FLANK

PROTECTING YOUR PERIMETER

FRAMEWORK MAPPING

HITRUST CSF V9 TO ISO 27001/27002:2013

Visit us online at Flank.org to learn more.

HITRUST CSF v9 Framework	ISO 27001/27002:2013 Framework	FLANK ISO 27001/27002:2013 Documentation from ISO our all-in-one toolkit
04.a Information Security Policy Document 05.a Management Commitment to Information Security	ISO/IEC 27002:2013 5.1.1	**5.1.1 -** Policies for Information Security Policy and Procedures (5 pages)
04.b Review of the Information Security Policy	ISO/IEC 27002:2013 5.1.2	**5.1.2 -** Review of the Policies for Information Security Policy and Procedures (5 pages)
02.a Roles and Responsibilities 02.g Termination or Change Responsibilities 05.c Allocation of Information Security Responsibilities	ISO/IEC 27002:2013 6.1.1	**6.1.1 -** Information Security Roles and Responsibilities Policy and Procedures (5 pages)
09.c Segregation of Duties	ISO/IEC 27002:2013 6.1.2	**6.1.2 -** Segregation of Duties Policy and Procedures (5 pages)
05.c Allocation of Information Security Responsibilities 05.f Contact with Authorities	ISO/IEC 27002:2013 6.1.3	**6.1.3 -** Contact with Authorities Policy and Procedures (4 pages)
05.g Contact with Special Interest Groups 06.a Identification of Applicable Legislation	ISO/IEC 27002:2013 6.1.4	**6.1.4 -** Contact with Special Interest Groups Policy and Procedures (4 pages)
01.x Mobile Computing and Communications 01.y Teleworking 08.k Security of Equipment Off-Premises	ISO/IEC 27002:2013 6.2.1	**6.2.1 -** Mobile Device Policy and Procedures (6 pages)
01.y Teleworking 08.k Security of Equipment Off-Premises	ISO/IEC 27002:2013 6.2.2	**6.2.2 -** Teleworking Policy and Procedures (8 pages)
02.b Screening 05.k Addressing Security in Third Party Agreements	ISO/IEC 27002:2013 7.1.1	**7.1.1 -** Employee and Contractor Screening Policy and Procedures (5 pages)
02.a Roles and Responsibilities 02.c Terms and Conditions of Employment	ISO/IEC 27002:2013 7.1.2	**7.1.2 -** Terms of Conditions and Employment Policy and Procedures (4 pages)
02.d Management Responsibilities 11.a Reporting Information Security Events	ISO/IEC 27002:2013 7.2.1	**7.2.1 -** Management Responsibilities Policy and Procedures (4 pages)

01.p Secure Log-on Procedures 02.e Information Security Awareness, Education, and Training 06.a Identification of Applicable Legislation 11.a Reporting Information Security Events	ISO/IEC 27002:2013 7.2.2	**7.2.2 -** Information Security Awareness, Education and Training Policy and Procedures (8 pages)
02.f Disciplinary Process	ISO/IEC 27002:2013 7.2.3	**7.2.3 -** Information Security Sanction & Disciplinary Process Policy and Procedures – Personal Data (EU) (6 pages) **7.2.3 -** Information Security Sanction & Disciplinary Process Policy and Procedures – Personally Identifiable Information (PII) (7 pages)
02.g Termination or Change Responsibilities	ISO/IEC 27002:2013 7.3.1	**7.3.1 -** Termination/Change of Employment Responsibilities Policy and Procedures (4 pages)
07.a Inventory of Assets 07.d Classification Guidelines	ISO/IEC 27002:2013 8.1.1	**8.1.1 - 8.1.2 -** Inventory and Ownership of Assets Policy and Procedures (4 pages)
07.b Ownership of Assets 07.d Classification Guidelines	ISO/IEC 27002:2013 8.1.2	**8.1.1 - 8.1.2 -** Inventory and Ownership of Assets Policy and Procedures (4 pages)
07.c Acceptable Use of Assets	ISO/IEC 27002:2013 8.1.3	**8.1.3 -** Information System Usage Policy and Procedures (5 pages) **8.1.3 -** Internet Usage Policy and Procedures (5 pages) **8.1.3 -** Laptop Usage Policy and Procedures (6 pages) **8.1.3 -** Software Usage Policy and Procedures (6 pages)
02.h Return of Assets	ISO/IEC 27002:2013 8.1.4	**8.1.4 -** Return of Assets Policy and Procedures (4 pages)
06.c Protection of Organizational Records 07.d Classification Guidelines	ISO/IEC 27002:2013 8.2.1	**8.2.1 - 8.2.3 -** Data and Information Classification Policy and Procedures (18 pages)
07.e Information Labeling and Handling	ISO/IEC 27002:2013 8.2.2	**8.2.1 - 8.2.3 -** Data and Information Classification Policy and Procedures (18 pages)
01.h Clear Desk and Clear Screen Policy 07.e Information Labeling and Handling 09.q Information Handling Procedures	ISO/IEC 27002:2013 8.2.3	**8.2.1 - 8.2.3 -** Data and Information Classification Policy and Procedures (18 pages)

