Process – incident response process.

Purpose -	The incident response process is the main security response / implementation in the case of xy innovate. This process would be in response to managing a security threat / vulnerability or a breach with the intention to mitigate the impact that this breach would cause to our organization. With the breach impacting operational stability, integrity of our financial data alongside the reputational risks that arise from cyberattacks. By xy innovate adhering to the iso/IEC 27001 clause 10.1 University of Bradford week 11 (2024) and 27305 standard this process would ensure an aspect of continual and gradual grown and alignment with our organizational objectives of increased safety and security especially in an industry where customer trust would be critical for success.
Scope	The scope of this process would be applicable to every aspect of the organisation for example the digital wallet application and external 3rd party individuals such as digital ocean, alongside the relationship with customers and financial data. The scope also includes all staff and individuals involved with ensuring the safety of organisational systems.
Process of implementation Analysis provided below	1) Detection and identification 2) The initial response of action. 3) Analysis and risk-based prioritisation 4) Nonconformity review 5) Containment and eradication 6) Recovery 7) External reporting 8) Post incident evaluation and improvement strategy.
Responsibility	The Ciso in this instance would take responsibility for ensuring the management of this entire procedure ensuring that the correct alignment with the implementation of the procedure with the objectives of the organisation. The IT and digital wallet team would establish an incident response team to execute the containment and implementation of new security measures. The dedicated soc team and the IT department would then monitor the system and conduct a technical review during the incident for more information and the employees involved would report any threats and vulnerabilities immediately to management and the relevant individuals involved
Integration with Training and Testing	The Procedure in place for this control would be to ensure that the organisation is conducting regular incident response drills to ensure the readiness of all parties involved. This would be implanted by ensuring that we are running regular training campaigns for our staff to reinforce employees understanding of security protocols.

1. The initial step that I have identified that would be the foundation of the process is the detection and identification process. We would utilise tools and techniques such as SIEM Systems (Security and event management) alongside ids systems and endpoint monitoring tools that would allow us to detect threats in the system. An example of how this look in the organisational in an implemented process would be that the system would flag an unusual log in pattern form inside the organisation which we could presume to be credential

theft. The Second step in the process would be the incident categorization, this step is crucial as it would allow us to make a decision on what is the severity of the incident for example minor system issues vs highly sensitive data being breached and this would be graded against the potential impact and the compliance obligations that are in place for example high risk issues would require escalation.

2. The second step in my process would be that of the initial response to a threat or vulnerability once detected. The main aspect of this would be to ensure a level of containment immediately which would include isolating the affected systems and revoking credentials that were utilised in the breach and to also active firewalls and the security measures to limit the spread of the issue. The next step in the Process would be to invoke a sense of team coordination to utilise the incident response specialist which would ensure a sense of responsibility and alignment with predefined roles and responsibilities that have been previously assigned in xy innovates case.

3. Conduct and analysis and risk-based prioritization scale. In this step of our process, it is essential to conduct a root case analysis, this would ensure that we are investigating the incidents origins such as an issue in access controls, credential management or misconfigurations. The second element in the step would be to conduct a risk assessment with the intention to assess the incidents impact on the confidentiality, integrity and availability (CIA Triad) of the assets and systems in question. An example of this in practice would be in the xy innovate case study where the breach exposed private customer financial information which resulted in GDPR penalties and reputational damage.

4. Nonconformity Review – this step would place the focus on documenting and assessing how controls and individuals are deviating from the isms protocol such as system that are yet to be updated, or unpatched systems alongside unauthorized access which would lead to intruders accessing our systems. The purpose of these reviews is that once they have been stabilised, we would be able to implement this into the organisations plan – do – check – act (PDAC) cycle for the ism's improvement process.

5. This section would be on containment and eradication. The intention behind this would that is essential to implement technical controls such as implementing technical controls to mitigate the threats. An example of this would be removing the malware from the system and to implement system software patching and

updates. It would also be the correct response to reset the configurations to appropriately handle the threats and breaches.

6. This next process in line to be implemented would be that of recovery. It would be essential to ensure that the systems have a level of integrity and security before restoring the operations back to normal which would be done by comparing the systems to the baseline normal. This step ensure that we would focus on restoring usability and access of critical infrastructure to ensure that the customers would not face any downtime and that the servers would resume their function promptly. This would be backed up by reference to the ISO/IEC 27031 (ISO27001 Security) 2024 framework which promotes the importance of (ICT) readiness for business continuity,

7. External Reporting – The implementation of this step would be crucial because Under the GDPR regulations Article 33 (General Data Protection Regulation, 2016). we are required to notify the regulatory authorities such as the ICO within 72 hours of the breach occurring to ensure a level of accountability and proactivity when recovering from cyberattacks and threats. Alongside the relevant communication externally, internal management could also notify customers and individuals involved of the data breach / threats at hand regarding the issue and the impact and what resolution is in place to mitigate the impact of the issue at hand.

8. Post incident Evaluation and improvement plan- the importance of this step would be that we would ensue that w conduct meeting and improvement strategies to analyse the effectiveness of all the measures I have just discussed alongside identifying gaps in the current processes and controls. From this step we would then look to update the isms documentation and revise the current policies, processes and procedures and provide training to staff based on what is currently lacking.

University of Bradford (2024) 'Week 11_Check and Act Phases' [PowerPoint presentation], University of Bradford.

ISO27001 Security, 2025. ISO/IEC 27031 – ICT Readiness for Business Continuity. *ISO27001 Security*. Available at: https://www.iso27001security.com/html/27031.html [Accessed 2 January 2025].

General Data Protection Regulation, 2016. Art. 33 GDPR – Notification of a personal data breach to the supervisory authority. *General Data Protection Regulation (GDPR)*. Available at: Art. 33 GDPR – Notification of a personal data breach to the supervisory authority - General Data Protection Regulation (GDPR) [Accessed 2 January 2025].