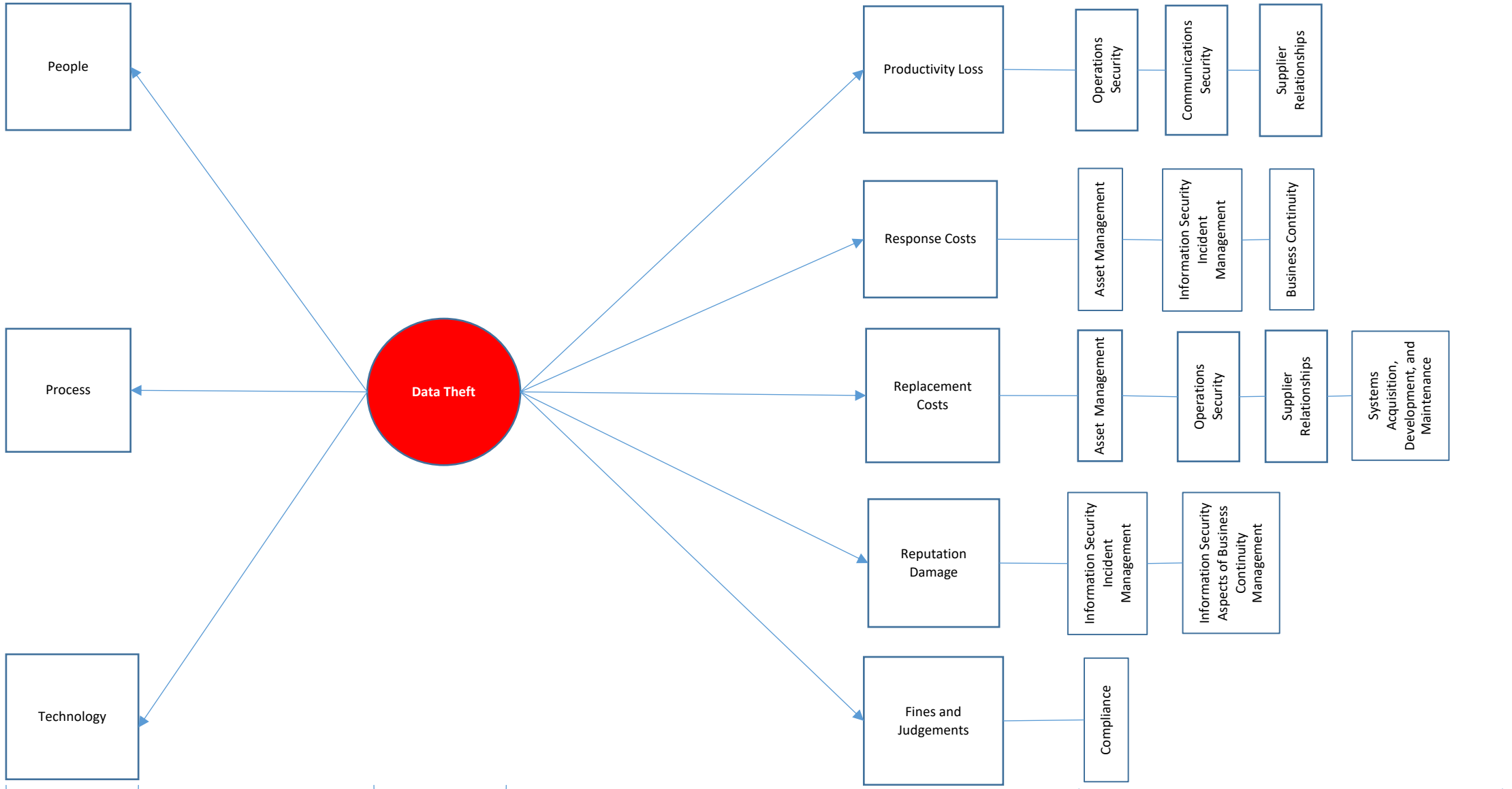
Information Breach – Insider Threat Actor (Preventative)

Asset	Organization of Information Security	Human Resource Security	Asset Management	Access Control	Physical and Environmental Security	Communications Security
People	6.1 Internal Organization	7.1 Prior to Employment	8.1 Responsibility for Assets	9.1 Business Requirements of Access Control	11.1 Secure Area	13.2 Information Transfer
	6.2 Mobile Devices and Teleworking	7.2 During Employment	8.2 Information Classification	9.2 User Access Management		
		7.3 Termination and Change of Employment	8.3 Media Handling	9.4 System and Application Access Control		

Processes	Human Resource Security	Asset Management	Access Control	Physical and Environmental Security	Operations Security	Supplier Relationships
	7.1 Prior to Employment	8.1 Responsibility for Assets	9.1 Business Requirements of Access Control	11.1 Secure Area	12.1 Operational Procedures and Responsibilities	15.1 Information Security in Supplier Relationships
	7.2 During Employment	8.2 Information Classification	9.2 User Access Management			
	7.3 Termination and Change of Employment	8.3 Media Handling	9.4 System and Application Access Control			

Technology	Asset Management	Cryptography	Operations Security	Communications Security		
	8.3 Media Handling	10.1 Cryptographic Controls	12.3 Backup	13.1 Network Security Management		
			12.4 Logging and Monitoring	13.2 Information Transfer		
			12.6 Technical Vulnerability Management			
			12.7 Information Systems Audit Considerations			

