|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Vanguard Invest** | | | | | | | | | |
| **Risk Assessment Table** | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |
| **S.No** | **Serial No** | **Item Name** | **Category** | **Value (£)** | **Location** | **Threats** | **Likelihood** | **Impact** | **Risk Level** |
| 1 | Eok4mVHU | F-Web-UKS-1 | Web Server | 5,450 | UK-South-Azure | Unauthorized access, DDoS attacks, Data breaches | Medium | High | High |
| 2 | UXQnEgLh | F-Web-UKS-2 | Web Server | 5,450 | UK-South-Azure | Unauthorized access, DDoS attacks, Data breaches | Medium | High | High |
| 3 | 4NVJa5Yk | F-Web-UKS-3 | Web Server | 5,450 | UK-South-Azure | Unauthorized access, DDoS attacks, Data breaches | Medium | High | High |
| 4 | LaRaeDrU | B-DB-UKS-1 | Database | 14,450 | UK-South-Azure | Unauthorized access, Data breaches | Low | High | Medium |
| 5 | xPR9RSj8 | B-DB-UKS-2 | Database | 14,450 | UK-South-Azure | Unauthorized access, Data breaches | Low | High | Medium |
| 6 | mVkWfvRB | B-DB-UKS-3 | Database | 14,450 | UK-South-Azure | Unauthorized access, Data breaches | Low | High | Medium |
| 7 | 9CUH9E42 | B-App-UKS-1 | Web Server | 6,250 | UK-South-Azure | Unauthorized access, DDoS attacks, Data breaches | Medium | High | High |
| 8 | 5rjTpxac | B-App-UKS-2 | Web Server | 6,250 | UK-South-Azure | Unauthorized access, DDoS attacks, Data breaches | Medium | High | High |
| 9 | R8Bhy6ye | B-App-UKS-3 | Web Server | 6,250 | UK-South-Azure | Unauthorized access, DDoS attacks, Data breaches | Medium | High | High |
| 10 | owNVvo8F | B-LBDB-UKS-1 | Load Balancer | 2,500 | UK-South-Azure | Unauthorized access, DDoS attacks | Low | High | Medium |
| 11 | pwkWs9cm | B-LBApp-UKS-1 | Load Balancer | 2,500 | UK-South-Azure | Unauthorized access, DDoS attacks | Low | High | Medium |
| 12 | U6RUoDwC | F-ALBWeb-UKS-1 | Load Balancer | 2500 | UK-South-Azure | Unauthorized access, DDoS attacks | Low | High | Medium |
| 13 | zuCtPLyx | INT-GW-UKS-1 | Internet Gateway | 1,850 | UK-South-Azure | Network breach | Low | High | Medium |
| 14 | AZ6GofYm | TMGR--UKS-1 | Traffic Manager | 1,500 | UK-South-Azure | Service outage | Medium | Medium | Medium |
| 15 | myiYweEd | VPN-GW-UKS-1 | VPN Gateway | 2,200 | UK-South-Azure | Unauthorized access | Medium | High | High |
| 16 | jTnsiqNg | B-FIA-App-UKS-1 | Finance App | 10,200 | UK-South-Azure | Data breach | High | High | Very High |
| 17 | 7gdUYizC | B-COL-App-UKS-1 | Collaboration App | 8,345 | UK-South-Azure | Data leakage | Medium | Medium | Medium |
| 18 | avDz7PDP | ST&FS-App-UKS-1 | File Sharing App | 12,145 | UK-South-Azure | Malware infection | Low | Medium | Low |
| 19 | DyWF39du | B-CB-App-UKS-1 | Core Banking App | 24,560 | UK-South-Azure | Denial of Service (DoS) | Medium | High | High |
| 20 | kxmvfcvD | B-Mob-App-UKS-1 | Mobile Banking App | 14,679 | UK-South-Azure | Account compromise | High | High | Very High |
| 21 | zJp9NTjK | B-PAY-App-UKS-1 | Payment Processing App | 38,450 | UK-South-Azure | Fraudulent transactions | Medium | High | High |
| 22 | kqKbxMmB | F-Web-UKW-1 | Web Server | 5,450 | UK-West-Azure | Website defacement | Low | Medium | Low |
| 23 | KvWFaE9Z | F-Web-UKW-2 | Web Server | 5,450 | UK-West-Azure | Data loss | Medium | Medium | Medium |
| 24 | WKFJ4ZAc | F-Web-UKW-3 | Web Server | 5,450 | UK-West-Azure | Server compromise | Medium | High | High |
