

CIS, NIST 800-53, ISO27000 - Mapping Leading Control Frameworks to FAIR-CAM™

Moderator: **Jack Jones**, Chairman, FAIR Institute

Daniel Stone, Associate Director, Security & Privacy, Protiviti

Erin Macuga, Manager Risk and Information Security, Thrivent Financial

Robert Immella, Global Leader of Cyber Risk Quantification, Caterpillar Inc

Tyler Britton, Quantitative Cyber Risk Manager, DropBox

Drew Brown, Information System Security Developer, FAA

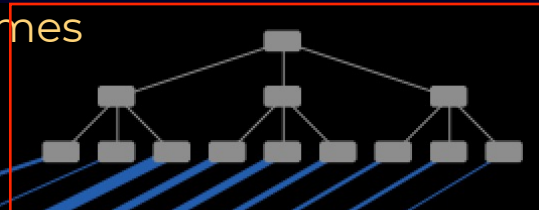
NIST-CSF

FAIR-CAM Control Function Names

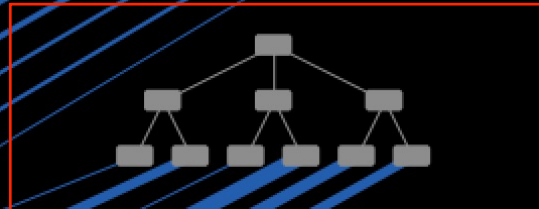
Mappings

ID.AM-1	PR.IP-3	RC.RP-1
ID.AM-2	PR.IP-4	RC.IM-1
ID.AM-3	PR.IP-5	RC.IM-2
ID.AM-4	PR.IP-6	RC.CO-1
ID.AM-5	PR.IP-7	RC.CO-2
ID.AM-6	PR.IP-8	RC.CO-3
ID.BE-1	PR.IP-9	
ID.BE-2	PR.IP-10	
ID.BE-3	PR.IP-11	
ID.BE-4	PR.IP-12	
ID.BE-5	PR.MA-1	
ID.CV-1	PR.MA-2	
ID.CV-2	PR.PT-1	
ID.CV-3	PR.PT-2	
ID.CV-4	PR.PT-3	
ID.RA-1	PR.PT-4	
ID.RA-2	PR.PT-5	
ID.RA-3	DE.AE-1	
ID.RA-4	DE.AE-2	
ID.RA-5	DE.AE-3	
ID.RA-6	DE.AE-4	
ID.RM-1	DE.AE-5	
ID.RM-2	DE.CM-1	
ID.RM-3	DE.CM-2	
ID.SC-1	DE.CM-3	
ID.SC-2	DE.CM-4	
ID.SC-3	DE.CM-5	
ID.SC-4	DE.CM-6	
ID.SC-5	DE.CM-7	
PR.AC-1	DE.CM-8	
PR.AC-2	DE.DP-1	
PR.AC-3	DE.DP-2	
PR.AC-4	DE.DP-3	
PR.AC-5	DE.DP-4	
PR.AC-6	DE.DP-5	
PR.AC-7	RS.RP-1	
PR.AT-1	RS.CO-1	
PR.AT-2	RS.CO-2	
PR.AT-3	RS.CO-3	
PR.AT-4	RS.CO-4	
PR.AT-5	RS.CO-5	
PR.DS-1	RS.AN-1	
PR.DS-2	RS.AN-2	
PR.DS-3	RS.AN-3	
PR.DS-4	RS.AN-4	
PR.DS-5	RS.AN-5	
PR.DS-6	RS.MI-1	
PR.DS-7	RS.MI-2	
PR.DS-8	RS.MI-3	
PR.IP-1	RS.IM-1	
PR.IP-2	RS.IM-2	

- Avoidance
- Deterrence
- Resistance
- Visibility
- Monitoring
- Recognition
- Event Termination
- Resilience
- Loss Minimization
- Reduce Change Frequency
- Reduce Variance Probability
- Threat Monitoring
- Controls Monitoring
- Prioritization
- Implementation
- Identify Misaligned Decisions
- Define Expectations & Objectives
- Communicate Expectations & Objectives
- Ensure Capability
- Incentives
- Analysis
- Reporting
- Asset Data
- Threat Data
- Control Data



