Group Notes

Table of Contents

1. Introduction

This is a consolidation of SRM_PCOM7E September 2022 Group 1 - The A Team's notes.

1.1 Team Admin

1. Timezone Comparison
2. Current roles (rotate every 2 weeks):
    a. Wed 28 Sep - Sun 16 Oct 2022
        - Project Lead/Arbitrator: Marios
        - Facilitator/Coordinator: Lee
        - Editor: Celine
        - Proofreader: Nomusa
    b. Sun 16 Oct - Sun 30 Oct 2022
        - Project Lead/Arbitrator: Nomusa
        - Facilitator/Coordinator: Marios
        - Editor: Lee
        - Proofreader: Celine
    c. Sun 30 Oct - Sun 13 Nov 2022
        - Project Lead/Arbitrator: Celine
        - Facilitator/Coordinator: Nomusa
        - Editor: Marios
        - Proofreader: Lee
    d. Sun 13 Nov - Sun 27 Nov 2022
        - **Project Lead/Arbitrator: Lee**
        - **Facilitator/Coordinator: Celine**
        - **Editor: Nomusa, James**

- **Proofreader: Marios**

1.2 Action Items

Due on Sunday 16/10/2022:

1. [25%] Before Digitalisation
    a. Profit risk assessment
        i. Logistics POV - Lee
        ii. Customer POV - Marios
        iii. Data POV - Celine
        iv. Legal/compliance POV - Bali
    b. Octave - Operationally Critical Threat, Asset and Vulnerability Evaluation
        i. Asset – less than 40 ppl in a company
    c. List of mitigations (threat trees?)
2. [15%] After Digitalization
    a. Profit risk assessment
        i. Logistics POV - Lee
        ii. Customer POV - Marios
        iii. Data POV - Celine
        iv. Legal/compliance POV - Bali
    b. List of proposed changes:
        i. Interactive web application
            1. Customer portal
                a. Web and mobile
            2. Supplier portal
                a. Web and mobile
            3. Administrative portal
                a. Owner
            4. Manager portal
                a. Owner and managers
            5. Wix for the web app
        ii. Database
            1. Amazon or Microsoft
            2. Insurance
            3. Back up
            4. Third party deniability
        iii. Staff knowledge
            1. Threat awareness
                a. Phishing
                b. Passwords
                c. Usernames
                d. malware

iv. Customer welcome tutorial + help article
    1. Pop-up on the website
        a. Threat advice
        b. Good password practices
        c. Good username practices
v. Payment
    1. Credit card
    2. Paypal
    3. Banking security
    4. Two/multiple factor auth
    5. PCI compliance (pcicompliance.org)

c. Octave and (threat trees?)
d. Potential mitigations
    i. Have beta testers
    ii. Authentication, session mgmt, access controls
    iii. Staff training
    iv. Customer tutorials
    v. Database security

1.3 Questions

Below are questions to ask/clarify with our tutor, Doug:

- For the individual e-Portfolio submission, how much of it can be similar to the other group members?
    - Meeting minutes
    - Individual work – what I did in the project
    - Peer reviews forms into consideration

  Can we consider separating the different risk management process steps (say 2 people looking at each) - sounds good to me -Lee; I second that - Celine
  Will give us an opportunity to represent different aspects especially for the eportfolio

- How are we meant to quantify numbers provided in the assignment prompt – does 50% mean 50%?
    - “We can not at this time provide numbers for…”
    - Qualitative : should we go the numerical quantitative route then we can use other companies as a benchmark
- Do we assume that Covid never happened?
    - Course text – very useful data here (need to look closer)
        - Supply chain, inventory, disasters
    - Effects of global disruptions (course text)
    - Supply chain , inventory and disasters

    - Separate C
- Charts
    - Percentage questions
    - Tables for open fare, come up with numerical qualitative assessment
    - Can be 3-4 for lit review

Meeting with Doug 20/10/2022:

- What is the timeline diagram/Gantt chart?
    - Project plan for implementation
        - Use excel for it
        - Whatever they should do with digitalization – how long do you think it would take to digitalize
            - List of activities, timeline of when these activities would happen
        - Implementation plan - our suggested changes
- What scope of assessment are we expected to perform?
    - Same as the NIST tier structure?
- Is following the NIST formula good enough for the RA?
- How detailed should we be in our TMs?
    - How many are acceptable?

