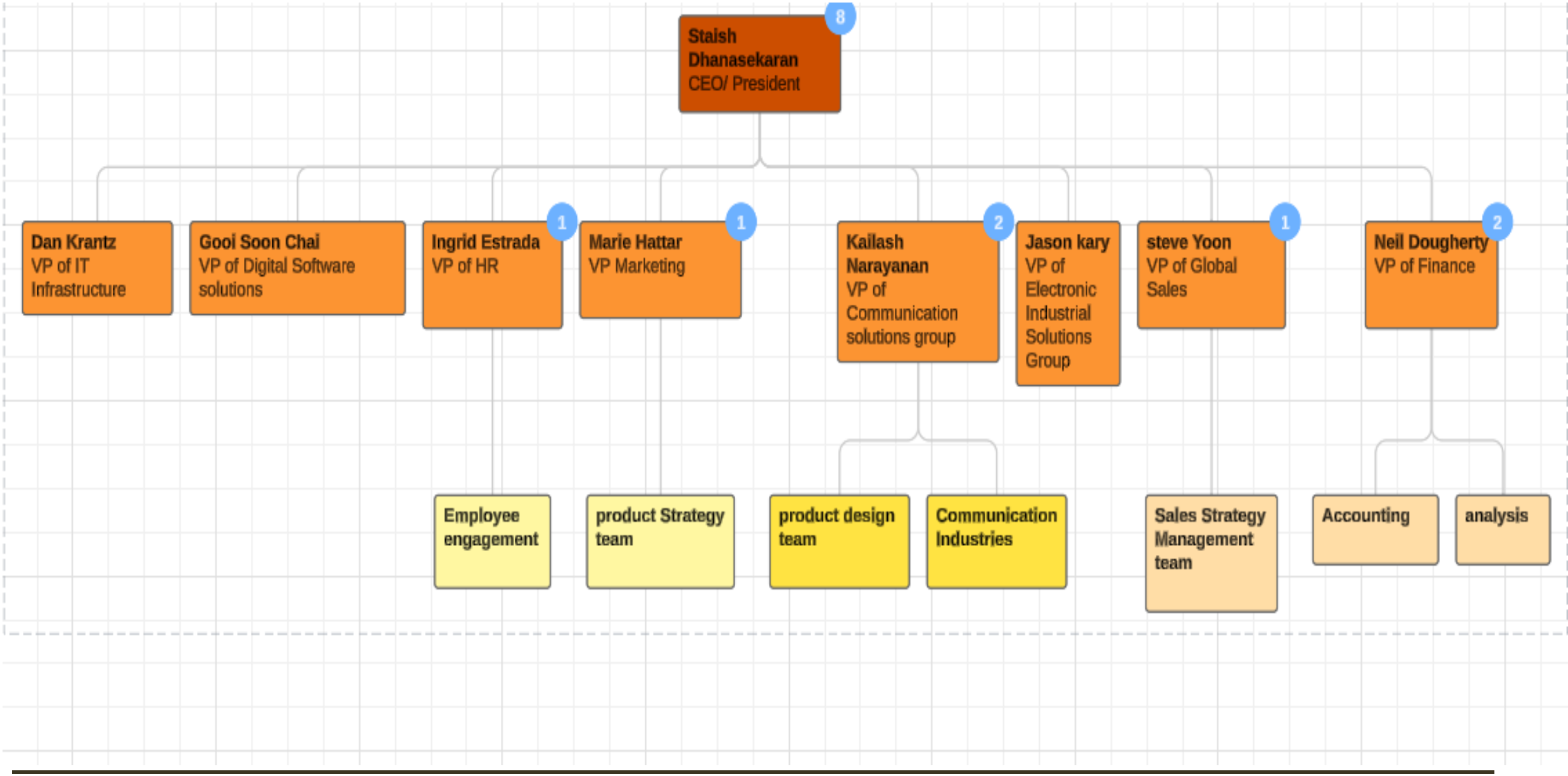