Loss Event Control Model



Variance Management Control Model



Decision Support Control Model

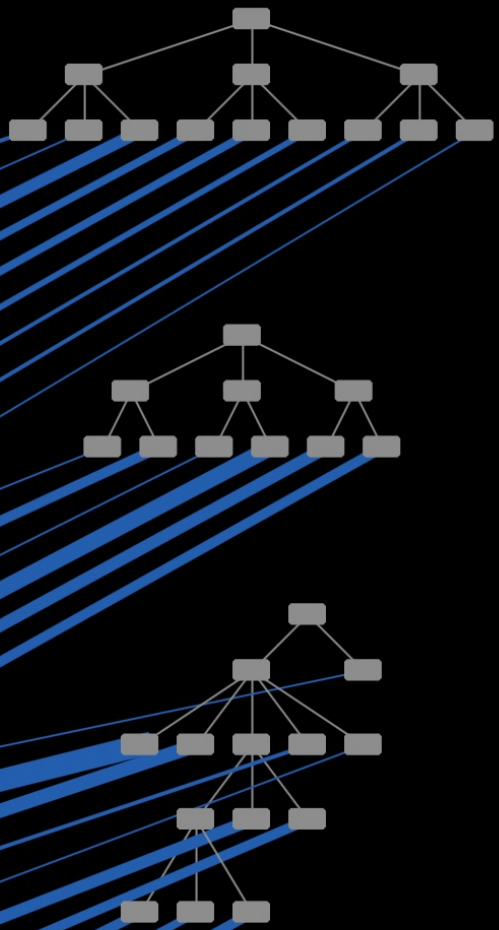
Volume of mappings by control function

NIST-CSF

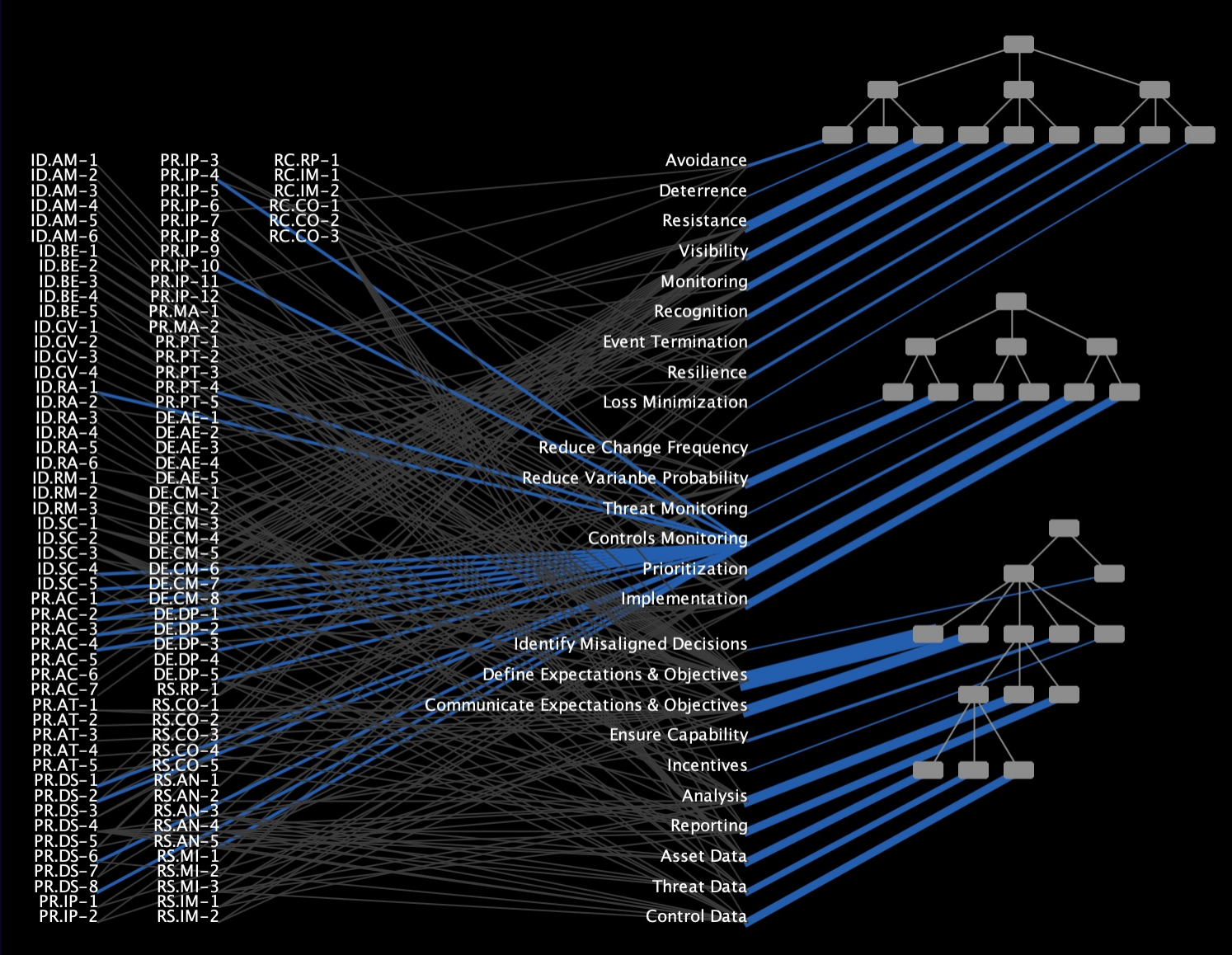
As discussed, many controls affect risk if multiple ways.