2. Reading Notes

Reading: A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000

- Some things we can possibly use when designing our risk measures
- Pictures can be enlarged

- ERM - enterprise risk mgmt
- COSO ERM cube
- Detailed risk:

Table 1: Detailed risk description

1	Name or title of risk	• Unique identifier or risk index
2	Scope of risk	• Scope of risk and details of possible events, including description of the events, their size, type and number
3	Nature of risk	• Classification of risk, timescale of potential impact and description as hazard, opportunity or uncertainty
4	Stakeholders	• Stakeholders, both internal and external, and their expectations
5	Risk evaluation	• Likelihood and magnitude of event and possible impact or consequences should the risk materialise at current level
6	Loss experience	• Previous incidents and prior loss experience of events related to the risk
7	Risk tolerance, appetite or attitude	• Loss potential and anticipated financial impact of the risk • Target for control of risk and desired level of performance • Risk attitude, appetite, tolerance or limits for the risk
8	Risk response, treatment and controls	• Existing control mechanisms and activities • Level of confidence in existing controls • Procedures for monitoring and review of risk performance
9	Potential for risk improvement	• Potential for cost-effective risk improvement or modification • Recommendations and deadlines for implementation • Responsibility for implementing any improvements
10	Strategy and policy developments	• Responsibility for developing strategy related to the risk • Responsibility for auditing compliance with controls

- Risk classification systems: financial control, operation efficiency, reputational exposure, commercial activities
    - Should have a focus and objective
    - Include an upside (benefits), downside (threat to success), or increased degree of uncertainty
- Risk mgmt process: 7Rs and 4Ts of (Hazard) RM

- recognition or identification of risks
- ranking or evaluation of risks
- responding to significant risks
  - tolerate
  - treat
  - transfer
  - terminate
- resourcing controls
- reaction planning
- reporting and monitoring risk performance
- reviewing the risk management framework

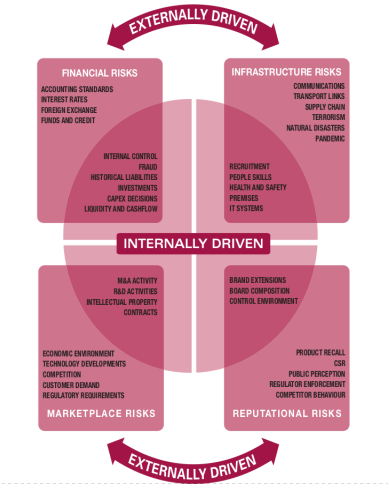
- Some of these can probably be applied:

Table 2: Contents of risk management policy

A risk management policy should include the following sections:
Risk management and internal control objectives (governance)
Statement of the attitude of the organisation to risk (risk strategy)
Description of the risk aware culture or control environment
Level and nature of risk that is acceptable (risk appetite)
Risk management organisation and arrangements (risk architecture)
Details of procedures for risk recognition and ranking (risk assessment)
List of documentation for analysing and reporting risk (risk protocols)
Risk mitigation requirements and control mechanisms (risk response)
Allocation of risk management roles and responsibilities
Risk management training topics and priorities
Criteria for monitoring and benchmarking of risks
Allocation of appropriate resources to risk management
Risk activities and risk priorities for the coming year

- employer/employee responsibilities in managing risk (table is loooong, p. 12)
- HAZOP and FMEA
- SWOT and PESTLE
- FIRM risk scorecard risk classification system

Figure 5: Drivers of risk management



- Risk appetite statement
  - Board levels, executive level, operational level
- Risk register
- Monitoring and measuring process

- the measures adopted achieved the intended result
- the procedures adopted were efficient
- sufficient information was available for the risk assessments
- improved knowledge would have helped to reach better decisions
- lessons can be learned for future assessments and controls

- Embedding risk mgmt w/o automatic blame culture
- (Future recommendations):
    - Annual review
        - Risk architecture, strategy, protocols
        - Control risk self assessment
    - External reporting
        - SOX law
    - Stakeholder opinions
- See Appendix A for risk mgmt checklist (p. 17)
- See Appendix B for implementation summary (p. 18)

Reading: Risks of Digitalisation of Business Models (Discussion forum case study)

- FARE method as a Multicriteria decision support method for expert evaluation
- Risk assessment matrix RADi (Risk Assessment of Digitalisation of Business Model)