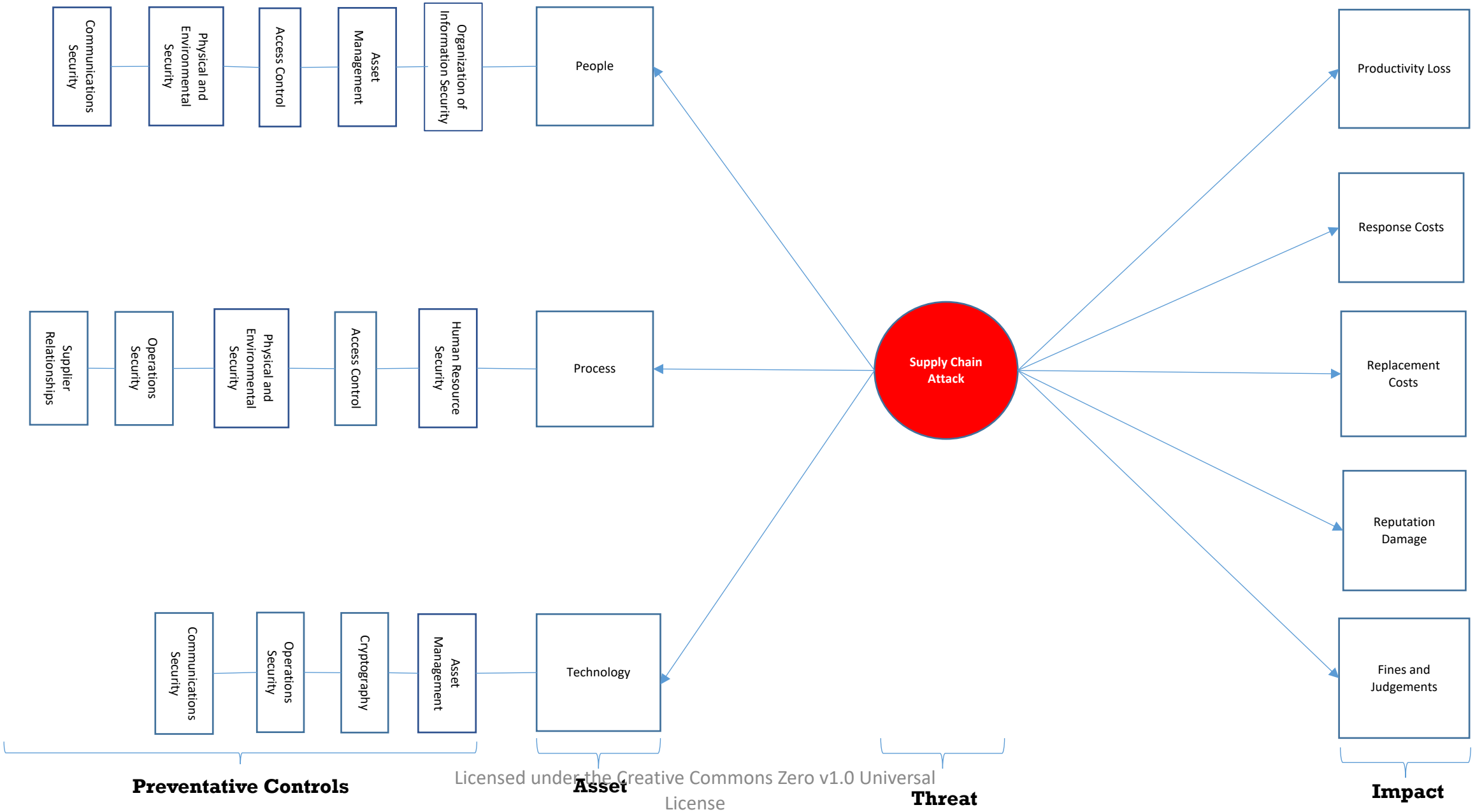
Information Breach – Insider Threat Actor (Mitigating)



Information Breach – Insider Threat Actor (Mitigating)

Impact	Operations Security	Communications Security	Supplier Relationships
Productivity Loss	12.3.1 Information Backup	13.1 Network Security Management	15.1 Information Security in Supplier Relationships
	12.4 Logging and Monitoring		
Response Costs	**Information Security Incident Response**	**Information Security Aspects of Business Continuity Management**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Replacement Costs	**Operations Security**	**Supplier Relationships**	**Systems Acquisition, Development, and Maintenance**
	12.5 Control of Operational Software	15.1.2 Addressing Security within Supplier Agreements	14.1 Security Requirements of Information Systems
		15.3 Information and Communication Technology Supply Chain	14.2 Security in Development and Support Processes
		15.2.1 Monitoring and review of supplier services.	
		15.2.2 Managing Changes to Supplier Services	
Reputation Damage	**Information Security Incident Response**	**Information Security Aspects of Business Continuity Management**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Fines and Judgement	**Compliance**		
	18.1 Compliance with Legal and Contractual Requirements		
	18.2 Information Security Review		

