CHAPTER VI
CLOSING

This chapter includes a conclusion of the research that has been done and some suggestions for further research.

6.1 Conclusion

The following conclusions from the research as below.

1. The risks identified in the Information Technology (IT) directorate of Universitas Andalas are 27 risks.
2. Based on the results of risk analysis, it was found that there were 2 risks in the high region, so that they were followed up as prioritized risks, namely the website cannot be accessed due to virus attacks (R14) and the network is disconnected and cannot be accessed by the entire UNAND environment (R18).
3. Through the assessment of the 2 prioritized risks, 19 risk events were identified.
4. Through risk event analysis and evaluation, the highest risk event in the prioritized risks was identified. This highest risk event is further studied which will be carried out risk mitigation strategies. Risk events that are in the high and prevent at source regions are designed risk mitigation strategies. The prioritized risk events are Denial of Service (DoS) attacks flood the network with traffic (E10), the website is infected with malware designed to disrupt the functionality of the website (E1), lack of security updates on software and plugins leaves websites vulnerable (E4), critical hardware failure (E12), and attackers exploit a vulnerability in website SQL injection (E2).
5. The recommended risk mitigation strategy for prioritized risk events, namely E10, E1, E4, E12, and E2 at the Information Technology (IT)

directorate of Universitas Andalas is designed in the form of a risk register, including:

1) Implement a Web Application Firewall (WAF) to detect and block web-based attacks.
2) Conducting regular anti-virus / anti-malware updates to keep up with virus developments
3) Implementation of parameterized queries
4) Ensure strict validation and sanitization of input
5) Establish a regular schedule for security updates and use an automated patch management system
6) Improved defense between users and servers with the implementation of cloud-based DDoS, namely cloudflare magic transit
7) Implementation of redundancy and failover systems

6.2 Suggestion

These are some suggestions for future research.

1. The formulation of risk mitigation strategies is expected for all risk levels.
2. In order to successfully implement the suggested risk mitigations, the Information Technology (IT) directorate of Universitas Andalas will likely face the following challenges based on the designed risk mitigation strategies such as budgetary constraints, ensuring technical expertise, compatibility issues with current systems, ongoing maintenance and updates, user compliance, and overcoming resistance to change through targeted training and awareness programs.
3. In order to observe the suggested risk reduction techniques, it is anticipated that future research will be able to put them into practice, monitor, and review them. It is advised in this study to view the pertinent mitigation suggestions that this organization can implement.