Reading: NIST 800-30 (2012)

- Frame, assess, respond, monitor risk (p. 4)
- Risk assessment methodology (p. 6)
    - Risk assessment process
    - Explicit risk model
    - An assessment approach
    - An analysis approach
- Threats, threat events, threat scenarios, and TTPs (p. 8), threat shifting (p. 9)
- vulnerability : IS and emergent (p.9)
- “Risk materializes as a result of a series of threat events, each of which takes advantage of one or more vulnerabilities” (10)
    - Group vulnerability analysis more valuable than single vuln in threat scenario
- Predisposing condition – when combined w vulnerability = threat event = adverse events (p. 10)
- Likelihood of occurrence
    - Combines estimate of likelihood that a threat event will be initiated + estimate of likelihood of impact:
        - Adversarial events:
            - Adversary intent

            - Adversary capability
            - Adversary targeting
        - Other TEs:
            - Specific time frame
            - Estimated frequency within timeframe
            - State of the organization
            - Predisposed conditions + presence/effectiveness of sec controls
    - Three step process to determine likelihood (p.11)
- Privacy Impact Assessment (p.11)
- General risk model:

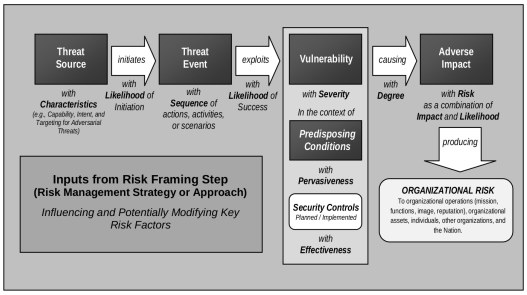


FIGURE 3: GENERIC RISK MODEL WITH KEY RISK FACTORS

- Analysis approach (p. 15)
    - Threat oriented
    - asset/impact oriented
    - Vulnerability oriented
        - Should be two approaches to account for any biases

Reading: Threat Modeling: A Summary of Available Methods

- Summary table (p. 18-19):

Table 3: Threat Modeling Methods Features

Threat Modeling Method	Features
STRIDE	• Helps identify relevant mitigating techniques • Is the most mature • Is easy to use but is time consuming
PASTA	• Helps identify relevant mitigating techniques • Directly contributes to risk management • Encourages collaboration among stakeholders • Contains built-in prioritization of threat mitigation • Is laborious but has rich documentation
LINDDUN	• Helps identify relevant mitigation techniques • Contains built-in prioritization of threat mitigation • Can be labor intensive and time consuming
CVSS	• Contains built-in prioritization of threat mitigation • Has consistent results when repeated • Automated components • Has score calculations that are not transparent
Attack Trees	• Helps identify relevant mitigation techniques • Has consistent results when repeated • Is easy to use if you already have a thorough understanding of the system
Persona non Grata	• Helps identify relevant mitigation techniques • Directly contributes to risk management • Has consistent results when repeated • Tends to detect only some subsets of threats
Security Cards	• Encourages collaboration among stakeholders • Targets out-of-the-ordinary threats • Leads to many false positives

Threat Modeling Method	Features
hTMM	• Contains built-in prioritization of threat mitigation • Encourages collaboration among stakeholders • Has consistent results when repeated
Quantitative TMM	• Contains built-in prioritization of threat mitigation • Has automated components • Has consistent results when repeated
Trike	• Helps identify relevant mitigation techniques • Directly contributes to risk management • Contains built-in prioritization of threat mitigation • Encourages collaboration among stakeholders • Has automated components • Has vague, insufficient documentation
VAST Modeling	• Helps identify relevant mitigation techniques • Directly contributes to risk management • Contains built-in prioritization of threat mitigation • Encourages collaboration among stakeholders • Has consistent results when repeated • Has automated components • Is explicitly designed to be scalable • Has little publicly available documentation
OCTAVE	• Helps identify relevant mitigation techniques • Directly contributes to risk management • Contains built-in prioritization of threat mitigation • Encourages collaboration among stakeholders • Has consistent results when repeated • Is explicitly designed to be scalable • Is time consuming and has vague documentation

Attack trees

Conjunctive and disjunctive refinements are different steps and alternatives to achieve an attacker's goal, respectively. (Qin & Lee, 2004)

Adversarial Tactics, Techniques and Common Knowledge (ATT&CK)