| 25 | QuyZBPDL | B-DB-UKW-1 | Database | 14,450 | UK-West-Azure | Data breach | Medium | High | High |
| 26 | VohMEkW9 | B-DB-UKW-2 | Database | 14,450 | UK-West-Azure | Unauthorized access | Low | High | Medium |
| 27 | 4btMVnfu | B-DB-UKW-3 | Database | 14,450 | UK-West-Azure | Data corruption | Low | Medium | Low |
| 28 | 7iprCpRv | B-App-UKW-1 | Web Server | 6,250 | UK-West-Azure | Service outage | Medium | Medium | Medium |
| 29 | oWwAqyWm | B-App-UKW-2 | Web Server | 6,250 | UK-West-Azure | Data loss | Low | High | Medium |
| 30 | tSz99RU9 | B-App-UKW-3 | Web Server | 6,250 | UK-West-Azure | Server compromise | Medium | High | High |
| 31 | b5qRn8x9 | B-LBDB-UKW-1 | Load Balancer | 2,500 | UK-West-Azure | Configuration error | Low | Medium | Low |
| 32 | ya94aEvL | B-LBApp-UKW-1 | Load Balancer | 2,500 | UK-West-Azure | DDoS attack | Medium | High | High |
| 33 | atrcp7Ct | F-ALBWeb-UKW-1 | Load Balancer | 2,500 | UK-West-Azure | Traffic overload | Medium | Medium | Medium |
| 34 | DuzPxSDE | INT-GW-UKW-1 | Internet Gateway | 1,850 | UK-West-Azure | Network breach | Low | High | Medium |
| 35 | 2pi7BUd5 | TMGR--UKW-1 | Traffic Manager | 1,500 | UK-West-Azure | Service outage | Medium | Medium | Medium |
| 36 | SMVHNcWR | VPN-GW-UKW-1 | VPN Gateway | 2,200 | UK-West-Azure | Unauthorized access | Medium | High | High |
| 37 | MXoicd9U | B-FIA-App-UKW-1 | Finance App | 10,200 | UK-West-Azure | Data breach | High | High | Very High |
| 38 | gjDB9tBe | B-COL-App-UKW-1 | Collaboration App | 8,345 | UK-West-Azure | Data leakage | Medium | Medium | Medium |
| 39 | vsVvVJWS | ST&FS-App-UKW-1 | File Sharing App | 12,145 | UK-West-Azure | Malware infection | Low | Medium | Low |
| 40 | YZuR24G6 | B-CB-App-UKW-1 | Core Banking App | 24,560 | UK-West-Azure | Unauthorized access | Medium | High | High |
| 41 | Pkt7tZAc | B-Mob-App-UKW-1 | Mobile Banking App | 14,679 | UK-West-Azure | Account compromise | High | High | Very High |
| 42 | asgcqv3e | B-PAY-App-UKW-1 | Payment Processing App | 38,450 | UK-West-Azure | Fraudulent transactions | Medium | High | High |
| 43 | TvXtvYXm | INT-FW-LON-1 | Firewall/VPN Gateway | 1,850 | HO-London | Network breach | Low | High | Medium |
| 44 | VRtchReQ | SW-ACC-LON-1 | Switch - 96 Port | 2,400 | HO-London | Hardware failure | Low | Medium | Low |
| 45 | Ke3wdGan | SW-ACC-LON-2 | Switch - 96 Port | 2,400 | HO-London | Power outage | Low | Medium | Low |
| 46 | uyUs5wYu | SW-ACC-LON-3 | Switch - 96 Port | 2,400 | HO-London | Configuration error | Low | Low | Low |
| 47 | zhKkocpT | SW-ACC-LON-4 | Switch - 96 Port | 2,400 | HO-London | Physical damage | Low | High | Medium |
| 48 | swVxiKEM | SW-ACC-LON-5 | Switch - 96 Port | 2,400 | HO-London | Software vulnerability | Medium | Low | Low |
| 49 | chSaAhud | AP-ACC-LON-1 | WiFi Access Point | 800 | HO-London | Signal interference | Low | Medium | Low |
| 50 | jrSZsqBb | AP-ACC-LON-2 | WiFi Access Point | 800 | HO-London | Unauthorized access | Low | High | Medium |
| 51 | BNPy92Ww | AP-ACC-LON-3 | WiFi Access Point | 800 | HO-London | Signal interference | Low | Medium | Low |
| 52 | 9PA4ZKc7 | AP-ACC-LON-4 | WiFi Access Point | 800 | HO-London | Unauthorized access | Low | High | Medium |
| 53 | EZSVNvSm | AP-ACC-LON-5 | WiFi Access Point | 800 | HO-London | Malicious activity | Medium | Medium | Medium |
| 54 | y24mABFG | INT-FW-MAN-1 | Firewall/VPN Gateway | 1,850 | REG-Manchester | Network breach | Low | High | Medium |