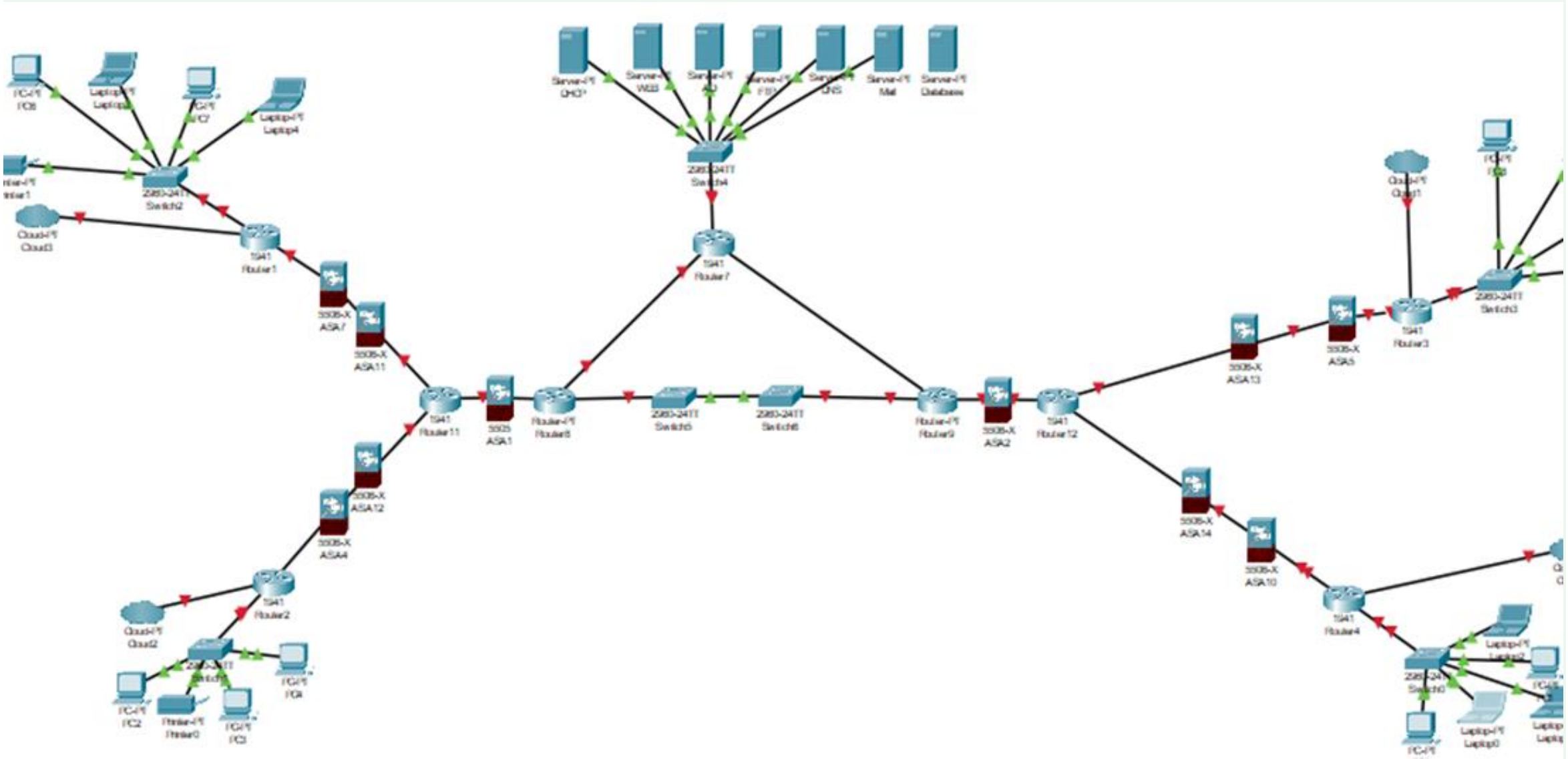
Keysight technologies