Vulnerabilities, threats, mitigations, cyber-espionage. Tactics:

- Persistence
- Privilege Escalation
- Defense Evasion

- Credential Access
- Discovery
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command and Control

Reference: Data harmonisation as a key to enable digitalisation of the food sector: A review (2021)

- Food sector: pet food
- Food value chain

Prospective harmonisation	Retrospective harmonisation
• Harmonisation before the data collection • Both stringent and flexible approaches • Agreement on identical data collection tools and procedures • Results in standardised and compatible data • Requires huge amounts of time & other resources	• Harmonisation after the data collection • Flexible approach, mostly • Studies choose data collection procedures • Utilisation of available data sources • Quantity of valid data to be harmonised is limited • Relatively modest time and other costs

Fig. 3 – Prospective and retrospective harmonisation.

Impact of digitalisation on value chain

Reference: The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks (2018)

Primary area	*Technology*	*Impact*
Marketing	Website, social network	Product info, advertisement, reputation (e.g. online reviews)

Sales	Website, mobile apps, cloud computing	New information and sales channels, partially automated. Customer prefill details.

Reference: Perceived risks and vulnerabilities of employing digitalization and digital data in agriculture – Socially robust orientations from a transdisciplinary process (2022)

Table 1
Overview of causal factors of digitalization and digital data use for the four identified areas of unseens (unintended side effects). All data refer to possibilities without quantification.

Unseens	Agro-ecological impacts	Data rights and market concentration	Automation, changing knowledge, and decision-making competencies	Food security
Causal factors	Insufficient digitalization – Insufficient exploitation of the potential of digitization Loss of biodiversity – Use of digital data is not optimized to "maximize" biodiversity; – Leveling of soil conditions in arable land and loss of marginal subsites Loss of ecological niches – Trend toward light and smart field robots – Use of previously inaccessible fallow land by means of field robots Soil compaction (soil erosion, unfavorable for water balance and nitrogen losses) – Trend toward larger machines continues Changed resource and ecological balance – Rebound effects due to increased energy and material use Changes in cultural landscapes – Adaptations of the landscape to technologies; – Influence on field sizes; – Loss of fringe structures and niche areas; – Changed field path infrastructures; – Homogenization of management practices leads to decreased diversity in agricultural landscapes	Trend toward the formation of monopolies – Trend toward smaller, more innovative companies being taken over by large companies; – Agreements between a few players (e.g., on interoperability of systems); – Exclusivity of data/market access Farmer's dependence on agricultural and data corporations increases, restricting his/her sovereignty – "Lock-in" effects (poor portability of data); – Uniqueness of services/lack of choice (and freedom of decision) in the market; – Some services linked to data sharing; – Lack of knowledge about (open source) offers Control over the farmer's own data decreases – Lack of exportability of data/lack of control over data/lack of awareness ("farmers actually have the upper hand"?); – Lack of qualification/knowledge to exercise data sovereignty; – Lack of transparency in services	Changed human–machine interactions – System complexity increases and possibilities for intervention become more difficult due to lack of "digital literacy"; – Reduced human intervention; – Importance of human labor decreases; – Work is changing into a form of "automation work" Changed knowledge and judgment skills – Virtualization leads to loss of visual, auditory, and tactile access to events; – "Automation bias" limits decision-making and judgment skills; – Practical knowledge is lost through "disuse" Restrictions at the decision-making level of the farmer – Farm machinery regularly collects data on the farm and passes it on to platform operators; – The farmer becomes transparent, influenceable, and more dependent on the platform operator; – Dependency leads to limited freedom of choice for the farmer, who is bound to the services of the platform operator; – Restricted choice leads to a decrease in diversity in agricultural landscapes	Increasing susceptibility to errors and faults – Increasing complexity of digital systems; – Hacker attacks; – Dependence on external factors increases Monopoly tendencies – Global technology corporations discover agriculture as a field of action; – "Are Microsoft/Amazon able to do agriculture?"; – Collusion among market participants; – No transparency rules "Digital divide" continues to grow – Unequal access to knowledge; – Unequal financial resources; – Global North versus Global South Wrong price signals on/speculation with agricultural commodities – Market prices influence decisions and the farmer's cultivation behaviors; – Digital systems optimize for economic success Decrease in the robustness of the food system – Optimized systems lose redundancy and diversity; – Digital systems optimize for specific crops; – Decrease in diversity of individual management practices

3. Project Notes

Risks:

- Financial risks
    - Risks as is
    - Risks with digitalisation
    - (Economic) Barriers to entry
        - Digitalisation process → cost analysis
            - Advertising
        - Bad reviews
        - Black Swan Theory in Risk Assessment
            - How some small event can demolish entire RA model
- Technical, network risks
    - One network and one work computer with excel
    - Expand w digit.
    - Single point of failure - natural disaster, system compromised, affects downtime
        - Disaster recovery, rate of recovery
    - Customer service
        - Online or by phone?