| 55 | CTLAFfrp | SW-ACC-MAN-1 | Switch - 96 Port | 2,400 | REG-Manchester | Hardware failure | Low | Medium | Low |
| 56 | N7z8KRT2 | AP-ACC-MAN-1 | WiFi Access Point | 800 | REG-Manchester | Unauthorized access | Low | High | Medium |
| 57 | wNPPzbBt | INT-FW-LVR-1 | Firewall/VPN Gateway | 1,850 | REG-Liverpool | Network breach | Low | High | Medium |
| 58 | qHjCv5ag | SW-ACC-LVR-1 | Switch - 96 Port | 2,400 | REG-Liverpool | Power outage | Low | Medium | Low |
| 59 | 7Grk6jwN | AP-ACC-LVR-1 | WiFi Access Point | 800 | REG-Liverpool | Configuration error | Low | Low | Low |
| 60 | 33Qgufhj | INT-FW-LED-1 | Firewall/VPN Gateway | 1,850 | REG-Leeds | Unauthorized access | Low | High | Medium |
| 61 | MrBmkDfz | SW-ACC-LED-1 | Switch - 96 Port | 2,400 | REG-Leeds | Software vulnerability | Medium | Low | Low |
| 62 | Y2RdPFY3 | AP-ACC-LED-1 | WiFi Access Point | 800 | REG-Leeds | Signal interference | Low | Medium | Low |
| 63 | 655wuNAQ | INT-FWAP-1 | Firewall/VPN/Access Point | 950 | BR1 | Network breach | Medium | High | High |
| 64 | S3naLEmZ | INT-FWAP-2 | Firewall/VPN/Access Point | 950 | BR2 | Network breach | Medium | High | High |
| 65 | uzTgoLup | INT-FWAP-3 | Firewall/VPN/Access Point | 950 | BR3 | Network breach | Medium | High | High |
| 66 | EDqDuBdj | INT-FWAP-4 | Firewall/VPN/Access Point | 950 | BR4 | Network breach | Medium | High | High |
| 67 | 4xbzJ2wp | INT-FWAP-5 | Firewall/VPN/Access Point | 950 | BR5 | Network breach | Medium | High | High |
| 68 | mnaBXGGd | INT-FWAP-6 | Firewall/VPN/Access Point | 950 | BR6 | Network breach | Medium | High | High |
| 69 | kZR9Yzq9 | INT-FWAP-7 | Firewall/VPN/Access Point | 950 | BR7 | Network breach | Medium | High | High |
| 70 | KC8TUj3H | INT-FWAP-8 | Firewall/VPN/Access Point | 950 | BR8 | Network breach | Medium | High | High |
| 71 | wS8GQVJz | INT-FWAP-9 | Firewall/VPN/Access Point | 950 | BR9 | Network breach | Medium | High | High |
| 72 | wLSASV3F | INT-FWAP-10 | Firewall/VPN/Access Point | 950 | BR10 | Network breach | Medium | High | High |
| 73 | jbQDdXmY | INT-FWAP-11 | Firewall/VPN/Access Point | 950 | BR11 | Network breach | Medium | High | High |
| 74 | rR25t4Zk | INT-FWAP-12 | Firewall/VPN/Access Point | 950 | BR12 | Network breach | Medium | High | High |
| 75 | m7xZpWEf | INT-FWAP-13 | Firewall/VPN/Access Point | 950 | BR13 | Network breach | Medium | High | High |
| 76 | rcaba5dS | INT-FWAP-14 | Firewall/VPN/Access Point | 950 | BR14 | Network breach | Medium | High | High |
| 77 | T7sxbN8h | INT-FWAP-15 | Firewall/VPN/Access Point | 950 | BR15 | Network breach | Medium | High | High |
| 78 | 6zNFe7Ma | INT-FWAP-16 | Firewall/VPN/Access Point | 950 | BR16 | Network breach | Medium | High | High |
| 79 | 2CrfMKqs | INT-FWAP-17 | Firewall/VPN/Access Point | 950 | BR17 | Network breach | Medium | High | High |
| 80 | 7hDzCfhE | INT-FWAP-18 | Firewall/VPN/Access Point | 950 | BR18 | Network breach | Medium | High | High |
| 81 | S4Wd4mpc | INT-FWAP-19 | Firewall/VPN/Access Point | 950 | BR19 | Network breach | Medium | High | High |
| 82 | NTmP6f2f | INT-FWAP-20 | Firewall/VPN/Access Point | 950 | BR20 | Network breach | Medium | High | High |
| 83 | 9TLKLxqX | INT-FWAP-21 | Firewall/VPN/Access Point | 950 | BR21 | Network breach | Medium | High | High |
| 84 | xtUSYvN6 | INT-FWAP-22 | Firewall/VPN/Access Point | 950 | BR22 | Network breach | Medium | High | High |