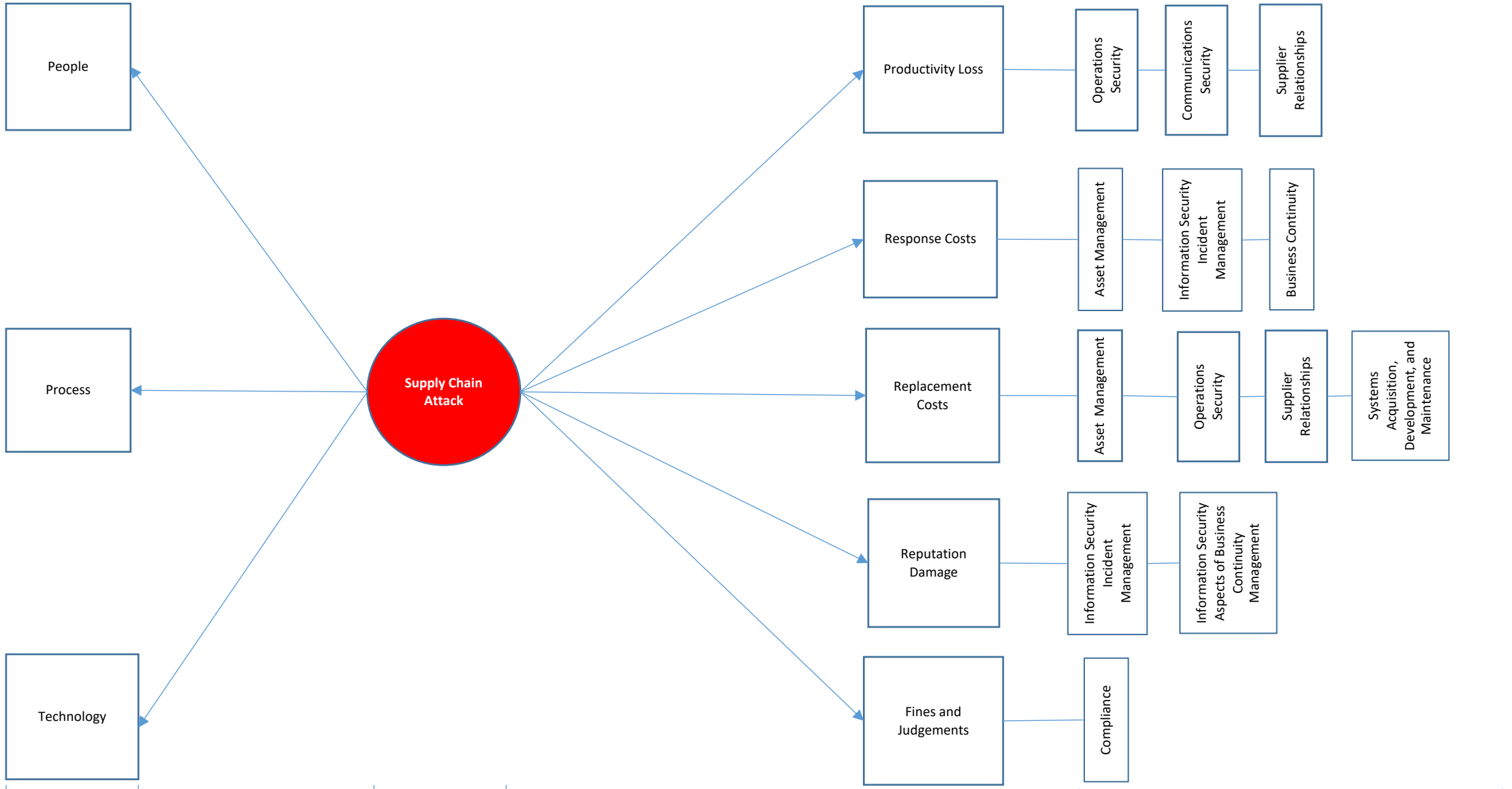
Information Breach – Insider Threat Actor (Preventative)



Information Breach – Insider Threat Actor (Preventative)

Asset	Organization of Information Security	Asset Management	Access Control	Physical and Environmental	Communications Security
People	6.1 Internal Organization	8.1 Responsibility for Assets	9.1 Business Requirements of Access Control	11.1 Secure Area	13.2 Information Transfer
	6.2 Mobile Devices and Teleworking	8.2 Information Classification	9.2 User Access Management		
		8.3 Media Handling	9.4 System and Application Access Control		
Processes	**Asset Management**	**Access Control**	**Physical and Environmental Security**	**Operations Security**	**Supplier Relationships**
	8.1 Responsibility for Assets	9.1 Business Requirements of Access Control	11.1 Secure Area	12.1 Operational Procedures and Responsibilities	15.1 Information Security in Supplier Relationships
	8.2 Information Classification	9.2 User Access Management			
	8.3 Media Handling	9.4 System and Application Access Control			
Technology	**Asset Management**	**Cryptography**	**Operations Security**	**Communications Security**	
	8.3 Media Handling	10.1 Cryptographic Controls	12.3 Backup	13.1 Network Security Management	
			12.4 Logging and Monitoring	13.2 Information Transfer	
			12.6 Technical Vulnerability Management		
			12.7 Information Systems Audit Considerations		

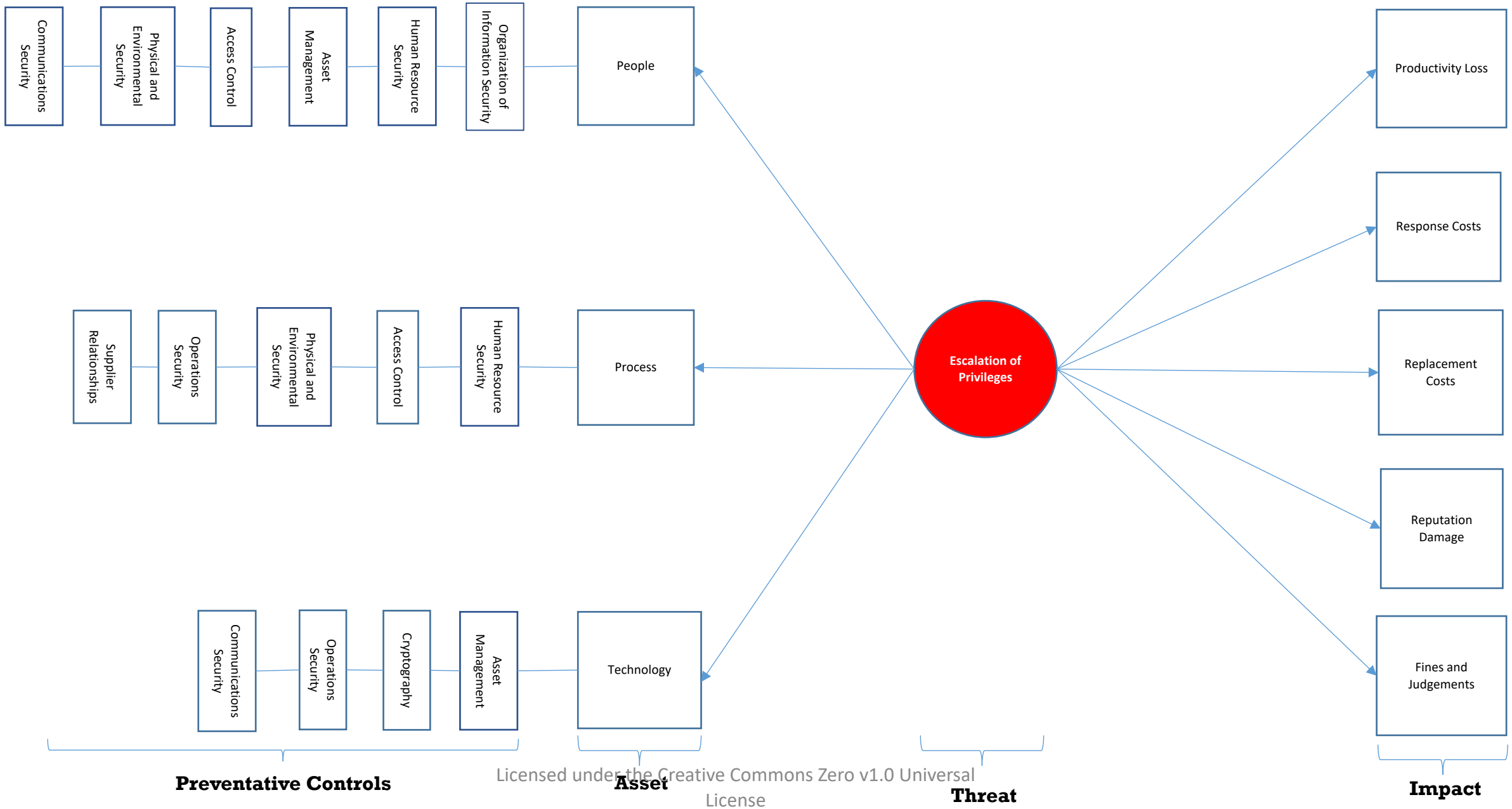
Information Breach – Insider Threat Actor (Mitigating)