        - Robot or a human?
    - Website portal
    - Database
    - Warehouse portal
    - Supplier portal
    - Payment transactions
        - Online payment with digitalization
    - Secure network
    - Employee training
    - Hardware security
        - Log-ins
        - Punch cards – digital version
- Operation risks
    - Competition → can destroy business with hacking
    - Digitalisation transition process
        - Hybrid model - Keeping the brick and mortar store
    - Logistics and transport
        - Will it stay local, or will it expand?
            - 50% expansion
            - Costs increase compared to customer increase
            - Delivery logistics
    - Clickbait → can bring a whole company down
    - Open Source Intelligence (OSINT)

Literature reviews:

- Match statistics for growth and decline
- Semi-quantified data
- SME specific
- Pet-food industry
- Risk assessment – business model/risk appetite, etc.
- Dangers and benefits of digitalisation

Meeting with Doug 07/10/2022

- Numbers should be treated qualitatively because they aren't symmetrical data (i.e. comparing apples and oranges)
    - Need a caveat in the report
        - These are qualitative as we don't have access to the raw data
        - This is how we're using them
        - The results indicate that… etc.

- Can have appendix of up to 1000 additional words
    - Use this to explain how we got our Threat Model numbers
        - From DREAD or STRIDE or whatever we use
    - Should show the details behind all risk data/analysis/etc
- The report itself is like an executive summary

    - So, for example,
        - we list the most likely threats in the report
            - The appendix shows how we got to that data
        - We state the usefulness of session mgmt, auth, and access controls for web apps
            - Appendix will have a table of likely attacks/how to mitigate them
- The small details matter
    - Having a separate network, passwords, employee training, etc should all be included
    - Big technical issues aren't necessarily what he's after if the above isn't included

Skimming and scanning papers:

- Go to the methods section and the discussion section
- Look for keywords about your question
- If there are no numbers – no need to read it
- Once you find 3-4 studies with the data, then go for it

Due on Sunday 09/10/2022, 3-4 studies per question:

1. Could an online presence grow the business by up to 50%?
    a. Lee (I've asked Doug about my math, so I may have to change the following)
        i. Gill, M. & VanBoskirk, S. (2016) The Digital Maturity Model 4.0, Forrester
            1. High web maturity: 57% online sales
            2. Low web maturity: 17% online sales
                a. 40% increase
        ii. Hornyak, M, Kruzslicz, F., Lanyi, B. (2021) The effect of online activity on SMEs' competitiveness, 31(3)
            1. No-web: 3.545 competitiveness mean
            2. Web-challenger: 5.567 competitiveness mean
                a. 44% difference
        iii. Capgemini & Salesforce (2019) Lookbook: Elevating the Customer Experience
            1. When implementing a website with a "multifaceted approach" (2)
                a. NYDJ: 33% revenue increase
                b. Chicco: 35% revenue increase
                c. Hibbet: 62% eCommerce sales increase
                d. e.l.f.: 37% revenue increase
                    i. 42% average
2. Could changing to an inter/national supply chain reduce costs by up to 24%?
    a. International: Celine

i. (Giusti et al., 2019) Sustainable and De-Stressed International Supply-Chains Through the SYNCHRO-NET Approach
    1. Cost 27%
    2. Tests performed in the East–West demonstrator
        a. 9% increase in rail
        b. 7% potentiality in implementing import/export pairings
        c. 23% reduction in km traveled by truck
        d. 15% decrease of CO2 emission
        e. 15% reduction in transportation costs
    3. SYNCHRO-NET: “Non-marginal impact in terms of sustainability of the freight transportation process”, and generally international supply chains
ii. (Lancioni, Smith & Schau, 2003) Strategic Internet application trends in supply chain management
    1. 8– 35% reductions in supply chain costs
    2. "The opportunity to take advantage of lower production costs and to source parts and finished goods from international suppliers was enhanced through the increased use of the Internet to coordinate production schedules and supply requirements with domestic and international locations (19.1 –38.4% and 16.4% and 43.6%)."
iii. (John Mathis & Cavinato, 2010) Financing the Global Supply Chain: Growing Need for Management Action
    1. Global supply chain costs (% of sales revenue)
        a. Transport 5.5%
        b. Warehousing 2.8%
        c. Order processing 0.8%
        d. Admin 0.5%
        e. Inventory 2.9%
        f. Trade finance 0.5%
        g. Interest & dividends 10%