09.o Management of Removable Media	ISO/IEC 27002:2013 8.3.1	**8.3.1 - 8.3.3 -** Removable Media Policy and Procedures (7 pages)
09.p Disposal of Media	ISO/IEC 27002:2013 8.3.2	**8.3.1 - 8.3.3 -** Removable Media Policy and Procedures (7 pages)
09.u Physical Media in Transit	ISO/IEC 27002:2013 8.3.3	**8.3.1 - 8.3.3 -** Removable Media Policy and Procedures (7 pages)
01.a Access Control Policy 01.c Privilege Management	ISO/IEC 27002:2013 9.1.1	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
01.a Access Control Policy 01.i Policy on the Use of Network Services	ISO/IEC 27002:2013 9.1.2	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
08.d Protecting Against External and Environmental Threats	ISO/IEC 27002:2013 9.1.4	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
01.a Access Control Policy 01.b User Registration 01.q User Identification and Authentication	ISO/IEC 27002:2013 9.2.1	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
01.a Access Control Policy 01.b User Registration	ISO/IEC 27002:2013 9.2.2	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
01.a Access Control Policy 01.c Privilege Management 01.q User Identification and Authentication	ISO/IEC 27002:2013 9.2.3	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
01.d User Password Management 01.r Password Management System	ISO/IEC 27002:2013 9.2.4	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
01.e Review of User Access Rights 02.g Termination or Change Responsibilities	ISO/IEC 27002:2013 9.2.5	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
02.g Termination or Change Responsibilities 02.i Removal of Access Rights	ISO/IEC 27002:2013 9.2.6	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
01.d User Password Management 01.f Password Use	ISO/IEC 27002:2013 9.3.1	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
01.v Information Access Restriction	ISO/IEC 27002:2013 9.4.1	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
01.d User Password Management 01.p Secure Log-on Procedures 01.t Session Time-out 01.u Limitation of Connection Time	ISO/IEC 27002:2013 9.4.2	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
01.d User Password Management 01.r Password Management System	ISO/IEC 27002:2013 9.4.3	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
01.s Use of System Utilities	ISO/IEC 27002:2013 9.4.4	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)