| 85 | FvbQbVyZ | INT-FWAP-23 | Firewall/VPN/Access Point | 950 | BR23 | Network breach | Medium | High | High |
| 86 | XUuurfaf | INT-FWAP-24 | Firewall/VPN/Access Point | 950 | BR24 | Network breach | Medium | High | High |
| 87 | 6UmveGps | INT-FWAP-25 | Firewall/VPN/Access Point | 950 | BR25 | Network breach | Medium | High | High |
| 88 | sGRXaaWk | INT-FWAP-26 | Firewall/VPN/Access Point | 950 | BR26 | Network breach | Medium | High | High |
| 89 | 6cG5L26D | INT-FWAP-27 | Firewall/VPN/Access Point | 950 | BR27 | Network breach | Medium | High | High |
| 90 | MMa2Ur32 | INT-FWAP-28 | Firewall/VPN/Access Point | 950 | BR28 | Network breach | Medium | High | High |
| 91 | dYfBRjvB | INT-FWAP-29 | Firewall/VPN/Access Point | 950 | BR29 | Network breach | Medium | High | High |
| 92 | fkdKiBgm | INT-FWAP-30 | Firewall/VPN/Access Point | 950 | BR30 | Network breach | Medium | High | High |
| 93 | aCkuAUss | INT-FWAP-31 | Firewall/VPN/Access Point | 950 | BR31 | Network breach | Medium | High | High |
| 94 | ZqcFJiM8 | INT-FWAP-32 | Firewall/VPN/Access Point | 950 | BR32 | Network breach | Medium | High | High |
| 95 | S7irgK4u | INT-FWAP-33 | Firewall/VPN/Access Point | 950 | BR33 | Network breach | Medium | High | High |
| 96 | twjg9SR7 | INT-FWAP-34 | Firewall/VPN/Access Point | 950 | BR34 | Network breach | Medium | High | High |
| 97 | k44Gn9vs | INT-FWAP-35 | Firewall/VPN/Access Point | 950 | BR35 | Network breach | Medium | High | High |
| 98 | CgiUF8XY | INT-FWAP-36 | Firewall/VPN/Access Point | 950 | BR36 | Network breach | Medium | High | High |
| 99 | UgG2TrdL | INT-FWAP-37 | Firewall/VPN/Access Point | 950 | BR37 | Network breach | Medium | High | High |
| 100 | URiFeG3c | INT-FWAP-38 | Firewall/VPN/Access Point | 950 | BR38 | Network breach | Medium | High | High |
| 101 | m6qjtb9L | INT-FWAP-39 | Firewall/VPN/Access Point | 950 | BR39 | Network breach | Medium | High | High |
| 102 | C5dcFg8S | INT-FWAP-40 | Firewall/VPN/Access Point | 950 | BR40 | Network breach | Medium | High | High |
| 103 | BQfZifu6 | INT-FWAP-41 | Firewall/VPN/Access Point | 950 | BR41 | Network breach | Medium | High | High |
| 104 | QdQjJT5m | INT-FWAP-42 | Firewall/VPN/Access Point | 950 | BR42 | Network breach | Medium | High | High |
| 105 | oKftiXha | INT-FWAP-43 | Firewall/VPN/Access Point | 950 | BR43 | Network breach | Medium | High | High |
| 106 | arZ8oo8n | INT-FWAP-44 | Firewall/VPN/Access Point | 950 | BR44 | Network breach | Medium | High | High |
| 107 | HnrQcyfB | INT-FWAP-45 | Firewall/VPN/Access Point | 950 | BR45 | Network breach | Medium | High | High |
| 108 | NA | HP-Win10 x 500 | Laptop | 525,000 | HO-London | Theft, data breach,Hardware failure, Malware attack,physical damage | Low | High | Medium |
| 109 | NA | HP-Win10 x 45 | Laptop | 47,250 | REG-Manchester | Theft, data breach,Hardware failure, Malware attack,physical damage | Low | High | Medium |
| 110 | NA | HP-Win10 x 45 | Laptop | 47,250 | REG-Liverpool | Theft, data breach,Hardware failure, Malware attack,physical damage | Low | High | Medium |
| 111 | NA | HP-Win10 x 45 | Laptop | 47,250 | REG-Leeds | Theft, data breach,Hardware failure, Malware attack,physical damage | Low | High | Medium |
| 112 | NA | HP-Win10 x 100 | Laptop | 105,000 | Remote | Theft, data breach,Hardware failure, Malware attack,physical damage | Low | High | Medium |