Information Breach – Insider Threat Actor (Mitigating)

Impact	Operations Security	Communications Security	Supplier Relations
Productivity Loss	12.3.1 Information Backup	13.1 Network Security Management	15.1 Information Security in Supplier Relationships
	12.4 Logging and Monitoring		
Response Costs	**Information Security Incident Response**	**Information Security Aspects of Business Continuity Management**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Replacement Costs	**Operations Security**	**Supplier Relations**	**Systems Acquisition, Development, and Maintenance**
	12.5 Control of Operational Software	15.1.2 Addressing Security within Supplier Agreements	14.1 Security Requirements of Information Systems
		15.3 Information and Communication Technology Supply Chain	14.2 Security in Development and Support Processes
		15.2.1 Monitoring and review of supplier services.	
		15.2.2 Managing Changes to Supplier Services	
Reputation Damage	**Information Security Incident Response**	**Information Security Aspects of Business Continuity Management**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Fines and Judgement	**Compliance**		
	18.1 Compliance with Legal and Contractual Requirements		
	18.2 Information Security Review		

Information Breach – Insider Threat Actor (Preventative)



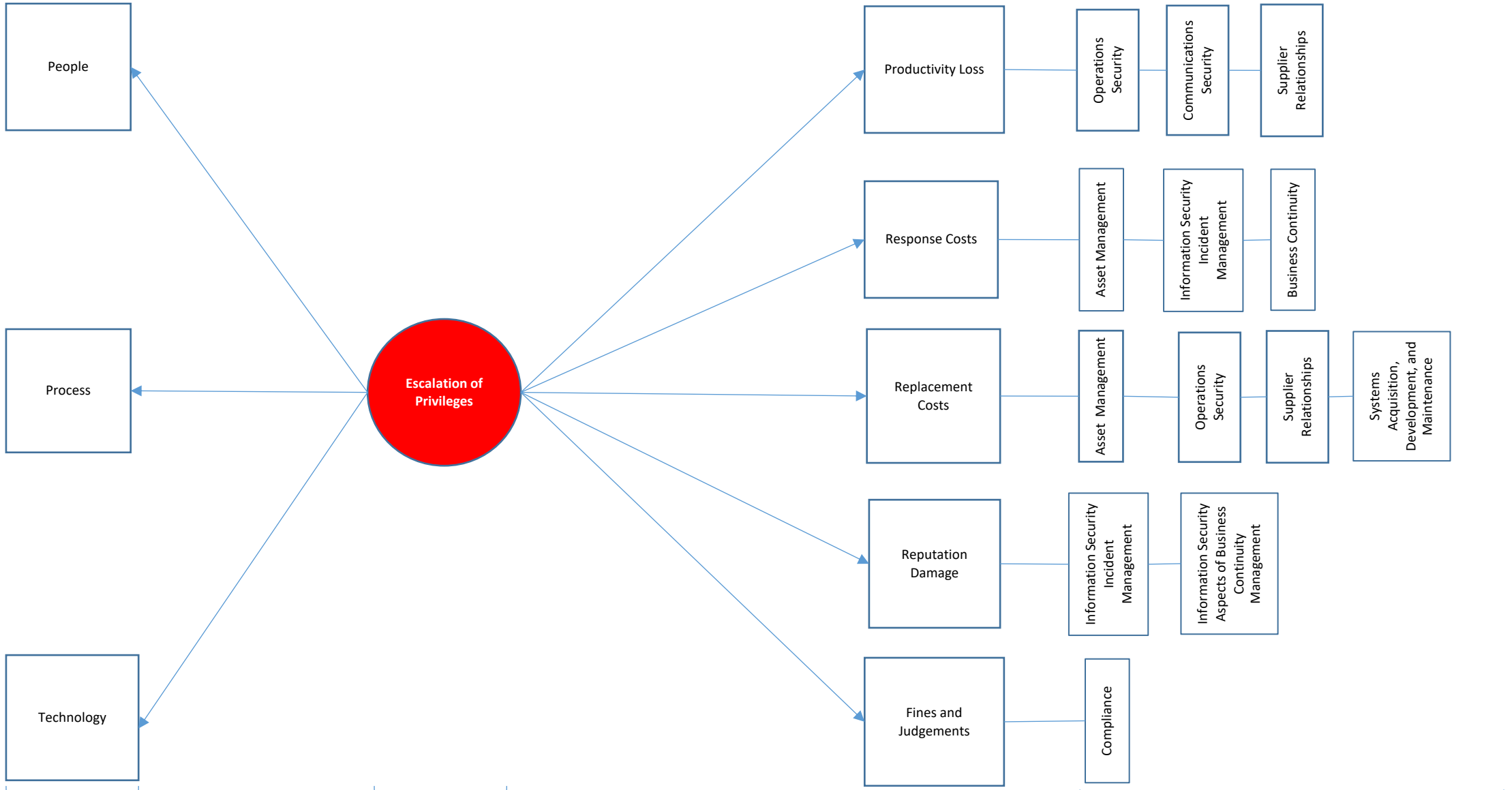
Information Breach – Insider Threat Actor (Preventative)