10.j Access Control to Program Source Code	ISO/IEC 27002:2013 9.4.5	**9.1 - 9.4.5 -** Access Control Policy and Procedures (22 pages)
10.d Message Integrity 10.f Policy on the Use of Cryptographic Controls	ISO/IEC 27002:2013 10.1.1	**10.1.1 - 10.1.2 -** Cryptography Policy and Procedures (17 pages)
10.g Key Management	ISO/IEC 27002:2013 10.1.2	**10.1.1 - 10.1.2 -** Cryptography Policy and Procedures (17 pages)
09.o Management of Removable Media	ISO/IEC 27002:2013 10.7.1	**8.3.1 - 8.3.3 -** Removable Media Policy and Procedures (7 pages)
08.a Physical Security Perimeter 08.b Physical Entry Controls	ISO/IEC 27002:2013 11.1.1	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)
08.b Physical Entry Controls	ISO/IEC 27002:2013 11.1.2	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)
08.c Securing Offices, Rooms, and Facilities	ISO/IEC 27002:2013 11.1.3	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)
08.d Protecting Against External and Environmental Threats 08.g Equipment Siting and Protection	ISO/IEC 27002:2013 11.1.4	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)
08.e Working in Secure Areas	ISO/IEC 27002:2013 11.1.5	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)
08.f Public Access, Delivery, and Loading Areas	ISO/IEC 27002:2013 11.1.6	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)
08.g Equipment Siting and Protection 08.h Supporting Utilities 08.h Supporting Utilities	ISO/IEC 27002:2013 11.2.1	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)
12.c Developing and Implementing Continuity Plans Including Information Security	ISO/IEC 27002:2013 11.2.2	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)
08.i Cabling Security	ISO/IEC 27002:2013 11.2.3	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)
08.h Supporting Utilities 08.j Equipment Maintenance	ISO/IEC 27002:2013 11.2.4	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)
08.m Removal of Property	ISO/IEC 27002:2013 11.2.5	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)
08.a Physical Security Perimeter 08.k Security of Equipment Off-Premises	ISO/IEC 27002:2013 11.2.6	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)
08.l Secure Disposal or Re-Use of Equipment	ISO/IEC 27002:2013 11.2.7	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)

01.g Unattended User Equipment	ISO/IEC 27002:2013 11.2.8	**11.1.1 - 11.2.8 -** Physical and Environmental Security Policy and Procedures (16 pages)
01.h Clear Desk and Clear Screen Policy	ISO/IEC 27002:2013 11.2.9	**11.2.9 -** Clear Desk and Clear Screen Policy and Procedures (5 pages)
09.a Documented Operations Procedures	ISO/IEC 27002:2013 12.1.1	**12.1.1 -** Documented Operating Policy and Procedures (4 pages)
03.d Risk Evaluation 09.b Change Management 09.d Separation of Development, Test, and Operational Environments	ISO/IEC 27002:2013 12.1.2	**12.1.2 -** Change Management Policy and Procedures (13 pages)
09.h Capacity Management	ISO/IEC 27002:2013 12.1.3	**12.1.3 -** Capacity Management Plan Policy and Procedures (6 pages)
09.d Separation of Development, Test, and Operational Environments	ISO/IEC 27002:2013 12.1.4	**12.1.4 -** Separation of Development, Testing, and Operational Environments Policy and Procedures (6 pages)
09.j Controls Against Malicious Code 09.k Controls Against Mobile Code	ISO/IEC 27002:2013 12.2.1	**12.2.1 -** Malware Policy and Procedures (9 pages)
09.l Back-up	ISO/IEC 27002:2013 12.3.1	**12.3.1 -** Information Backup Policy and Procedures (10 pages)
09.aa Audit Logging 09.ab Monitoring System Use 09.ad Administrator and Operator Logs 09.ae Fault Logging	ISO/IEC 27002:2013 12.4.1	**12.4.1 - 12.4.3 -** Logging and Monitoring Policy and Procedures (10 pages)
09.aa Audit Logging 09.ac Protection of Log Information	ISO/IEC 27002:2013 12.4.2	**12.4.1 - 12.4.3 -** Logging and Monitoring Policy and Procedures (10 pages)
09.aa Audit Logging 09.ac Protection of Log Information 09.ad Administrator and Operator Logs	ISO/IEC 27002:2013 12.4.3	**12.4.1 - 12.4.3 -** Logging and Monitoring Policy and Procedures (10 pages)
09.af Clock Synchronization	ISO/IEC 27002:2013 12.4.4	**12.4.4 -** Clock Synchronization Policy and Procedures (4 pages)
09.k Controls Against Mobile Code 10.h Control of Operational Software	ISO/IEC 27002:2013 12.5.1	**12.5.1 -** Installation of Software Policy and Procedures (5 pages)
03.b Performing Risk Assessments 03.c Risk Mitigation 10.m Control of Technical Vulnerabilities	ISO/IEC 27002:2013 12.6.1	**12.6.1 -** Vulnerability Management Policy and Procedures (21 pages)
09.j Controls Against Malicious Code	ISO/IEC 27002:2013 12.6.2	**12.6.2 -** Software Usage Policy and Procedures (6 pages)
03.c Risk Mitigation 06.i Information Systems Audit Controls 06.j Protection of Information Systems Audit Tools	ISO/IEC 27002:2013 12.7.1	**12.7.1 -** Information System Audit Controls Policy and Procedures (5 pages)

