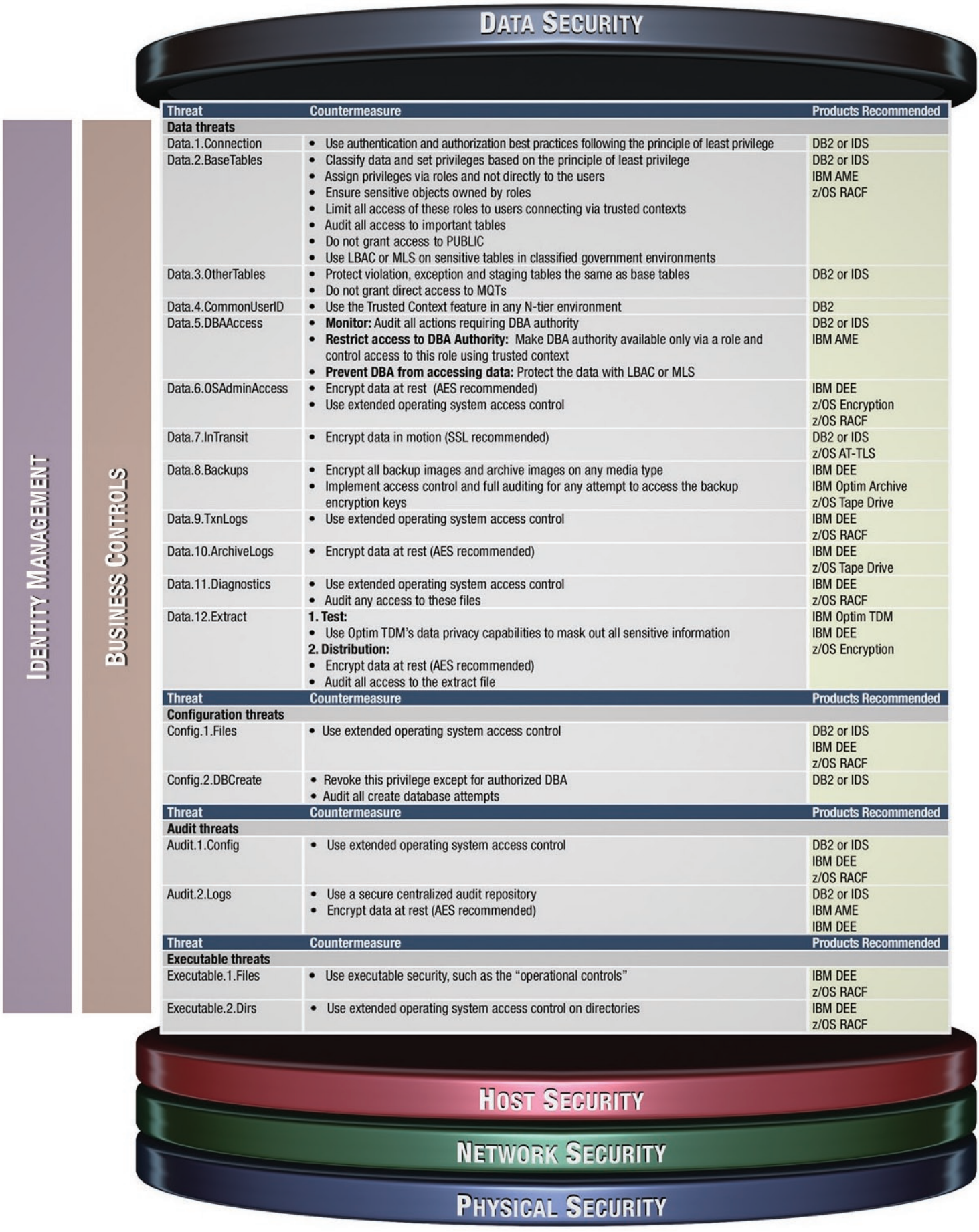

Threat	Countermeasure	Products Recommended
Data threats		
Data.1.Connection	• Use authentication and authorization best practices following the principle of least privilege	DB2 or IDS
Data.2.BaseTables	• Classify data and set privileges based on the principle of least privilege • Assign privileges via roles and not directly to the users • Ensure sensitive objects owned by roles • Limit all access of these roles to users connecting via trusted contexts • Audit all access to important tables • Do not grant access to PUBLIC • Use LBAC or MLS on sensitive tables in classified government environments	DB2 or IDS IBM AME z/OS RACF
Data.3.OtherTables	• Protect violation, exception and staging tables the same as base tables • Do not grant direct access to MQTs	DB2 or IDS
Data.4.CommonUserID	• Use the Trusted Context feature in any N-tier environment	DB2
Data.5.DBAAccess	• **Monitor:** Audit all actions requiring DBA authority • **Restrict access to DBA Authority:** Make DBA authority available only via a role and control access to this role using trusted context • **Prevent DBA from accessing data:** Protect the data with LBAC or MLS	DB2 or IDS IBM AME
Data.6.OSAdminAccess	• Encrypt data at rest (AES recommended) • Use extended operating system access control	IBM DEE z/OS Encryption z/OS RACF
Data.7.InTransit	• Encrypt data in motion (SSL recommended)	DB2 or IDS z/OS AT-TLS
Data.8.Backups	• Encrypt all backup images and archive images on any media type • Implement access control and full auditing for any attempt to access the backup encryption keys	IBM DEE IBM Optim Archive z/OS Tape Drive
Data.9.TxnLogs	• Use extended operating system access control	IBM DEE z/OS RACF
Data.10.ArchiveLogs	• Encrypt data at rest (AES recommended)	IBM DEE z/OS Tape Drive
Data.11.Diagnostics	• Use extended operating system access control • Audit any access to these files	IBM DEE z/OS RACF
Data.12.Extract	**1. Test:** • Use Optim TDM's data privacy capabilities to mask out all sensitive information **2. Distribution:** • Encrypt data at rest (AES recommended) • Audit all access to the extract file	IBM Optim TDM IBM DEE z/OS Encryption
Threat	**Countermeasure**	**Products Recommended**
Configuration threats		
Config.1.Files	• Use extended operating system access control	DB2 or IDS IBM DEE z/OS RACF
Config.2.DBCreate	• Revoke this privilege except for authorized DBA • Audit all create database attempts	DB2 or IDS
Threat	**Countermeasure**	**Products Recommended**
Audit threats		
Audit.1.Config	• Use extended operating system access control	DB2 or IDS IBM DEE z/OS RACF
Audit.2.Logs	• Use a secure centralized audit repository • Encrypt data at rest (AES recommended)	DB2 or IDS IBM AME IBM DEE
Threat	**Countermeasure**	**Products Recommended**
Executable threats		
Executable.1.Files	• Use executable security, such as the "operational controls"	IBM DEE z/OS RACF
Executable.2.Dirs	• Use extended operating system access control on directories	IBM DEE z/OS RACF