Asset	Organization of Information Security	Human Resources	Asset Management	Access Control	Physical and Environmental Security	Communications Security
People	6.1 Internal Organization	7.1 Prior to Employment	8.1 Responsibility for Assets	9.1 Business Requirements of Access Control	11.1 Secure Area	13.2 Information Transfer
	6.2 Mobile Devices and Teleworking	7.2 During Employment	8.2 Information Classification	9.2 User Access Management		
		7.3 Termination and Change of Employment	8.3 Media Handling	9.4 System and Application Access Control		

Processes	Human Resources	Asset Management	Access Control	Physical and Environmental Security	Operations Security	Supplier Relationships
	7.1 Prior to Employment	8.1 Responsibility for Assets	9.1 Business Requirements of Access Control	11.1 Secure Area	12.1 Operational Procedures and Responsibilities	15.1 Information Security in Supplier Relationships
	7.2 During Employment	8.2 Information Classification	9.2 User Access Management			
	7.3 Termination and Change of Employment	8.3 Media Handling	9.4 System and Application Access Control			

Technology	Asset Management	Cryptography	Operations Security	Communications Security		
	8.3 Media Handling	10.1 Cryptographic Controls	12.3 Backup	13.1 Network Security Management		
			12.4 Logging and Monitoring	13.2 Information Transfer		
			12.6 Technical Vulnerability Management			
			12.7 Information Systems Audit Considerations			

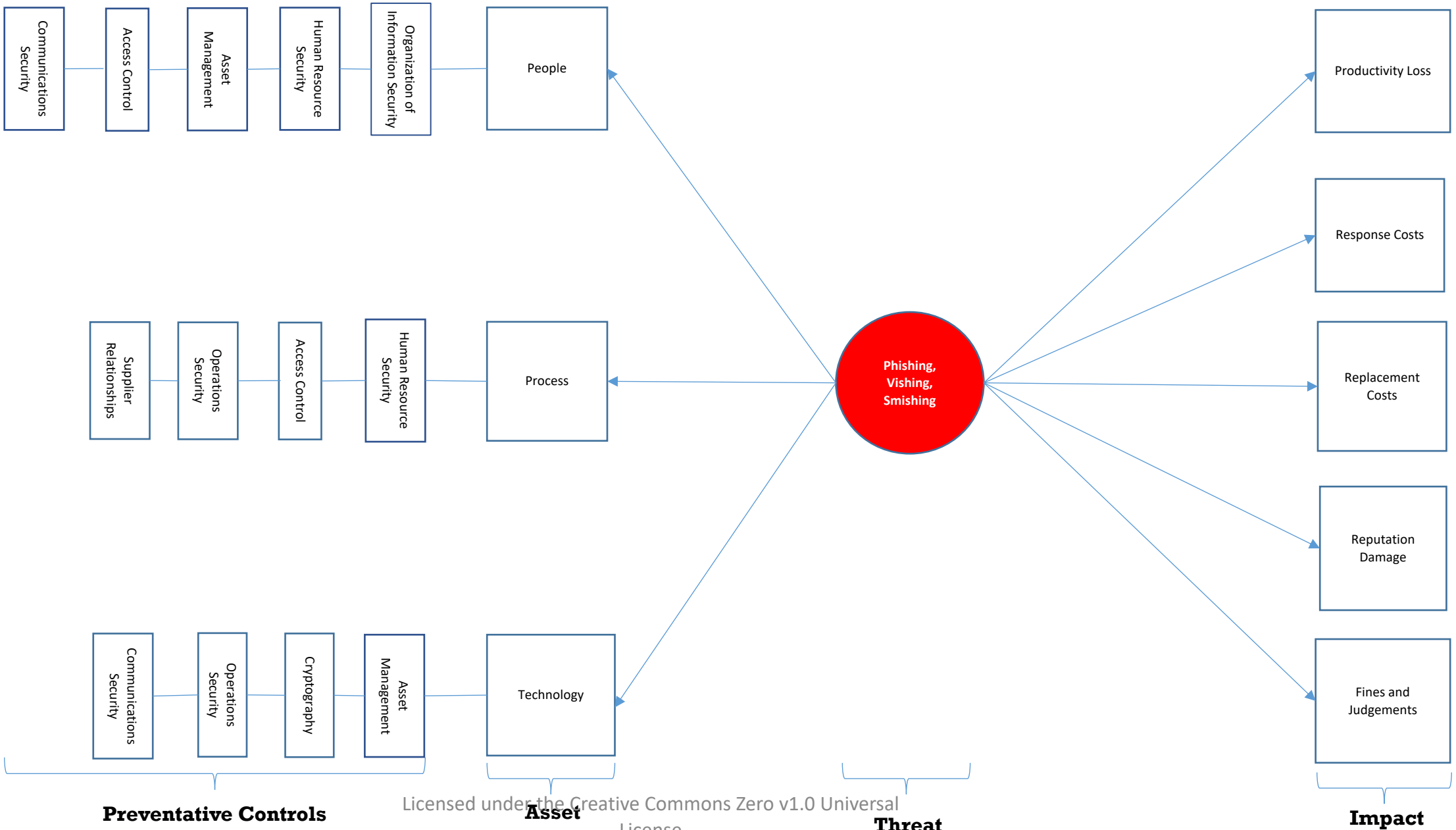
Information Breach – Insider Threat Actor (Mitigating)