09.m Network Controls	ISO/IEC 27002:2013 13.1.1	**13.1.1 -** Network Controls Policy and Procedures (5 pages)
09.f Monitoring and Review of Third Party Services 09.m Network Controls 09.n Security of Network Services	ISO/IEC 27002:2013 13.1.2	**13.1.2 -** Security of Network Services Policy and Procedures (4 pages)
01.m Segregation in Networks 01.o Network Routing Control 09.m Network Controls 09.w Interconnected Business Information Systems	ISO/IEC 27002:2013 13.1.3	**13.1.3 -** Segregation in Networks Policy and Procedures (5 pages)
09.s Information Exchange Policies and Procedures	ISO/IEC 27002:2013 13.2.1	**13.2.1 -** Information Transfer Policy and Procedures (6 pages)
09.t Exchange Agreements	ISO/IEC 27002:2013 13.2.2	**13.2.2 -** Agreements on Information Transfer Policy and Procedures (6 pages)
09.v Electronic Messaging	ISO/IEC 27002:2013 13.2.3	**13.2.3 -** Electronic Mail (E-Mail) and Electronic Messaging Policy and Procedures (6 pages)
05.e Confidentiality Agreements	ISO/IEC 27002:2013 13.2.4	**13.2.4 -** Confidentiality/Non-Disclosure Agreements Policy and Procedures (4 pages)
10.a Security Requirements Analysis and Specification	ISO/IEC 27002:2013 14.1.1	**14.1.1 - 14.3.1 -** System Acquisition, Development, and Maintenance Policy and Procedures (16 pages)
05.j Addressing Security When Dealing with Customers 09.x Electronic Commerce Services 09.z Publicly Available Information	ISO/IEC 27002:2013 14.1.2	**14.1.1 - 14.3.1 -** System Acquisition, Development, and Maintenance Policy and Procedures (16 pages)
09.y On-line Transactions	ISO/IEC 27002:2013 14.1.3	**14.1.1 - 14.3.1 -** System Acquisition, Development, and Maintenance Policy and Procedures (16 pages)
10.a Security Requirements Analysis and Specification	ISO/IEC 27002:2013 14.2.1	**14.1.1 - 14.3.1 -** System Acquisition, Development, and Maintenance Policy and Procedures (16 pages)
09.i System Acceptance 10.k Change Control Procedures	ISO/IEC 27002:2013 14.2.2	**14.1.1 - 14.3.1 -** System Acquisition, Development, and Maintenance Policy and Procedures (16 pages)
10.k Change Control Procedures	ISO/IEC 27002:2013 14.2.3	**14.1.1 - 14.3.1 -** System Acquisition, Development, and Maintenance Policy and Procedures (16 pages)
10.k Change Control Procedures	ISO/IEC 27002:2013 14.2.4	**14.1.1 - 14.3.1 -** System Acquisition, Development, and Maintenance Policy and Procedures (16 pages)
10.a Security Requirements Analysis and Specification 10.e Output Data Validation	ISO/IEC 27002:2013 14.2.5	**14.1.1 - 14.3.1 -** System Acquisition, Development, and Maintenance Policy and Procedures (16 pages)
10.a Security Requirements Analysis and Specification 10.k Change Control Procedures	ISO/IEC 27002:2013 14.2.6	**14.1.1 - 14.3.1 -** System Acquisition, Development, and Maintenance Policy and Procedures (16 pages)