Lojain Idris
Glory Imo
Joshua Quick

Company profile

- Keysight Technologies specializes in innovative electronics test and measurement equipment and provides electronic design and test solutions for various industries.
- headquarter: Santa Rosa, California, USA.
- Industry: Electronics, Test, and Measurment solutions.


Staish Dhanasekaran
CEO/ President
8
Dan Krantz
VP of IT Infrastructure
Gooi Soon Chai
VP of Digital Software solutions
Ingrid Estrada
VP of HR
1
Marie Hattar
VP Marketing
1
Kailash Narayanan
VP of Communication solutions group
2
Jason kary
VP of Electronic Industrial Solutions Group
steve Yoon
VP of Global Sales
1
Neil Dougherty
VP of Finance
2
Employee engagement
product Strategy team
product design team
Communication Industries
Sales Strategy Management team
Accounting
analysis


Server-PT
DHCP
Server-PT
WEB
Server-PT
AD
Server-PT
FTP
Server-PT
DNS
Server-PT
Mail
Server-PT
Database
2960-24TT
Switch4
1941
Router7
PC-PT
PC0
Laptop-PT
Laptop1
PC-PT
PC1
Laptop-PT
Laptop4
2960-24TT
Switch2
Cloud-PT
Cloud0
1941
Router1
5505-X
ASA7
5505-X
ASA11
1941
Router11
5505
ASA1
Router-PT
Router8
2960-24TT
Switch5
2960-24TT
Switch6
Router-PT
Router9
5505-X
ASA2
1941
Router12
5505-X
ASA13
5505-X
ASA5
Cloud-PT
Cloud1
1941
Router3
PC-PT
PC4
2960-24TT
Switch3
5505-X
ASA12
5505-X
ASA4
1941
Router2
Cloud-PT
Cloud2
PC-PT
PC2
Printer-PT
Printer0
PC-PT
PC3
PC-PT
PC5
5505-X
ASA14
5505-X
ASA10
1941
Router4
Laptop-PT
Laptop2
Laptop-PT
Laptop0
PC-PT

Control Family Implementation

Awareness and Training (AT):

AT-2: Regularly train employees on basic security concepts and threat identification.

AT-4: Use a Learning Management System (LMS) to track training progress, certifications, and deadlines, with automatic notifications for overdue courses.

Identification and Authorization (IA):

IA-1: Enforce multi-factor authentication (MFA) for sensitive data access and require MFA enrollment within 30 days of employment.

IA-2: Deploy Mobile Device Management (MDM) software to authenticate and secure devices accessing company resources.

Personnel Security (PS):

PS-3: Perform thorough background checks on all employees, particularly those handling sensitive data.

PS-4: Implement an offboarding process to revoke system access, retrieve devices, and conduct exit interviews.

Incident Response (IR):

IR-2: Provide quarterly incident response training, simulating cyber threats.

IR-3: Conduct tabletop exercises and penetration testing to evaluate response plans and identify gaps.

System and Communications Protection (SC):

SC-3: Isolate critical security functions on separate network segments to prevent unauthorized access.

SC-4: Use encryption and strict access controls for shared resources to protect sensitive data.

PII Processing and Transparency (PT):

PT-3: Define and document the purposes for collecting PII, notifying users of changes.

PT-4: Implement a double opt-in process for PII consent, allowing users to withdraw consent and maintaining records.

Risk Assessment (RA):

RA-1: Enforce an annual risk assessment policy to identify and mitigate security risks.

RA-2: Categorize systems using NIST SP 800-60, applying security controls based on system classification.

Implemnting security

Incident Response (IR):

IR-2: Monitor & report suspicious activities with SIEM tools through all servers and endpoints

IR-4: Contain/mitigate incidents using EDR across all laptops& NIPS solutions to perimeter.

Maintenance (MA):

MA-4: Log remote sessions with PAM tools to data center.

MA-5: Track personnel via RBAC in IAM systems to switches, servers, firewalls.