Information Breach – Insider Threat Actor (Mitigating)

Impact	Operations Security	Communications Security	Supplier Relationships
Productivity Loss	12.3.1 Information Backup	13.1 Network Security Management	15.1 Information Security in Supplier Relationships
	12.4 Logging and Monitoring		
Response Costs	**Information Security Incident Response**	**Information Security Aspects of Business Continuity Management**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Replacement Costs	**Operations Security**	**Supplier Relationships**	**Systems Acquisition, Development, and Maintenance**
	12.5 Control of Operational Software	15.1.2 Addressing Security within Supplier Agreements	14.1 Security Requirements of Information Systems
		15.3 Information and Communication Technology Supply Chain	14.2 Security in Development and Support Processes
		15.2.1 Monitoring and review of supplier services.	
		15.2.2 Managing Changes to Supplier Services	
Reputation Damage	**Information security Incident Response**	**Information Security Aspects of Business Continuity Management**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Fines and Judgement	**Compliance**		
	18.1 Compliance with Legal and Contractual Requirements		
	18.2 Information Security Reviews		

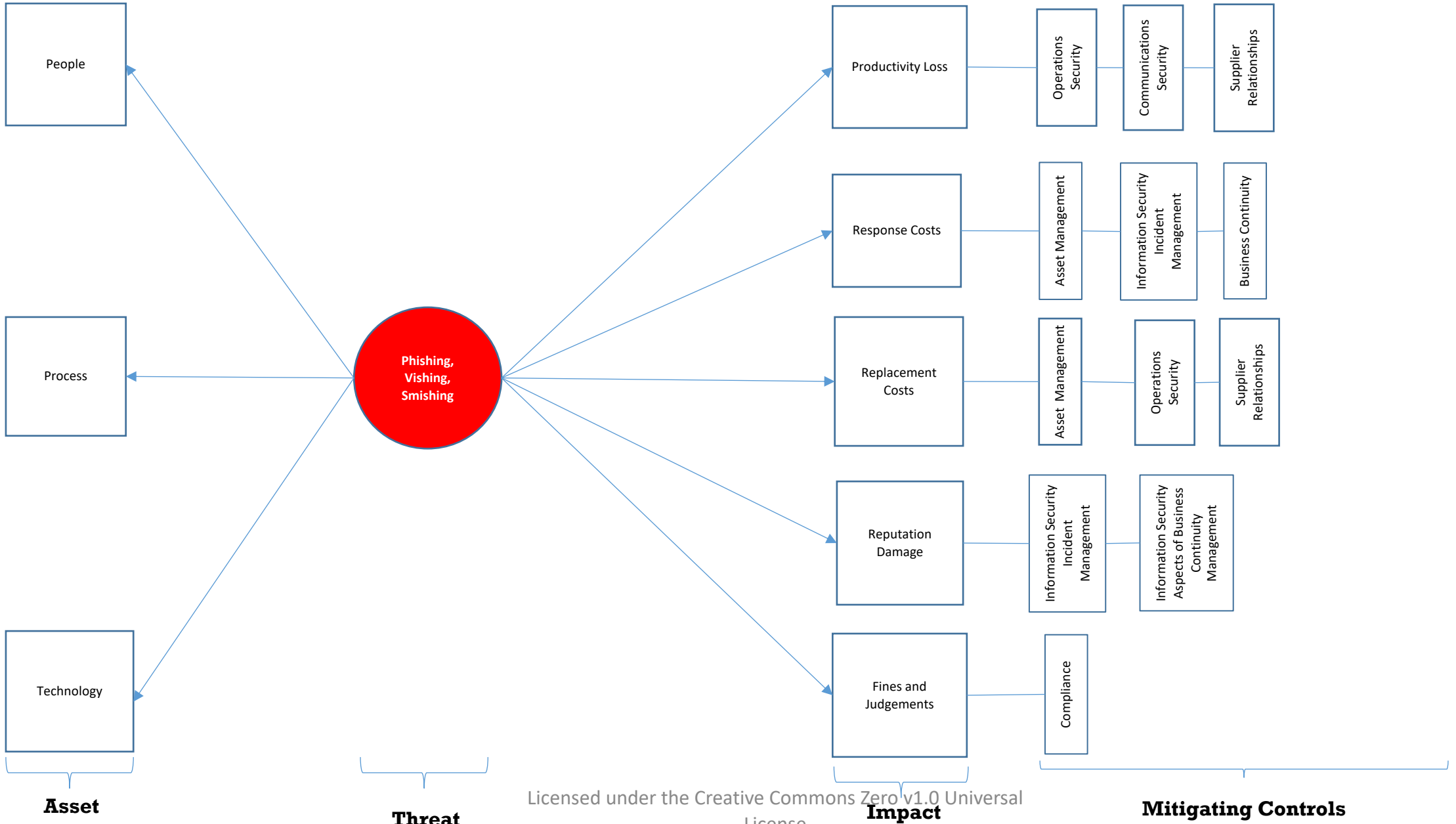
Social Engineering– External Threat Actor (Preventative)



Social Engineering– External Threat Actor (Preventative)