10.k Change Control Procedures 10.l Outsourced Software Development	ISO/IEC 27002:2013 14.2.7	**14.1.1 - 14.3.1 -** System Acquisition, Development, and Maintenance Policy and Procedures (16 pages)
10.a Security Requirements Analysis and Specification	ISO/IEC 27002:2013 14.2.8	**14.1.1 - 14.3.1 -** System Acquisition, Development, and Maintenance Policy and Procedures (16 pages)
09.i System Acceptance	ISO/IEC 27002:2013 14.2.9	**14.1.1 - 14.3.1 -** System Acquisition, Development, and Maintenance Policy and Procedures (16 pages)
10.i Protection of System Test Data	ISO/IEC 27002:2013 14.3.1	**14.1.1 - 14.3.1 -** System Acquisition, Development, and Maintenance Policy and Procedures (16 pages)
05.i Identification of Risks Related to External Parties 05.k Addressing Security in Third Party Agreements 09.e Service Delivery	ISO/IEC 27002:2013 15.1.1	**15.1.1 – 15.2.2 -** Supplier Relationships (Third-Party Due Diligence & Vendor Management Program (52 pages)
05.i Identification of Risks Related to External Parties 05.k Addressing Security in Third Party Agreements	ISO/IEC 27002:2013 15.1.2	**15.1.1 – 15.2.2 -** Supplier Relationships (Third-Party Due Diligence & Vendor Management Program (52 pages)
05.i Identification of Risks Related to External Parties 05.k Addressing Security in Third Party Agreements	ISO/IEC 27002:2013 15.1.3	**15.1.1 – 15.2.2 -** Supplier Relationships (Third-Party Due Diligence & Vendor Management Program (52 pages)
09.l Back-up	ISO/IEC 27002:2013 15.2	**15.1.1 – 15.2.2 -** Supplier Relationships (Third-Party Due Diligence & Vendor Management Program (52 pages)
09.e Service Delivery 09.f Monitoring and Review of Third Party Services	ISO/IEC 27002:2013 15.2.1	**15.1.1 – 15.2.2 -** Supplier Relationships (Third-Party Due Diligence & Vendor Management Program (52 pages)
09.g Managing Changes to Third Party Services	ISO/IEC 27002:2013 15.2.2	**15.1.1 – 15.2.2 -** Supplier Relationships (Third-Party Due Diligence & Vendor Management Program (52 pages)
11.a Reporting Information Security Events 11.c Responsibilities and Procedures 11.e Collection of Evidence	ISO/IEC 27002:2013 16.1.1	**15.1.1 – 15.2.2 -** Supplier Relationships (Third-Party Due Diligence & Vendor Management Program (52 pages)
11.a Reporting Information Security Events	ISO/IEC 27002:2013 16.1.2	**15.1.1 – 15.2.2 -** Supplier Relationships (Third-Party Due Diligence & Vendor Management Program (52 pages)
11.a Reporting Information Security Events 11.b Reporting Security Weaknesses 11.c Responsibilities and Procedures	ISO/IEC 27002:2013 16.1.3	**15.1.1 – 15.2.2 -** Supplier Relationships (Third-Party Due Diligence & Vendor Management Program (52 pages)
11.a Reporting Information Security Events	ISO/IEC 27002:2013 16.1.4	**15.1.1 – 15.2.2 -** Supplier Relationships (Third-Party Due Diligence & Vendor Management Program (52 pages)

