Threat Model for a Large International Bank

1. Identify Assets: Start by identifying the critical assets of the bank, such as customer data, financial transactions, internal systems, servers, applications, and infrastructure.
2. Identify Threats: Refer to the OWASP Threat Modeling Cookbook and the ATTACK libraries to identify potential threats. This may include insider threats, external hacking attempts, social engineering attacks, malware, data breaches, and denial of service attacks.
3. Identify Vulnerabilities: Assess the bank's systems and infrastructure to identify vulnerabilities that could be exploited by the identified threats. This could include outdated software, weak authentication mechanisms, unencrypted data, misconfigured access controls, or poor security awareness training.
4. Rate Risks: Evaluate the potential impact and likelihood of each identified threat exploiting a vulnerability. This will help prioritize risks and allocate resources effectively.
5. Mitigation Strategies: Develop mitigation strategies based on the Threat Modeling Manifesto. This could involve implementing strong access controls, regular patching and updates, secure coding practices, employee training programs, network segmentation, incident response plans, and encryption of sensitive data.
6. Validate and Test: Periodically validate the effectiveness of the implemented security controls by conducting penetration testing, vulnerability assessments, and security audits. This will help identify any new risks or vulnerabilities.
7. Monitor and Evaluate: Continuously monitor the bank's systems and infrastructure for any suspicious activities or anomalies. Implement a robust logging and monitoring system to detect and respond to security incidents promptly.
8. Incident Response: Develop an incident response plan that outlines the steps to be taken in the event of a security breach or incident. This should include procedures for containment, eradication, recovery, and post-incident analysis.
9. Continuous Improvement: Regularly review and update the threat model based on emerging threats, new vulnerabilities, and changes in the bank's infrastructure. This will ensure that the threat model remains relevant and effective over time.

Budget Allocation for Security Controls: Allocate the budget based on the criticality of assets and the risks identified. Consider investing in:

- Robust firewall and intrusion detection/prevention systems

- Secure coding practices and regular code reviews
- Employee training and awareness programs
- Encryption of sensitive data in transit and at rest
- Regular vulnerability assessments and penetration testing
- Incident response and disaster recovery planning
- Security monitoring and logging systems
- Regular updates and patching of software and systems
- Red teaming exercises to test the effectiveness of security controls