- ID.AM-1
- ID.AM-2
- ID.AM-3
- ID.AM-4
- ID.AM-5
- ID.AM-6
- ID.BE-1
- ID.BE-2
- ID.BE-3
- ID.BE-4
- ID.BE-5
- ID.GV-1
- ID.GV-2
- ID.GV-3
- ID.GV-4
- ID.RA-1
- ID.RA-2
- ID.RA-3
- ID.RA-4
- ID.RA-5
- ID.RA-6
- ID.RM-1
- ID.RM-2
- ID.RM-3
- ID.SC-1
- ID.SC-2
- ID.SC-3
- ID.SC-4
- ID.SC-5
- PR.AC-1
- PR.AC-2
- PR.AC-3
- PR.AC-4
- PR.AC-5
- PR.AC-6
- PR.AC-7
- PR.AT-1
- PR.AT-2
- PR.AT-3
- PR.AT-4
- PR.AT-5
- PR.DS-1
- PR.DS-2
- PR.DS-3
- PR.DS-4
- PR.DS-5
- PR.DS-6
- PR.DS-7
- PR.DS-8
- PR.IP-1
- PR.IP-2
- PR.IP-3
- PR.IP-4
- PR.IP-5
- PR.IP-6
- PR.IP-7
- PR.IP-8
- PR.IP-9
- PR.IP-10
- PR.IP-11
- PR.IP-12
- PR.MA-1
- PR.MA-2
- PR.PT-1
- PR.PT-2
- PR.PT-3
- PR.PT-4
- PR.PT-5
- DE.AE-1
- DE.AE-2
- DE.AE-3
- DE.AE-4
- DE.AE-5
- DE.CM-1
- DE.CM-2
- DE.CM-3
- DE.CM-4
- DE.CM-5
- DE.CM-6
- DE.CM-7
- DE.CM-8
- DE.DP-1
- DE.DP-2
- DE.DP-3
- DE.DP-4
- DE.DP-5
- RS.RP-1
- RS.CO-1
- RS.CO-2
- RS.CO-3
- RS.CO-4
- RS.CO-5
- RS.AN-1
- RS.AN-2
- RS.AN-3
- RS.AN-4
- RS.AN-5
- RS.MI-1
- RS.MI-2
- RS.MI-3
- RS.IM-1
- RS.IM-2
- RC.RP-1
- RC.IM-1
- RC.IM-2
- RC.CO-1
- RC.CO-2
- RC.CO-3

- Avoidance
- Deterrence
- Resistance
- Visibility
- Monitoring
- Recognition
- Event Termination
- Resilience
- Loss Minimization
- Reduce Change Frequency
- Reduce Variance Probability
- Threat Monitoring
- Controls Monitoring
- Prioritization
- Implementation
- Identify Misaligned Decisions
- Define Expectations & Objectives
- Communicate Expectations & Objectives
- Ensure Capability
- Incentives
- Analysis
- Reporting
- Asset Data
- Threat Data
- Control Data