11.c Responsibilities and Procedures	ISO/IEC 27002:2013 16.1.5	**15.1.1 – 15.2.2 -** Supplier Relationships (Third-Party Due Diligence & Vendor Management Program (52 pages)
11.a Reporting Information Security Events 11.c Responsibilities and Procedures 11.d Learning from Information Security Incidents	ISO/IEC 27002:2013 16.1.6	**15.1.1 – 15.2.2 -** Supplier Relationships (Third-Party Due Diligence & Vendor Management Program (52 pages)
07.e Information Labeling and Handling 11.e Collection of Evidence	ISO/IEC 27002:2013 16.1.7	**15.1.1 – 15.2.2 -** Supplier Relationships (Third-Party Due Diligence & Vendor Management Program (52 pages)
03.b Performing Risk Assessments 03.c Risk Mitigation 12.b Business Continuity and Risk Assessment	ISO/IEC 27002:2013 17.1.1	**17.1 - 17.2.1 -** Business Continuity and Disaster Recovery Planning (BCDRP) Policy and Procedures (44 pages)
12.a Including Information Security in the Business Continuity Management Process 12.b Business Continuity and Risk Assessment 12.c Developing and Implementing Continuity Plans Including Information Security 12.d Business Continuity Planning Framework	ISO/IEC 27002:2013 17.1.2	**17.1 - 17.2.1 -** Business Continuity and Disaster Recovery Planning (BCDRP) Policy and Procedures (44 pages)
12.e Testing, Maintaining and Re-Assessing Business Continuity Plans	ISO/IEC 27002:2013 17.1.3	**17.1 - 17.2.1 -** Business Continuity and Disaster Recovery Planning (BCDRP) Policy and Procedures (44 pages)
10.a Security Requirements Analysis and Specification	ISO/IEC 27002:2013 17.2.1	**17.1 - 17.2.1 -** Business Continuity and Disaster Recovery Planning (BCDRP) Policy and Procedures (44 pages)
06.a Identification of Applicable Legislation 06.f Regulation of Cryptographic Controls	ISO/IEC 27002:2013 18.1.1	**18.1.1 –** Identification of Applicable Legislation and Contractual Requirements Policy and Procedures (4 pages)
06.b Intellectual Property Rights 06.f Regulation of Cryptographic Controls	ISO/IEC 27002:2013 18.1.2	**18.1.2 –** Intellectual Property Rights Policy and Procedures (5 pages)
06.c Protection of Organizational Records 06.d Data Protection and Privacy of Covered Information 06.f Regulation of Cryptographic Controls 09.l Back-up	ISO/IEC 27002:2013 18.1.3	**18.1.3 -** Data Retention, Disposal, and Protection of Records Policy and Procedures (10 pages)
06.d Data Protection and Privacy of Covered Information 06.f Regulation of Cryptographic Controls	ISO/IEC 27002:2013 18.1.4	**18.1.4 -** Personally Identifiable Information (PII) Policy and Procedures (11 pages)
06.f Regulation of Cryptographic Controls	ISO/IEC 27002:2013 18.1.5	**18.1.5 -** Regulation of Cryptographic Controls Policy and Procedures (4 pages)
05.a Management Commitment to Information Security 05.h Independent Review of Information Security	ISO/IEC 27002:2013 18.2.1	**18.2.1 -** Independent Review of Information Security Policy and Procedures (5 pages)

06.g Compliance with Security Policies and Standards 06.h Technical Compliance Checking	ISO/IEC 27002:2013 18.2.2	**18.2.2 -** Compliance with Security Policies and Standards Policy and Procedures (5 pages)
06.g Compliance with Security Policies and Standards 06.h Technical Compliance Checking	ISO/IEC 27002:2013 18.2.3	**18.2.3 -** Technical Compliance Review Policy and Procedures (5 pages)

Total Number of Pages: Approximately 569+ Pages

Disclaimer: FLANK provides a wide-range of security, governance and regulatory compliance services and solutions as requested by healthcare organizations who contact us in need of assistance. At times, such assistance may include professional recommendations/advice for internal controls relating to HITRUST compliance that are based on ISO 27001/27002 publications and/or the actual CSF guidelines. Such recommendations are only offered when a client provides us with relevant HITRUST documentation for which they have accessed from https://hitrustalliance.net/, and then provided to FLANK. Because FLANK is not a HITRUST assessor, we do not access the HITRUST portal at https://hitrustalliance.net/. Additionally, our documentation, the ISO 27001/27002:2013 All-in-One Toolkit, contains proprietary, copyrighted information that was developed independent from any input from the HITRUST CSF, rather, exclusively by FLANK personnel who have years of relevant ISO 27k expertise. FLANK does not endorse, promote HITRUST, and FLANK is not affiliated in any manner with HITRUST.

ABOUT US

We're global experts when it comes to security, governance, and compliance solutions, there's no debating that, and we can help you implement efficient and scalable solutions for your growing business. Security can be difficult, compliance can be challenging, and governance can be costly – we more than understand these issues – and it's why you should be talking to Flank, the organization that helps you in "protecting your perimeter".

WE'RE FLANK. **"TO DEFEND OR GUARD AT THE FLANK".**

Looking for more information? Get in touch with us at info@flank.org