Media Protection (MP):

MP-4: Track media with DAM software to data center.

MP-7: Use encryption & DLP systems for sensitive data to network endpoints

Physical/Environmental Protection (PE):

PE-3: Install PACS for access logs in server room.

PE-10: Use UPS & emergency switches for power control.

Planning (PL):

PL-2: Secure policies in encrypted document systems.

PL-8: Use FWs & redundant backups for security.

Program Management (PM):

PM-8: Oversee systems with GRC tools .

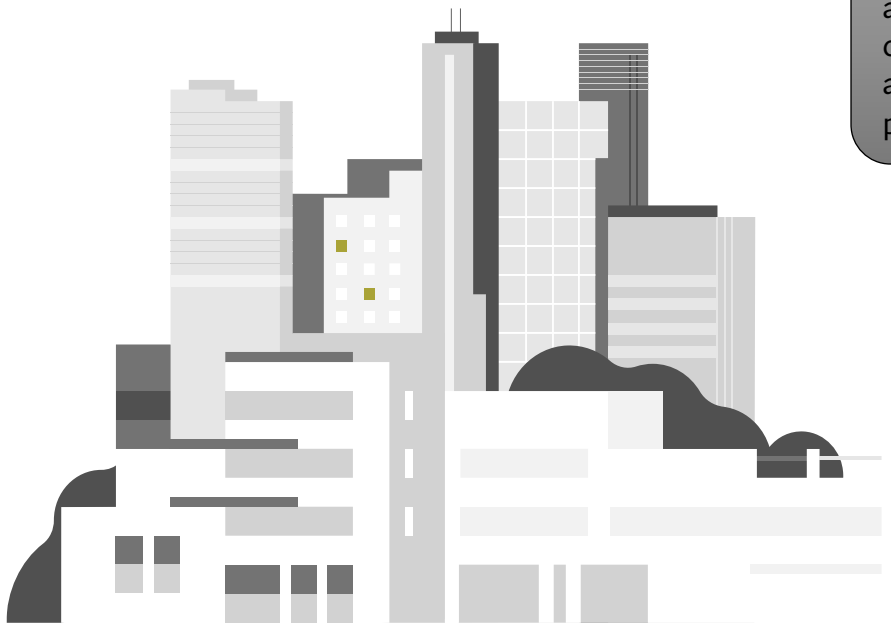
PM-11: Audit tools& update critical devices

Securing Critical Systems for Business Continuity

PM-8/ PM-9: Essential systems are prioritized & secured to minimize downtime, protect intellectual property, and enable rapid recovery aligned with business goals

SI-2: Quickly identifies and patches risk in proprietary software and systems, supporting security during and after recovery.

SI-4: Continuously monitors systems for anomalies, enabling rapid detection and response to accidents during disaster recovery



SA-4: Embeds security in acquiring systems and services, ensuring disaster recovery tools and backup solutions meet safety standards.

SA-9: Defines security requirements for third- party services like cloud storage or offsite recovery facilities, reducing risk during recovery operations.

RA-3: Identifies operational risks, such as supply chain vulnerabilities or cyber-attacks, to prioritize mitigation strategies in disaster planning.

RA-5: Regularly scans systems for weaknesses, ensuring recovery systems and backups are secure and reliable.

PE-3: Ensures only authorized personnel access critical facilities like R&D labs and data centers, protecting proprietary

PE-9: Maintains backup power and climate control systems to safeguard sensitive testing equipment and servers, ensuring uptime during outages.

PS-3: Screens employees and contractors to prevent unathorized access to sensitive information or systems, critical in protecting intellectual property during recovery efforts.

PS-7: Manages and limits third-party access, ensuring vendors or contractors involed in disater recovery follow strict security protocols

References

https://www.securityscientist.net/blog/nist-sp-800-53-control-families/#control-family-8incident-response

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. Computer Science & Information Technology (CS & IT), 7(3), 51-62.

https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final