**ITN 100 ASSIGNMENT 4 SECTION: 1**

**LAST NAME (capitals) :**

**F NAME**

**EAST VIRGINIA STATE BANK :** Perform a risk assessment. Fill out the control table for East Virginia State Bank

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Fire | Flood | Power loss | Circuit failure | Virus | External intruder | Internal intruder |
| (70) Client computers at branches |  |  |  |  |  |  |  |
| (60) ATMs at branches |  |  |  |  |  |  |  |
| (90) Servers at branches |  |  |  |  |  |  |  |
| (80) Dedicated circuits to central facility |  |  |  |  |  |  |  |
| INTENTIONAL LEFT BLANK | | | | | | | |
| (80) Dial-up circuits |  |  |  |  |  |  |  |
| (60) Branches |  |  |  |  |  |  |  |
| (60) Central computing facility |  |  |  |  |  |  |  |
| (90) Software applications |  |  |  |  |  |  |  |
| (100) Data files |  |  |  |  |  |  |  |

**“SMART-TOYS-SMART KIDS” IS A TOY MANUFACTURING COMPANY.**

They have been providing toys to more than 150 different Toy retail stores in the region. The company has 500 employees and 150 Toy retail stores ( the clients). And conduct B2B transactions between his employees and the Toy retail stores ( the clients). Perform a risk assessment for “Smart-Toys-Smart Kids”. Fill out the control table for the Company

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Fire | Flood | Power loss | Circuit failure | Virus | External intruder | Internal intruder |
| (80) Client computers-sales |  |  |  |  |  |  |  |
| (75) Client computers-warehouse |  |  |  |  |  |  |  |
| (70) Client computers-other |  |  |  |  |  |  |  |
| (90) Internal app server |  |  |  |  |  |  |  |
| (90) E-mail server |  |  |  |  |  |  |  |
| INTENTIONAL LEFT BLANK | | | | | | | |
| (90) Web server |  |  |  |  |  |  |  |
| (80) T-1 circuit |  |  |  |  |  |  |  |
| (80) Wireless circuits |  |  |  |  |  |  |  |
| (60) Branches |  |  |  |  |  |  |  |
| (60) Central computing facility |  |  |  |  |  |  |  |
| (90) Software applications |  |  |  |  |  |  |  |
| (100) Data files |  |  |  |  |  |  |  |

**FOR BOTH CASES USE THE FOLLOWING CONTROL ITEMS**

1. Disaster recovery plan
2. Halon fire system in server room; sprinklers in the rest of building
3. Not on or below ground level
4. UPS (uninterruptible power source )
5. Contract guarantees from interexchange carriers
6. Extra fiber backbone laid in different conduits
7. Virus checking software present and updated
8. Extensive user training about viruses and reminders in monthly newsletter
9. Strong password software
10. Extensive user training about password security and reminders in monthly newsletter
11. Application-layer firewall