b. National: Marios

1. Although without any numbers of cost reduction by 24% found by (Saini, 2020) that B2B e-commerce platforms such as Udaan, Amazon Small Business, and Amazon Seller Services, along with many similar platforms, have extended the reach for SMEs to practically every nook and corner of the country Not only do they provide them with platforms to

showcase their products but also help them with logistics and warehousing as an add-on. All this makes the entire sale and purchase function not only efficient but also cost-effective as economies of scale come into play, which was earlier present just for large players.

Reference

Saini, N.(2020)How SMEs are reducing their business costs and increasing efficiency with technology.Availableat:https://yourstory.com/smbstory/sme-msme-business-cost-technology/amp[Accessed 8 October 2022]

2. Also, in UK, if our pet shop is based, there are serious challenges in the supply chain due to three major issues.

- With the exit of the UK from the EU, A national quarterly survey of SMEs run by the South West Manufacturing Advisory Service (SWMAS), found that the cost of raw materials for some SMEs had increased by up to 350 per cent in some instances. Other companies were facing lead times of up to a year. Reference: Businessgrowthhub (2021) 96% of SME manufacturers struggling with price changes. Available at https://www.businessgrowthhub.com/manufacturing/news/2021/08/96-of-sme-manufacturers-struggling-with-price-changes[Accessed 8 October 2022]

- Lack of Drivers due to covid-19

- The war between Russia and Ukraine has seriously disrupted the global supply chain in every industry resulting in delays in deliveries and scarcity in specific products like pet supplies. My point is that it is not the time to shift to an international supplier.

Source:https://www.petfoodindustry.com/articles/11189-european-pet-food-industry-responds-to-russia-ukraine-war

3. By establishing distribution hubs,standardizing and consolidating stores, enhancing product quality, expanding services offered, shifting away from a focus on low prices, and creating a welcoming in-store environment for customers and their pets, the supply chain has been enhanced (Brennan, 2013).Reference: Brennan, D. (2013) "Case study: PetSmart searches for a sustainable strategy" . Marketing Faculty Publications. 30.University of St. Thomas, Minnesota.http://ir.stthomas.edu/ocbmktgpub/30.

A. People intend to pay more for local food by 95% in preferences. More recently, as of spring 2015, the number of people who said they buy locally grown food amounted to about 82 million, according to Statista. And in 2018, Packaged Facts research showed that 32 per cent of U.S. food shoppers said they seek locally raised or grown foods.

B. For pet food, local sourcing aids in ingredient transparency

C. Elimination of logistics costs and not affected by global crises.

D. Example: Champion company achieved revenue of US$180 million in 2017, according to our Top Pet Food Companies Database, ranking 31st globally.

Source :
Https://www.petfoodindustry.com/blogs/7-adventures-in-pet-food/post/7377-why-local-pet-food-ingredient-sourcing-can-pay-off

3. Could the business lose up to 33% of its existing customers if the business doesn't provide some online features?
    a. Bali - see Assignment Piece document

Managing compliance

- Easily view, sort, and prioritize a Common Vulnerability Scoring System (CVSS) score, and filter impacted supply chain blocks.
- Understand how many and which part of the new system will be affected, and assess the potential risk to the Pet Shop revenue.
- Remediate known CVEs based on business risk and relevance.
- Compare current system profiles to the suggested systems to identify differences and troubleshoot operational issues.
- Generate comma-separated value (CSV) reports to keep relevant stakeholders informed.
- Determine which systems are noncompliant to one or more policies for customers using the purchasing system.
- Determine the percentage of policy compliance. For example, proposed system might be xxx% compliant with the Data protection Act 2018 and only xxxx % compliant with the Payment Card Industry Data Security Standard
- Remediate known issues of noncompliance.