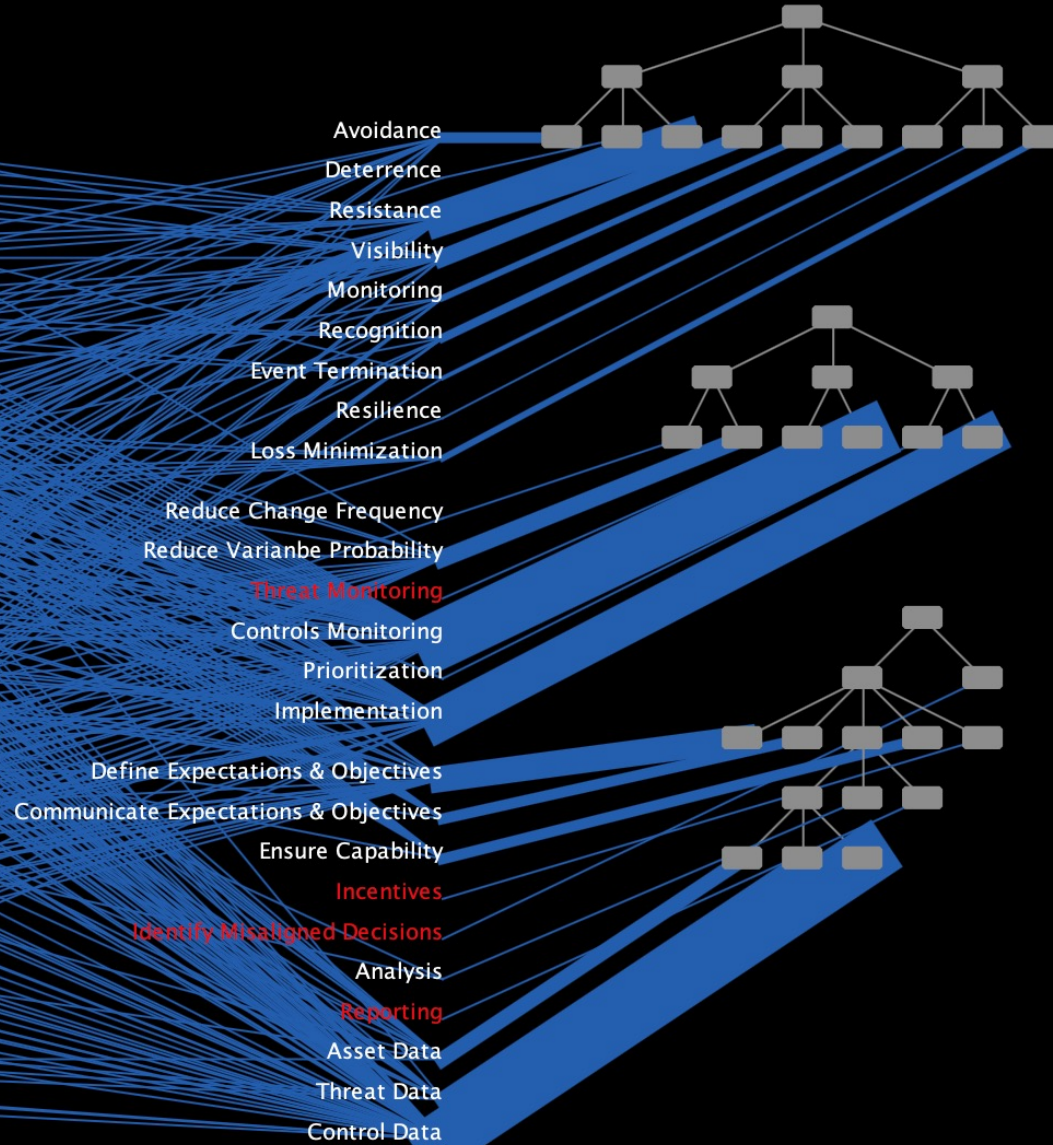


NIST-CSF



CIS Controls

1.1	6.8	13.5
1.2	7.1	13.6
1.3	7.2	13.7
1.4	7.3	13.8
1.5	7.4	13.9
2.1	7.5	13.1
2.2	7.6	13.11
2.3	7.7	14.1
2.4	8.1	14.2
2.5	8.2	14.3
2.6	8.3	14.4
2.7	8.4	14.5
3.1	8.5	14.6
3.2	8.6	14.7
3.3	8.7	14.8
3.4	8.8	14.9
3.5	8.9	15.1
3.6	8.1	15.2
3.7	8.11	15.3
3.8	8.12	15.4
3.9	9.1	15.5
3.1	9.2	15.6
3.11	9.3	15.7
3.12	9.4	16.1
3.13	9.5	16.2
3.14	9.6	16.3
4.1	9.7	16.4
4.2	10.1	16.5
4.3	10.2	16.6
4.4	10.3	16.7
4.5	10.4	16.8
4.6	10.5	16.9
4.7	10.6	16.1
4.8	10.7	16.11
4.9	11.1	16.12
4.11	11.2	16.13
4.11	11.3	16.14
4.12	11.4	17.1
5.1	11.5	17.2
5.2	12.1	17.3
5.3	12.2	17.4
5.4	12.3	17.5
5.5	12.4	17.6
5.6	12.5	17.7
6.1	12.6	17.8
6.2	12.7	17.9
6.3	12.8	18.1
6.4	13.1	18.2
6.5	13.2	18.3
6.6	13.3	18.4
6.7	13.4	18.5