Asset	Organization of Information Security	Human Resource Security	Asset Management	Access Control	Physical and Environmental Security	Communications Security
People	6.1 Internal Organization	7.2.2 Information Security Awareness, Education and Training	8.2 Information Classification	9.1.2 Access to Networks and Network Services	11.2.8 Unattended User Equipment	13.2 Information Transfer
	6.2 Mobile Devices and Teleworking		8.3 Media Handling	9.4.1 Information Access Restriction		
Processes	**Human Resource Security**	**Asset Management**	**Access Control**	**Operations Security**	**Supplier Relationships**	
	7.2 During Employment	8.1 Responsibility for Assets	9.1.2 Access to Networks and Network Services	12.1 Operational Procedures and Responsibilities	15.1 Information Security in Supplier Relationships	
		8.2 Information Classification	9.4.1 Information Access Restriction			
		8.3 Media Handling				
Technology	**Asset Management**	**Cryptography**	**Operations Security**	**Communications Security**		
	8.3 Media Handling	10.1 Cryptographic Controls	12.3 Backup	13.1 Network Security Management		
			12.4 Logging and Monitoring	13.2 Information Transfer		
			12.6 Technical Vulnerability Management			
			12.7 Information Systems Audit Considerations			

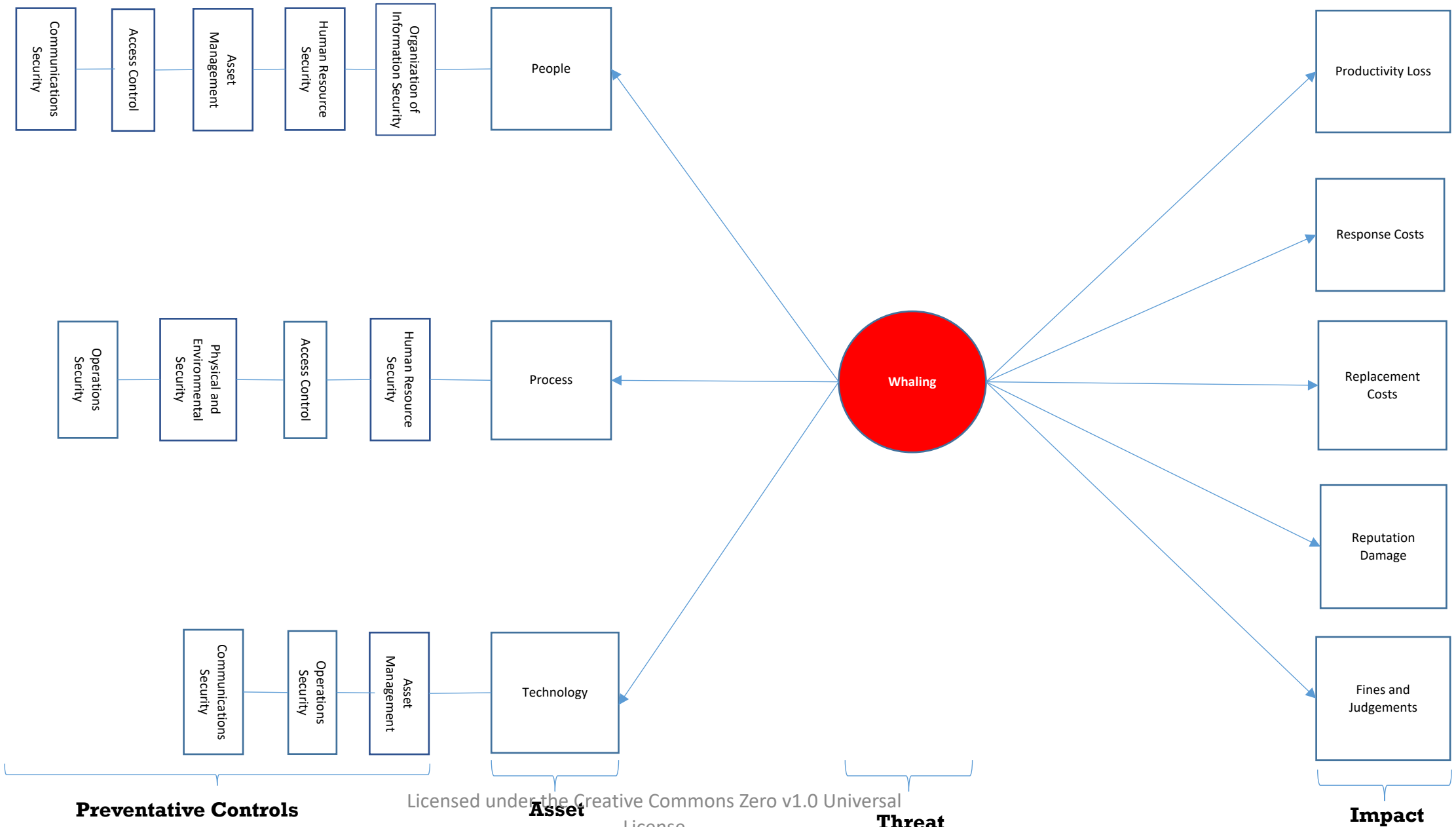
Social Engineering– External Threat Actor (Mitigating)



Social Engineering– External Threat Actor (Mitigating)

Impact	Operations Security	Communications Security	Supplier Relationships
Productivity Loss	12.3.1 Information Backup	13.1 Network Security Management	15.1 Information Security in Supplier Relationships
	12.4 Logging and Monitoring		
Response Costs	**Information Security Incident Response**	**Information Security Aspects of Business Continuity Management**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Replacement Costs	**Operations Security**	**Supplier Relationships**	
	12.5 Control of Operational Software	15.1.2 Addressing Security within Supplier Agreements	
		15.3 Information and Communication Technology Supply Chain	
		15.2.1 Monitoring and review of supplier services.	
		15.2.2 Managing Changes to Supplier Services	
Reputation Damage	**Information Security Incident Response**	**Information Security Aspects of Business Continuity Management**	
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity	
		17.2 Redundancies	
Fines and Judgement	**Compliance**		
	18.1 Compliance with Legal and Contractual Requirements		
	18.2 Information Security Reviews		