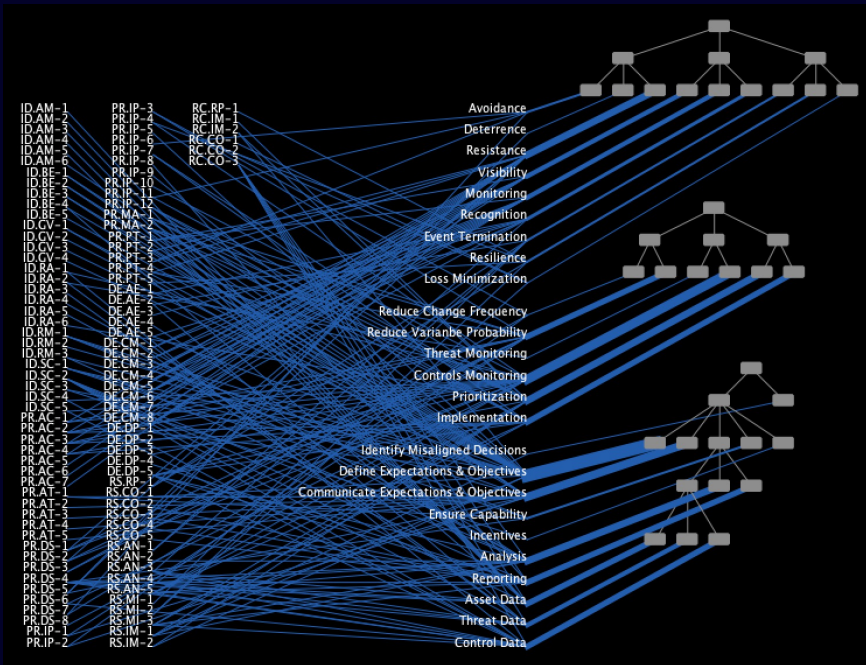
Mitre Mitigations

M1036
M1015
M1049
M1013
M1048
M1047
M1040
M1046
M1045
M1043
M1053
M1057
M1042
M1055
M1041
M1039
M1038
M1050
M1037
M1035
M1034
M1033
M1032
M1031
M1030
M1028
M1027
M1056
M1026
M1025
M1029
M1022
M1044
M1024
M1021
M1054
M1020
M1019
M1051
M1052
M1018
M1017
M1016

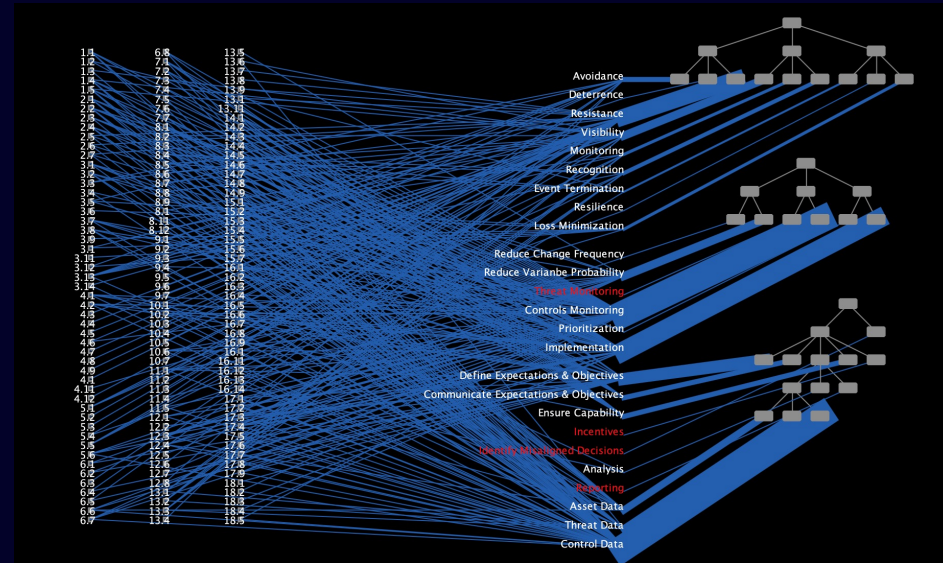
Avoidance
Deterrence
Resistance
Visibility
Monitoring
Recognition
Event Termination
Resilience
Loss Minimization
Reduce Change Frequency
Reduce Variance Probability
Threat Monitoring
Controls Monitoring
Prioritization
Implementation
Define Expectations & Objectives
Communicate Expectations & Objectives
Ensure Capability
Incentives
Identify Misaligned Decisions
Analysis
Reporting
Asset Data
Threat Data
Control Data



NIST CSF



CIS Controls



Mitre Mitigations