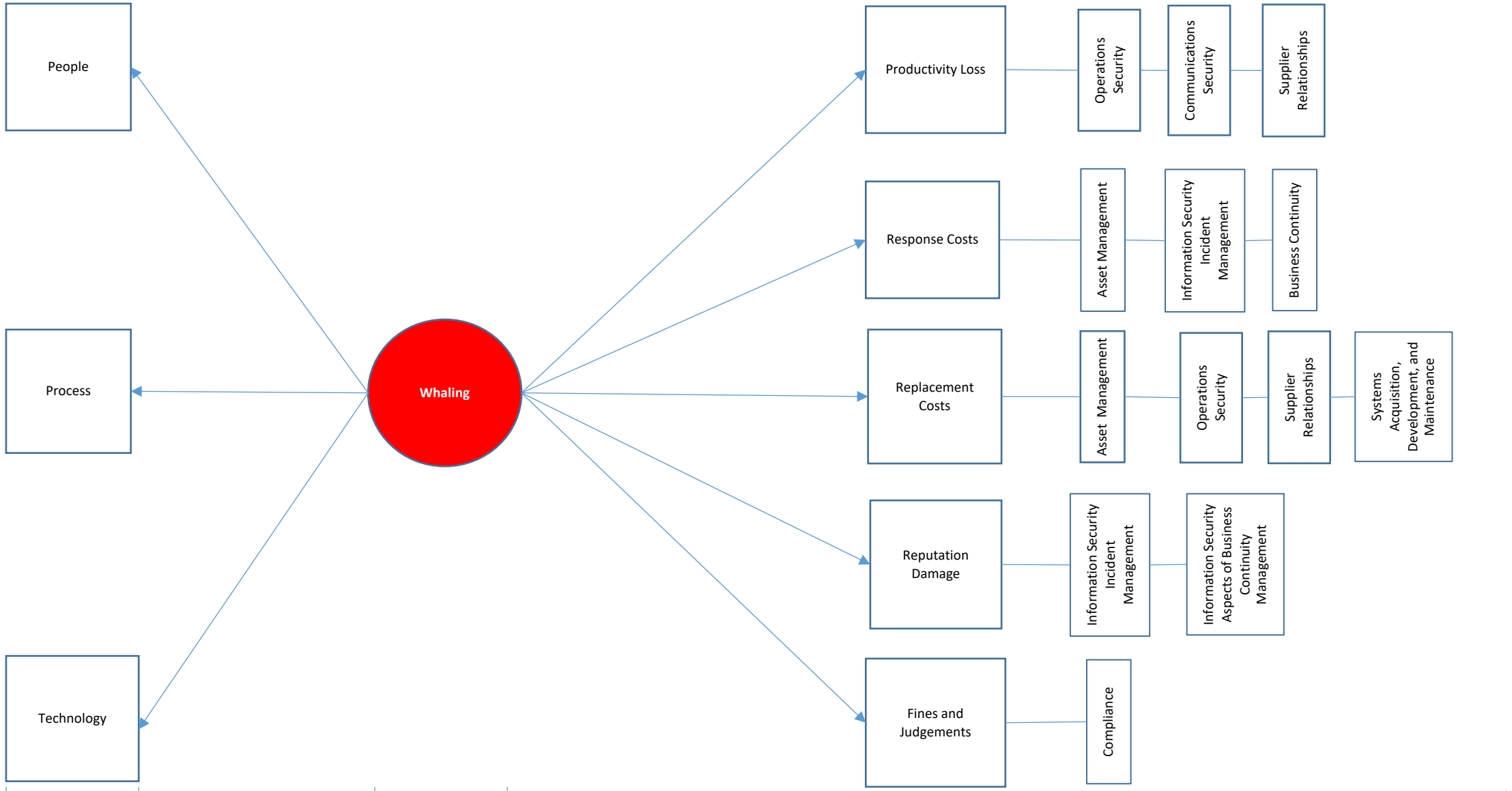
Social Engineering – External Threat Actor (Preventative)



Social Engineering – External Threat Actor (Preventative)

Asset	Organization of Information Security	Human Resource Security	Asset Management	Access Control	Communications Security
People	6.1 Internal Organization	7.2.2 Information Security Awareness, Education and Training	8.2 Information Classification	9.1.2 Access to Networks and Network Services	13.2 Information Transfer
	6.2 Mobile Devices and Teleworking		8.3 Media Handling	9.4.1 Information Access Restriction	
Processes	**Human Resource Security**	**Asset Management**	**Access Control**	**Operations Security**	
	7.2 During Employment	8.1 Responsibility for Assets	9.1.2 Access to Networks and Network Services	12.1 Operational Procedures and Responsibilities	
		8.2 Information Classification	9.4.1 Information Access Restriction		
		8.3 Media Handling			
Technology	**Asset Management**	**Operations Security**	**Communications Security**		
	8.3 Media Handling	12.3 Backup	13.1 Network Security Management		
		12.4 Logging and Monitoring	13.2 Information Transfer		
		12.6 Technical Vulnerability Management			
		12.7 Information Systems Audit Considerations			

Social Engineering – External Threat Actor (Mitigating)



Social Engineering – External Threat Actor (Mitigating)

Impact	Operations Security	Communications Security
Productivity Loss	12.3.1 Information Backup	13.1 Network Security Management
	12.4 Logging and Monitoring	
Response Costs	**Information Security Incident Response**	**Information Security Aspects of Business Continuity Management**
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity
		17.2 Redundancies
Replacement Costs	**Operations Security**	**Supplier Relations**
	12.5 Control of Operational Software	15.1.2 Addressing Security within Supplier Agreements
		15.3 Information and Communication Technology Supply Chain
		15.2.1 Monitoring and review of supplier services
		15.2.2 Managing Changes to Supplier Services
Reputation Damage	**Information security Incident Response**	**Information Security Aspects of Business Continuity Management**
	16.1 Management of Information Security Incidents and Improvements	17.1 Information Security Continuity
		17.2 Redundancies
Fines and Judgement	**Compliance**	
	18.1 Compliance with Legal and Contractual Requirements	